НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Троян Оксана Анатоліївна

УДК 004.921 + 004.93:002.1-028.25(043.5)

ДИСЕРТАЦІЯ
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РОЗРОБЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ЛАТЕНТНИХ ЗОБРАЖЕНЬ

05.13.06 – інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Троян О.А.

Науковий керівник – Назаркевич Марія Андріївна, доктор технічних наук, професор

Львів – 2019

АНОТАЦІЯ

Троян О.А. Інформаційна технологія розроблення та ідентифікації латентних зображень. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.06 «Інформаційні технології» (122 – Комп'ютерні науки). - Національний університет «Львівська Політехніка» МОН України, Львів, 2019.

З розвитком інформаційних технологій усе частіше постає питання забезпечення захищеності та достовірності друкованих документів, оскільки кількість фальсифікації із кожним роком збільшується як у державному, так і у приватному секторах. Підробка друкованих документів стає все поширенішою, тому потрібно кожного року удосконалювати методи та засоби захисту документів. ДД мають велике значення, оскільки посвідчують особу та підтверджують її статус у суспільстві. Відсутність захищеності документів може завдати шкоди та збитків державі та її громадянам. Для документів, які потребують захисту, існує низка економічно вигідних способів захисту, серед яких вагоме місце займають графічні елементи. Підвищення надійності друкованих документів можливе із застосуванням латентних зображень. Латентні зображення мають властивість зміни видимості елементів при зміні умов спостереження, що забезпечує ідентифікацію документа внаслідок захисних властивостей зображення.

В дисертаційній роботі представлено розв'язання наукового завдання, яке полягає у підвищенні захисту друкованих документів, завдяки розробленню інформаційної технології формування латентних елементів, яка містить методи побудови цих елементів та встановлення їх достовірності.

Перший розділ роботи містить огляд літературних та інформаційних джерел за темою дисертації в рамках існуючих інформаційних технологій розроблення моделей та засобів достовірності й ідентифікації друкованих документів, методів моделювання і виявлення прихованих елементів.

Проведено дослідження методів та існуючого інструментарію, інформаційних технологій, які використовуються для формування графічних елементів, а саме елементи тонкої графіки, латентні зображення, фрактали.

Опрацьовані статистичні дані показують, що в майбутньому з кожним роком буде зростати потреба у створенні інформаційних технологій різних видів, зокрема інформаційних технологій ідентифікації документів. Дослідження інформаційних технологій показали, що методи формування латентних зображень надають можливість підвищення надійності та ідентифікації документів.

Для розроблення таких інформаційних технологій є необхідно здійснити аналіз існуючих моделей захисту документів, розглянути та дослідити їхні переваги та недоліки.

На підставі проведеного огляду літературних джерел розглянуто методи формування латентних зображень, формування елементів тонкої графіки, моделі графічних пасток на основі муару, та різних модифікацій таких моделей.

У другому розділі показано метод формування латентних зображень для захисту друкованих документів, які захищають документ від несанкціонованого доступу накладанням на документ прихованих елементів. Розроблені методи моделювання латентних зображень і моделі формування латентних зображень з впровадженням прихованих зображень.

За допомогою розробленої математичної моделі формувати латентне зображення можливо не тільки шляхом комбінації різних растрових структур, що утворюють основне зображення, області яких визначаються на основі взаємно зворотних позитивної й негативної масок впроваджуваного зображення, а й внаслідок комбінації двох низькочастотних аперіодичних структур.

Розроблений метод створення латентних елементів у якому графічним елементом є зображення, яке складається з шарів з наперед заданими параметрами, що забезпечує підвищення точності побудови графічних елементів.

Третій розділ роботи присвячено реалізації методу тонкої графіки, призначений для імітаційного моделювання збурень ліній. Вдосконалено векторний метод для захисту друкованих документів, що ґрунтується на використанні математичного апарату, який забезпечує генерацію нових захисних елементів з високою точністю обчислень на основі формування тонкої графіки.

Удосконалено метод формування фрактальних елементів, в яких вибір параметрів генерації фракталу залежить від ступеня необхідного захисту: створення сіток на основі однотипних фракталів; створення сіток на основі двотипних фракталів, генератором яких є інший фрактал; створення сіток на основі патерну.

Також в третьому розділі реалізовано побудову моделей графічних пасток на основі формування муару. Враховуючи всі особливості методу муаротворення, для вирішення поставлених в дисертаційній роботі завдань за основу було вибрано класичний метод формування муру, оскільки він підходить для переважної більшості випадків виявлення спотворень в зображеннях. Було проведено експерименти та виведено 3 методи для ефективного виявлення спотворень в документах при спробі фальсифыкації. На основі розроблених методів запропоновано систему формування прихованих зображень з муаром, що дозволяють виявляти спотворення в латентному зображенні за допомогою чого дозволяють виявити фальсифікацію.

У четвертому розділі описано алгоритм побудови інформаційної технології для ідентифікації достовірності документів та приведено результати визначення параметрів оригінальних документів та копій; здійснено порівняльні характеристики документів на різних видах паперу відносно оригіналу та підробки (копії).

Проведено експерементальні дослідження розроблених методів, а також подано підтвердження ефективності розробленої інформаційної технології за допомогою засобів ідентифікації оригіналу та копій, що показало можливі

варіанти виявлення фальсифікації.

Для проведення експериментів використано метод оцінювання ефективності визначення достовірності даних на основі попіксельного порівняння та відповідно до результатів запропоновано критерій оцінювання параметрів, що впливають на ефективність.

Також було розроблено рекомендації для ідентифікації документів. Відповідно до запропонованого методу контролю достовірності документів було розглянуто та досліджено оригінали та копії на різних сортах паперу. Підтверджено ефективність роботи методу використання латентних зображень створених на основі тонкої гафіки, фракталів та виявлення муару, оскільки підвищує показники оригінальності відносно PSNR.

В ході досліджень було проведено експерименти на різних видах паперу, на яких було відображено документ з латентним зображеням та видрукувано копії кожного документу на різних пристроях. На основі цього експериментального дослідження було проаналізовано та досліджено оригінали та копії документів різного типу, а також можливість виявлення фальсифікації. Одним зі спеціальних інструментів для визначення ідентифікації та достовірності документа було використано денситометр та спектрофотометр x-rite spectroeye, який вимірює оптичну щільність, чіткість відтворення, рівномірність розподілення фарби на відбитку та розтиснення.

Значення отриманих результатів верифікують точність проведених експериментів та порогові значення показників оригінальності для ідентифікації. З результатів можна зробити висновки, що впровадження методу ідентифікації для забезпечення достовірності документів створює умови для прогнозування та прийняття рішень розв’язку достовірності документів на основі аналітичної залежності виміряних показників на оригіналі та копії знятої спектрофотометричним приладом. Розроблена система ідентифікації латентних зображень в документах характеризується високою точністю виявлення фальсифікації, функціональними можливостями врахування денсометричних показників, а також грунтується на використанні сучасної

техніки та програмних засобів, що дозволило використати для формування латентних зображень елементи тонкої графіки, фракталів та графічний пасток на основі формування муару. Такий підхід дав змогу підвищити ефективність інформаційної технології опрацювання параметрів ідентифікації, в якому порівняно з існуючими аналогами характерна нижча собівартість та висока точність визначення фальсифікації. Дані, отримані в результаті роботи можуть бути використані для вироблення друкованих документів з захищеними елементами для підвищення ефективності ідентифікації і, як наслідок, підвищення якості захисних властивостей документів та візуальне спотворення їх при спробі фальсифікації. Отже розроблений метод ідентифікації, що включає в себе формування латентних зображень, тонкої графіки, фракталів та муару показав кращі результати у порівнянні з існуючими за критеріальними ознаками порогових характерстиками на 10-15%.

Ключові слова: інформаційна технологія, латентні зображення, тонка графіка, графічні елементи на основі фракталів, графічні пастки з муару, ідентифікація, оригінальність докумсенту.

Список публікацій здобувача:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Назаркевич М.А. Розробка методу захисту документів латентними елементами на основі фракталів / М.А. Назаркевич, І.І. Дронюк, О.А. Троян, Т.Ю. Томащук // Захист інформації. – 2015. – № 1. – С. 21–26 (формування методу захисту на основі латентних елементів).
2. Troyan Oksana Identification latent elements in the printed and electronic documents // Вісник Національного університету «Львівська політехніка». Комп’ютерні науки та інформаційні технології. – 2016. – Вип. № 843. – С. 213 – 220 (аналіз методів захисту графічних елементів у друкованих документах).
3. Troyan Oksana Method of forming latent image to protect documents based on the effect moire // Вісник Національного університету «Львівська політехніка». Комп’ютерні науки та інформаційні технології. – 2015. – №

826. – С. 394 - 403.

4. Назаркевич М.А. Метод захисту документів на основі ефекту муару / М.А. Назаркевич, О.А. Троян // Науковий вісник НЛТУ України. – 2015. – Вип. 25.8. – С. 337 – 346 (метод формування графічних пасток на основі муару).
5. Dronjuk Ivanna “The Modified Amplitude-Modulated Screening Technology for the High Printing Quality” / Ivanna Dronjuk, Maria Nazarkevych, Oksana Troyan // International Symposium on Computer and Information Sciences, ISCIS 2016: Computer and Information Sciences, Krakow-Poland, Springer, 26 - 27October 2016. С. 270 - 276.
6. Назаркевич М.А. Розроблення програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням // М. А.Назаркевич, О.А.Троян // Вісник Національного університету «Львівська політехніка». Комп’ютерні системи та мережі. – Львів. – 2014. – Вип. № 806. – С. 187-194 (розроблення інформаційної технології захисту на основі латентних елементів).
7. Назаркевич М.А. Аналіз сучасних методів та видів графічного захисту друкованих документів // Назаркевич М.А., Троян О.А. // Вісник Національного університету «Львівська політехніка». Комп’ютерні науки та інформаційні технології. – Львів. – 2014. – Вип. № 800. – С. 61-65 (аналіз методів формування графічних захисних елементів).
8. Nazarkevych M.A. Method of electronic and printed documents of protection on the basis of moire effect / M. A. Назаркевич, О.А.Троян, І.М. Дронюк // Актуальні проблеми економіки, Київ – 2016. – Вип №5 (179) С. 382-394. (аналіз побудови моделей формування муару).
9. Назаркевич М.А. Математична модель захисту документів з формуванням муару на основі кратних періодичних решіток // М. А. Назаркевич, О.А. Троян // Комп’ютерні технології друкарства: Зб. наук. праць. – Львів: УАД, – 2015. – Вип. № 34 – С. 156 – 163 (аналіз та розроблення моделей муароутворення).

10. Назаркевич М.А. Разработка скрытого изображения для защиты документов с использованием эффекта муара. / Мария Назаркевич, Иванна Дронюк, Оксана Троян // Wspolczesne problemy bezpieczenstwa i marketingu. Marketing : [monogr. nauk.] / Wyzsza szkola zarzadzania marketingowego i jez. obcych w Katowicach ; pod red. nauk. A. Limanskiego, Katowice – 2015. – С. 215-226. (аналіз методів формуваня прихованих зображень).

Наукові праці, які додатково відображають наукові результати дисертації:

11. Пат. України на корисну модель 06221 України, МПК(2006) G 06 K 15/22. Спосіб захисту друкованих та електронних документів / І.М.Дронюк, М.А.Назаркевич, О.А.Троян, Л.В.Легкий; заявник і патентовласник Національний університет «Львівська політехніка».–№ a201406221; заявл. 05.06.2014; опубл. 26.08.2014, Бюл. № 16.– 4с.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Troyan O.A Analysis of threats falsification of printed documents / Troyan O.A, Korobchynskyi M., Didyk O. // Proceedings of the 2016 IEEE 1st International Conference on Data Stream Mining and Processing, DSMP – 2016. С. 248 - 253. (аналіз фальсифікації документів та способів їх виявлення).

13. Nazarkevych M. A. Data protection based on encryption using Ateb-functions / Nazarkevych M., Oliarnyk R., Troyan O., Nazarkevych H // Proceedings of the 11-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2016), Lviv. – 2016. – P. 30 - 32 (аналіз побудови графічних елементів).

14. Назаркевич М.А. Захист цінних паперів на основі нових методів захисту інформації / М. А. Назаркевич, О.А. Троян // Мат.V-ої міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем» – Львів. – 2016. – С. 150-151 (аналіз захисту цінних документів).

15. Troyan O. A. Development system of protection electronic document to

ensure the integrity and confidentiality of information / Troyan O. A. // Materials of the XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics. – Поляна. – 2015. – С. 376 – 378.

16. Medykovskyy M Methods of protection document formed from latent element located by fractals / Medykovskyy M., Lipinski P., Troyan O., Nazarkevych M., // Proceedings of the 10-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2015) Lviv. – 2015. – P. 70–73 (аналіз методів побудови графічних елементів з використанням фракталів).
17. Троян О.А. Розроблення вільного програмного забезпечення для захисту документів на основі латентних муарових елементів / О.А. Троян // Матеріали п’ятої міжнародної конференції FOSS Lviv. – Львів. – 2015. – С. 91-92.
18. Дронюк І.М. Метод створення мультимедійних документів, захищених ементами на основі ефекту «муар» / І.М.Дронюк, М. А. Назаркевич, О.А. Троян // Мат.XIV-ої міжнародного наукового семінару «Сучасні проблеми інформатики в управлінні, економіці, освіті». – Київ-Світязь. – 2015. – С. 207-209 (аналіз побудови муарних елементів).
19. Дронюк І.М. Метод захисту латентними елементами на основі ефекту муару / І.М.Дронюк, М. А. Назаркевич, О.А. Троян // Мат.IV-ої міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів. – 2015. – С. 179-180 (розроблення програмних засобів на основі методів формування муару).
20. Троян О.А. Спосіб захисту друкованих документів на основі латентних елементів за допомогою ефекту муару / О.А. Троян // Всеукраїнська конференція «Сучасні комп’ютерні інформаційні технології» АСІТ-2015. – Тернопіль. – 2015. – С.180-182.
21. Троян О.А. Спосіб захисту документів на основі латентних елементів побудованих за допомогою фрак талів / О.А. Троян // Міжнародна

науково-практична конференція «Комп'ютерні технології та інформаційна безпека». – Кіровоград. – 2015. – С. 31-32.

22. Назаркевич М. А. Розроблення вільного програмного забезпечення для захисту друкованих документів мікрографікою / М. А. Назаркевич, О.А. Троян // Матеріали четвертої міжнародної конференції FOSS Lviv – Львів. – 2014. – С.132-134 (аналіз створення захисних елементів мікрографікою).
23. Troyan O. Analysis and development of latent elements as a metod to protected documents / Troyan O.A., Tomashchyk T.Yu. // Proceedings of the 9-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2014) Lviv. – 2014. – P. 91- 92 (алгоритм побудови латентних зображень).
24. Троян О.А. Метод формування гільйошних елементів для задач захисту графічних зображень / О.А. Троян // Всеукраїнська конференція «Сучасні комп'ютерні інформаційні технології» ACIT-2014. – Тернопіль. – 2014. – С. 222-223.
25. Троян О.А. Аналіз латентних елементів на основі теорії Ateb-функцій / О.А.Троян // Міжнародна науково-практична конференція молодих вчених та студентів «Інформаційні технології, економіка та право: стан та перспективи розвитку». – Чернівці. – 2014. – С. 34-35.
26. Назаркевич М.А. Розроблення програмного забезпечення для захисту друкованих документів / М. А. Назаркевич, О.А. Троян // Матеріали IV науково-технічної конференції ITSEC. – Київ. – 2014. – С. 33-34 (розроблення програмних засобів для захисту документів).
27. Троян О.А. Аналіз біометричних видів захисту інформації / О. А.Троян , М. А.Назаркевич, З. Я.Шпак , І.І.Клюйник // матеріали Міжнародної науково-практична конференція «Сучасні наукові підходи до стабільного економічного розвитку та економічної безпеки». – Чернігів. – 2014. – С. 45-47 (аналіз біометричних способів захисту).
28. Troyan O. A. Development protection software document based on the

engraving / O.A.Troyan , Terlecka N. T., Oliyarnik R. // Global scientific unity 2014. – Prague, Czech Republic. – 2014. – С. 146-152 (аналіз програмних засобів формування прихованих елементів).

29. Назаркевич М.А. Технологія графічного способу захисту документів на основі гравюр // М. А. Назаркевич, О.А. Троян // ІІІ-ої Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології». – Одеса. – 2014 – С.175-178 (аналіз засобів захисту на основі гравюр).
30. Назаркевич М.А. Аналіз сучасних методів та програмних ужитків з графічним захистом друкованих документів / М. А. Назаркевич, О.А. Троян // Технічні вісті: 2013/1 (37), 2 (38). – С. 42-44 (аналіз формування тонкої графіки).
31. Nasarkevych M.A. Analysis of software protection and development of methods of latency in printed documents/ Nasarkevych M.A., Troyan O. A. // Proceedings of the 8-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2013) Lviv. – 2013. – P. 120-121 (аналіз методів захисту друкованих документів з вбудованими латентними елементами).

ABSTRACT

Troyan O.A. Information technology for the development and identification of latent images. – Proficiency scientific treatise on the rights of the manuscript.

A thesis submitted in fulfilment of the candidate of sciences (Ph.D.) degree in technical sciences on specialty 05.13.06 «Information technologies» (122 – Computer Sciences). - Lviv Polytechnic National University of Ministry for Education and Science of Ukraine, Lviv, 2018.

With the development of information technology, the issue of identification of printed documents is increasingly being raised, as the amount of fraud is continuously increasing in both public and private sectors. Counterfeiting of printed documents is becoming more widespread. Every year, the means and methods of protection are becoming more modern and combined. The printed documents play a significant role in society, because they are used to identify a person, to certify certain legal aspects, and to support money circulation. Such documents usually require protection, as they are advantageous for falsification. The lack of protection for such documents can cause the damage to the state and its citizens. Therefore, there is a need to develop the security tools for the printed documents. The increase of reliability becomes possible by applying graphic elements, namely latent images. The latent images have one common property - a change in the elements visibility of an image when changing the conditions of observation.

The dissertation presents the solution of the scientific problem, which is to provide the appropriate level of security of printed documents using the latent elements of the information technology, which includes the methods for forming these elements and establishing their reliability.

The first section of the paper contains an overview of and informational sources on the topic of the dissertation within the framework of existing information technology development models and means of authenticity and identification of printed documents, methods of modeling and detecting hidden elements. The

research of methods and existing tools, information technologies, which are used for the formation of graphic elements, namely, elements of thin graphics, latent images, fractals, are carried out.

The processed statistics show that in the future, with each passing year, the need to create information technologies of different types, in particular, information technologies of document identification will increase. The study of the laws of building information technology has shown that the methods of latent image creation provide an opportunity to increase the reliability and identification of documents.

For the development of such information technologies, it is necessary to analyze the existing models of document security, to consider and explore their advantages and disadvantages.

Based on the review of literary sources, methods of forming latent images, forming elements of fine graphics, models of graphic traps on the basis of a moiré, and various modifications of such models are considered.

The second section shows a method for creating the latent images for the protection of the printed documents that protect the documents from an unauthorized access by overlaying a document on the hidden elements. The methods of modeling the latent images and the model of latent image formation with the implementation of the concealed images are developed.

With the help of the developed mathematical model, a latent image can be formed by the combination of different raster structures forming the main image, which areas are determined on the basis of mutually reversible positive and negative masks of the image being introduced, but also due to the combination of two low frequency aperiodic structures.

The method of creating latent elements in contrast to the known graphic element is an image consisting of layers with pre-set parameters, which provides an increase in the accuracy of constructing graphic elements.

The third section of the work is devoted to the implementation of the fine-grained method, designed to imitate the simulation of lines perturbations. The vector method for the protection of printed documents, based on the use of a mathematical

apparatus is improved. The apparatus provides the generation of new protective elements with high accuracy of calculations based on the formation of fine graphics.

The method of fractal elements formation, in which a choice of a fractal generation parameters depends on the degree of the necessary protection is developed. The following parameters were used: the creation of grids based on the same type of fractals; creation of networks based on two-type fractals, the generator of which is another fractal; creating grids based on the pattern.

Taking into account all the features of the method of moire, for the solution of the problems posed in the dissertation work, the classic method of forming the wall was chosen as the basis, since it is suitable for the vast majority of cases of detecting distortions in images. On the basis of the developed methods, a system of formation of hidden images with a hidden moire, which allows revealing inaccurate information in a latent image and a numerical method of control of latent images, which depend on a specific method of latent image formation, is proposed.

The fourth section describes the structural-functional model of information technology for the development and identification of the document authenticity shows the results of determining the parameters of original documents and copies. The coefficients of document security efficiency are determined. The comparative characteristics of the preprint processes on different types of paper in relation to the original and fake copies are carried out.

The testing of the developed methods is carried out in aggregate. In addition, the confirmation of the developed information technology effectiveness with the help of identification means of the original and copies showed the possible variants of falsification detection.

For conducting experiments, a method for evaluating the effectiveness of information technology per the results is proposed as a criterion for evaluating the parameters that affect efficiency. An example of using a guaranteed result in the field of measuring technology is the valuation of errors in measuring instruments by classes of accuracy.

The recommendations for optimizing document identification were developed

as well. In accordance with the previously proposed method of checking the authenticity of the documents, the original and copies of different types of paper were examined and investigated. The efficiency of the method of using the latent images created on the basis offine wafers, fractals and the detection of moiré has been confirmed, as it increases the quality indices relative to the PSNR and increases the reliability of the documents on the basis of indicators.

During the research, the experiments were conducted on paper models, in which a latent image document was displayed, and 3 copies of each document were printed on different devices. On the basis of this study, the originals and copies of different document types were analyzed and investigated, as well as the possibility of generating samples of falsification and the possibility of their detection. One of the special tools for identifying and verifying the document was the densitometer and x-rite spectroeye spectrophotometer, which measures optical density, reproducibility, and evenness of ink distribution and print.

The value of the obtained results verifies the accuracy of the performed experiments and the selected data samples, and the parameters of the identification efficiency. The results demonstrate that the introduction of the identification method to ensure document authenticity and on the basis of collected and processed values of the parameters of printed documents and their counterfeits creates conditions for forecasting and decision-making of the decision of the authenticity of documents and on the basis of analytical dependence of the original and a copy of the captured spectrophotometric instrument of indicators. The developed system of identification of the latent images in documents is characterized by high accuracy of detection of falsification and functional capabilities of accounting the densitometric indicators. Moreover, based on the use of modern elemental base and software tools the system allowes using thin graphic elements, fractals and graphic traps on the basis of moiré formation for the creation of latent images. Such approach enabled us to increase the efficiency of information technology for the processing of identification parameters, which, in comparison with existing ones, is characterized by lower cost and high accuracy of the definition of falsification. The obtained data can be used for the

production of printed documents with protected elements for increasing the efficiency of identification and, as a consequence, improving the quality of original documents and visual distortion of documents when attempting to falsify. Thus, the developed method of identification, which includes the formation of latent images, fine graphics, fractals, and moiré showed better results comparing with the threshold criteria by 10 – 15%.

Keywords: information technology, latent images, thin graphics, graphic elements on the basis of fractals, graphic traps from the moiré, identification, originality of the document.

The list of author's publications:

Proceedings where basic scientific results of thesis were published:

1. Nazarkevych M.A. Development of the method of protection of documents by latent elements on the basis of fractals / M.A. Nazarkevych, I.I. Dronyuk, O.A.Troyan, T.Yu. Tomashchuk // Information Protection. - 2015. - № 1. - P. 21-26.
2. Troyan Oksana Identification latent elements in the printed and electronic documents // Bulletin of the National University "Lviv Polytechnic". Computer Science and Information Technology. - 2016. - Voip. No. 843. - P. 213-220.
3. Troyan Oksana Method of forming latent image to protect documents based on the effect of moire // Bulletin of the National University "Lviv Polytechnic". Computer Science and Information Technology. - 2015. - No. 826. P. 394-403.
4. Nazarkevych MA The method of document protection based on the effect of the miura / M.A. Nazarkevych, O.A. Troyan // Science jor. of NLTU of Ukraine. - 2015. - Issue 25.8 C. 337-346.
5. Dronjuk I. "The Modified Amplitude-Modulated Screening Technology for High-Quality Printing" / Ivanna Dronjuk, Maria Nazarkevych, Oksana Troyan // International Symposium on Computer and Information Sciences, ISCIS 2016: Computer and Information Sciences (Krakow-Poland, 26-27 October

2016) p. 270-276 (Sciometric database of Scopus and IEEE);

6. Nazarkevych M.A. A review of the program for the protection of infrmation on the proper films with a positive logging // M. A.Nazarkevych, O.A.Trojan // Bulletin of the National University of Lviv Polytechnic. Competitive Systems and Measurements. - Lviv. - 2014. - Vip. №806. - P. 187-194.
7. Nazarkevych M.A. Analisation of common materials and types of graffiti protection of printed materials / Nazarkevych MA, Troyan O.A. // Bulletin of the National University of Lviv Polytechnic. Computational nauki and infromativnye tehnologii.- Lviv. - 2014. - Vip. No. 800.- P. 61-65.
8. Nazarkevych M.A. Method of electronic and printed documents of protection on the basis of moire effect // MA Nazarbekevich, O. A. Troyan, I. M. Dronyuk / / Actual Problems of Economics, Kyiv // K .: 2016.- Vip No. 5 (179) S.382-394.
9. Nazarkevych M.A. A mathematical model for the protection of students in the formulation of a múrau on the basis of crude periodic reticheks // MA Nazarkevych, O.A. Troyan // Computational Teaching of the Printing Company: Assoc. naak work - Lviv: UAD, 2015. - Vip. No. 34- P.156-163.
10. Nazarkevych M.A. Development of a latent image for protection of documents using Moira's effect. / Nazarkevych M., Dronyuk I., Troyan O. // Wspolczesne problemy bezpieczenstwa i marketingu. Part III Uncategorized about the current technology. Monografia naukowa pod red. Jerzego Kuck Katowice 2015.- 215-226.

Scientific works, which additionally reflect the scientific results of the dissertation:

11. Pat. 06221 Ukraine, IPC: (2006) G 06 K 15/22 Workers for the protection of printers and ecclesiastical engineers / I.M.Dronyuk, M.A.Nazarkevych, O.A.Trooyan, L.V.Legky; Owner: Lviv Polytechnic National University. - № 201406221; stated. 5.06.2014; Publicated Aug 26, 2014, Bul. No. 16. - 4p.

Proceedings that certify an approvement of thesis materials:

12. Troyan OA Analysis of threats falsification of printed documents / Troyan OA, Korobchynskyi M., Didyk O. // Proceedings of the 2016 IEEE 1st

International Conference on Data Stream Mining and Processing, DSMP - 2016. - 978-1-5090- 3736-0 - pp. 248 – 253.

13. Nazarkevych M. A. Data protection based on encryption using Ateb-functions / Nazarkevych M., Oliarnyk R., Troyan O., Nazarkevych H. // Proceedings of the 11th International Scientific and Technical Conference "Computer Science and Information Technologies »(CSIT 2016) Lviv. - 2016. - P. 30 - 32.
14. Nazarkevych M.A. Securities protection on the basis of new methods of information security // MA Nazarkevych, OA Troyan // Mat.V-th international scientific and technical conference "Information Protection and Security of Information Systems" .- Lviv. - 2016. - p.150-151.
15. Troyan O. A. Development of a system of electronic document security for the integrity and confidentiality of information // Troyan O. A. // Materials of the XIIIth International Conference. The Experience of Designing and Application of CAD Systems in Microelectronics. - Polyana - 2015. - pp. 376 - 378.
16. Medykovskyy M. Methods of protection document formed from latent element located by fractals / Medykovskyy M., Lipinski P., Troyan O., Nazarkevych M. // Proceedings of the 9th International Scientific and Technical Conference "Computer Science and Information Technologies »(CSIT 2015) Lviv. - 2015 - P. 70 - 73.
17. Troyan O.A. Development of free software for protection of documents on the basis of latent moirial elements / O.A. Troyan // Proceedings of the Fifth International Conference FOSS Lviv.- Lviv. - 2015. - p.91 - 92.
18. Dronyuk I.M. Method of creating multimedia documents protected by elements based on the moire effect // I.M.Druniuk, M.A. Nazarkevych, O.A. Troyan // Mat.HIV-th international scientific seminar "Modern problems of informatics in management, economy, education". .- Kyiv-Svityaz .- 2015.- p.207 - 209.
19. Dronyuk I.M. The method of protection of latent elements on the basis of the moiar effect // I.M.Dronyuk, MA Nazarkevych, O.A. Troyan // Mat. IV

International Scientific and Technical Conference "Information Protection and Security of Information Systems." Lviv.-2015. - P.179 - 180.

20. Troyan O.A. A method for protecting printed documents based on latent elements using the effect of moir / OA. Troyan // All-Ukrainian Conference "Modern Computer Information Technologies" ASIT-2015.-Ternopil.-2015. - p.180 - 182.
21. Troyan O.A. A method for protecting documents based on latent elements constructed using coats / O.A. Troyan // International scientific-practical conference "Computer technologies and information security" .- Kirovograd.- 2015. - P. 31 - 32.
22. Nazarkevych MA Development of free software for protecting printed documents by micrography / MA Nazarkevych, O.A. Troyan // Proceedings of the Fourth International Conference FOSS Lviv-Lviv. - 2014.-pp. 132 - 134.
23. Troyan O. Analysis and development of latent elements as a metod to protected documents / O. A. Troyan, T. Yu. Tomashchyk // Proceedings of the 9-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2014) Lviv. – 2014. – P. 91 - 92.
24. Troyan O.A. Method of formation of guilloche elements for protection of graphic images / O.A. Troyan // All-Ukrainian Conference "Modern Computer Information Technologies" ASIT-2014.- Ternopil.- 2014.- P.222 - 223.
25. Troyan O.A. Analysis of latent elements based on the theory of Ateb-functions / O.A.Troyan // International scientific and practical conference of young scientists and students "Information technologies, economics and law: state and prospects of development" .- Chernivtsi. - 2014. p. 34 - 35
26. Nazarkevych M.A. Development of software for the protection of printed documents / MA Nazarkevych, OA Troyan // Proceedings of IV scientific and technical conference ITSEC.- Kyiv.-2014. - p.33-34.
27. Troyan O.A. Analysis of Biometric Types of Information Protection / O.A.Troyan, M.A.Nazarkevych, Z.Ya.Shpak, I.I.Klyunik // Materials of the International Scientific and Practical Conference "Modern Scientific

Approaches to Sustainable Economic Development and Economic Security". - Chernigov - 2014. - p.45 - 47.

28. Troyan O. A. Development protection software document based on the engraving / O.A.Troyan, Terlecka N.T., Oliyarnik R. // Global scientific unity 2014.- Prague, Czech Republic. - 2014. - p.146 - 152.
29. Nazarkevych M.A. Technology of Graphic Method for the Protection of Documents Based on Engravings // MA Nazarkevych, OA Troyan // Third International Scientific and Practical Conference "Information Control Systems and Technologies." - Odesa. - 2014. - p.175 - 178.
30. Nazarkevych MA Analysis of modern methods and software applications with graphic protection of printed documents / MA Nazarkevych, OA Troyan // Technical News: Coll. naak work - Lviv - 2013 - S. 42 - 44.
31. Nasarkevych M.A. Analysis of software protection and development of latency in printed documents / Nasarkevych MA, Troyan O. A. // Proceedings of the 8th International Scientific and Technical Conference "Computer Science and Information Technologies" (CSIT 2013) Lviv . - 2013. - P. 120 - 121.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АЦП - аналогово-цифрових перетвореннь

ГКЗ - графічні кодовані зображення

ГР – графічний елемент

ГКД - графічним кодованим зображенням

ГСЗ – графічний спосіб захисту

ГП – графічні пастки

ДД – друковані документи

перетворенню

ЕЦП – електронний цифровий підпис

ЗЕ – захисний елемент

ЗК – захисний комплекс

ЗДП - захисту друкованої продукції

ЗДД - захист друкованих документів

ЗПП – захищена поліграфічна продукція

ІЧ- – інфрачервоне випромінювання

КІ – конфіденційна інформація

ЛЗ – латентні зображення

МЗ – модель загроз

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ПЗ – програмне забезпечення

УФ – ультрафіолетове випромінювання

ТЗ – текстуровані зображення

ПОСШ – відношення попіксельного об’єкту сигнал/шум

ДВП – дискретне вейвлет-перетворення

ЕДП – електрографічними друкуючими пристроями

РЗ – Роздільна здатність

СКО – середньоквадратичної описки

ЦПДСО – цінні папери та документи суворого обліку

ЦАП - цифро-аналогових перетвореннь

ISO – міжнародна організація по стандартизації

PDF – *Portable Document Format*

PS – *PostScript* файл

ВСТУП

Актуальність теми. З розвитком інформаційних технологій усе частіше постає питання забезпечення захищеності та достовірності друкованих документів, оскільки кількість фальсифікації із кожним роком збільшується як у державному, так і у приватному секторах. Підробка друкованих документів стає все поширенішою, тому потрібно кожного року удосконалювати методи та засоби захисту документів. Друковані документи мають велике значення, оскільки посвідчують особу та підтверджують її статус у суспільстві. Відсутність захищеності документів може завдати шкоди та збитків державі та її громадянам. Для документів, які потребують захисту, існує низка економічно вигідних способів захисту, серед яких вагоме місце займають графічні елементи. Підвищення надійності друкованих документів можливе із застосуванням латентних зображень.

Латентні зображення мають властивість зміни видимості елементів при зміні умов спостереження, що забезпечує ідентифікацію документа внаслідок захисних властивостей зображення. Це потребує розробленння технології створення і виявлення прихованої частини, що формує вимоги до точності друку і складності відтворення. Розроблення інформаційних технологій, які ідентифікують фальсифікації документів, включено в перелік пріоритетних завдань у сфері інформаційних та комунікаційних технологій, затверджених Постановою Кабінету Міністрів України № 4198 від 11.03.2016.

Аналіз сучасного стану інформаційних технологій вказує на існування певного протиріччя між високими технічними вимогами створення латентних зображень, які б забезпечували точну побудову прихованих елементів із подальшою ідентифікацією та певними прогалинами їх формування на базі сучасних наукових підходів.

Методи та засоби формування графічних елементів підтверджено великою кількістю наукових досягнень українських і закордонних дослідників. Серед них варто відзначити результати, отримані такими науковцями як

Amidror I. (дослідження муару), Коростіль Ю.М., Шевчук А. В., Киричок П.О. (захист документів спеціального призначення), Коншин А. А. (рівні контролю фальсифікації), Шовгенюк М.В., Козловський М.П., Крохмальський Т.Є. (спосіб формування цінних паперів графічним кодованим зображенням), Дурняк Б. В., Пашкевич В.З (розроблення математичної моделі створення графічних елементів), Пелешко Д.Д. (локальні спотворення зображень), Медиковський М.О. (методи аналізу та пошуку за вмістом графічних об'єктів), Цмоць І.Г., Ткаченко Р.О., Березький О.М. (методи обробки зображень), Теслюк В.М., Пукач А.І. (методи фрактального стиснення зображень).

Незважаючи на велику кількість праць у цій області, залишається нерозв’язаною задача забезпечення достовірності друкованих документів. Таким чином, актуальність теми дисертаційного дослідження визначає важливість завдання підвищення захищеності друкованих документів, завдяки розробленню інформаційної технології формування латентних елементів, яка містить методи побудови цих елементів та встановлення їх достовірності.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційна робота пов’язана з планами науково-дослідної та навчальної роботи Інституту комп’ютерних наук та інформаційних технологій Національного університету «Львівська політехніка». Дисертація відповідає науковому напряму кафедри інформаційних технологій видавничої справи «Технологія підвищення графічного рівня захищеності друкованих та електронних документів». Робота виконано в межах держбюджетних науково-дослідних робіт на кафедрі інформаційних технологій видавничої справи: «Розвиток теорії синтезу нейронних мереж на НГВС-структурах для обробки сигналів в робототехнічних системах» (№ державної реєстрації 0112U001204), «Відслідкування рухомих об’єктів у відеопотоках реального часу» (№ державної реєстрації 0115U000432) та на основі досліджень наданої грантової підтримки Державного фонду фундаментальних досліджень (проект № Ф62 / 75 - 2015).

Мета і завдання дослідження. Метою дисертаційної роботи є розроблення інформаційної технології формування латентних зображень для підвищення захисту та зменшення вартості документів при їх створенні.

Досягнення цієї мети забезпечує розв'язання таких завдань:

1. дослідити та проаналізувати моделі та методи формування графічних елементів, а також встановити переваги та недоліки;
2. розробити метод формування латентних зображень для забезпечення достовірності документа;
3. реалізувати моделі побудови графічних пасток на основі формування муару, які покращують ідентифікацію областей фальсифікації;
4. удосконалити моделі побудови графічних елементів на основі формування фракталів, які під час копіювання частково чи повністю спотворюють об'єкти;
5. удосконалити метод формування елементів тонкої графіки в інформаційній технології, які завдяки їх побудови із врахуванням умов друку унеможливлюють несанкціоновану модифікацію документа;
6. розробити інформаційну технологію, яка містить латентні зображення, тонку графіку, фрактали, графічні пастки на основі муару і за результатами аналізу надати підтвердження практичної цінності розроблених методів та моделей.

Об'єктом дослідження є процеси розроблення латентних зображень для ідентифікації оригінальності документів.

Предметом дослідження є методи та засоби створення інформаційної технології ідентифікації документів, що ґрунтується на використанні моделей формування графічних елементів для контролю та виявлення спотворень у документах.

Методи дослідження. Для розв'язання поставлених в дисертаційній роботі завдань використано: методи математичного аналізу та моделювання,

методи комп'ютерної графіки, методи наближених обчислень, теорію алгоритмів та методи денситометрії для вимірювання оптичної густини та контролю якості друку.

Наукова новизна одержаних результатів полягає в розробленні інформаційної технології формування латентних елементів та ідентифікації документів, які сформовано на основі графічних елементів:

вперше:

- розроблено метод формування латентних зображень у якому елементами є лінії векторного формату, які формують зображення шарами з наперед заданими градієнтними властивостями та забезпечують підвищення графічних характеристик побудови документу;
- розроблено моделі графічних пасток на основі муару, які завдяки зміні періодів решіток, кутів нахилу та товщин ліній дають змогу встановити оригінальність елементів;
- розроблено інформаційну технологію, яка передбачає формування прихованих зображень із латентними елементами, тонкою графікою, фракталами, графічними пастками на основі муару та ідентифікує ці зображенння за критеріальними ознаками, що дає змогу визначити оригінальність документа з урахуванням умов друкування.

вдосконалено:

- моделі побудови графічних елементів на основі формування фракталів, які завдяки рекурсивній процедурі покривають всю площу зображення із заданими параметрами дроблення, що забезпечує побудову відбитка із високою точністю;

отримав подальший розвиток:

- метод створення елементів тонкої графіки, який на етапі формування захищених документів створює умови для вибору позитивних та негативних ліній, що забезпечує візуалізацію прихованих елементів під час копіювання та дозволяє виявити спотворення в документах.

Практичне значення отриманих результатів. Полягає у розробленні інформаційної технології формування та ідентифікації латентних зображень способом ускладнення відтворюваності прихованих елементів, а саме:

1. на основі розробленого методу формування латентних елементів, який завдяки використанню технології накладання шарів із деякими градієнтними характеристиками підвищує ефективність виявлення підробки на 4.2%;
2. на основі методу формування елементів тонкої графіки розширено функціональні можливості створення графічних елементів для позитивного виконання ліній 40 - 80 мкм та для негативного – 60 - 100 мкм, що характеризується стійкістю до спотворення зображення внаслідок розпадання векторних ліній на растрові крапки під час копіювання (патент «Спосіб захисту друкованих та електронних документів»);
3. використання графічних пасток, які формуються при створенні тонких паралельних ліній завширшки 0.25мм та частотами повторень, які кратні цілому числу і виявляються при муарі для друкованих документів підвищують достовірність документів;
4. розроблено моделі графічних елементів, які утворюють на основі фракталу у векторному форматі за допомогою рекурсивної процедури підвищують надійність та гарантують високу якість відтворення документів;

Розроблені методи ідентифікації документів підвищують точність оцінювання достовірності документів на основі сумісного використання графічних елементів та структурних характеристик прихованих зображень на 10 - 15%.

Результати дисертаційних досліджень реалізовано та впроваджено.

Роботу виконано на основі досліджень за грантової підтримки Державного фонду фундаментальних досліджень «Технологія підвищення графічного рівня захищеності друкованих та електронних документів» (номер

державної реєстрації 0115U004704). У проведених експериментальних дослідженнях розроблені в роботі методи на основі аналітичної залежності оригіналу та копії підтвердили свою ефективність. Розроблена в процесі досліджень інформаційна технологія розширює функціональні можливості захисних властивостей документів, а також підвищує надійність та достовірність документів. Достовірність результатів. Для перевірки достовірності отриманих здійснено практичну реалізацію запропонованої інформаційної технології, яка використовувалась для організації та обслуговування технологічних процесів виготовлення та використання захищених документів на Нафтогазовидобувне управління «Бориславнафтогаз» відкритого акціонерного товариства «Укрнафта».

Результати випробувань свідчать про коректність програмної реалізації розробленої інформаційної технології. Результати захисту документів у достатній мірі корелюють із результатами теоретичного дослідження, що відображено у дисертаційній роботі.

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи отримані автором самостійно. Одноосібно опубліковані праці – [2, 3, 15] розроблення латентних зображень на основі локального викривлення лінії сітки; [17, 20] – фомування латентних зображень з застосуванням муару; [21, 24, 25] – формування захисних елементів для підвищення захисту документів. У працях, опублікованих у співавторстві, автору належать: [12, 13, 22] –способи побудови графічних елементів для захисту документів; [1, 16] – розроблення методу захисту на основі фракталів; [4, 8, 9, 10, 18] – формування графічних пасток на основі муару; [6, 14, 19] – розроблення латентних зображень; [7, 30] – спосіб захисту графічними побудовами; [5, 26] – формування інформаційної технології підвищення рівня захищеності; [23, 31] – ідентифікація латентних елементів в документах; [11] – ідентифікація та формування градієнтних властивостей графічних елементів; [27] – аналіз біометричних способів захисту; [28, 29] – розроблення графічного способу на основі гравюр..

Апробація результатів дисертації. Основні положення та результати роботи були представлені та обговорені та доповідались на міжнародних та всеукраїнських конференціях, а саме: Wspolczesne problemy bezpieczenstwa i marketingu. Bezpieczenstwo w obszarze nowych technologi, Katowice, Poland, 2015; International Symposium on Computer and Information Sciences, Krakow, Poland, 2016; IEEE First International Conference on Data Stream Mining & Processing (DSMP), Львів, Україна, 2016; The XII International scientific conference «Intellectual systems for decision making and problems of computational intelligence» (ISDMCI-2016), Херсон, Україна, 2016; 5-а міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», Львів, 2016; The XIV International Scientific workshop «Modern problems of computer science in management, economics, and education», Київ - Шацьк, Україна, 2015; Global scientific unity, Prague, Czech Republic, 2014; IEEE International Conference «Computer Sciences and Information Technologies» (CSIT'2013), Львів, Україна, IEEE International Conference «Computer Sciences and Information Technologies» (CSIT'2014), Львів, Україна 2014, IEEE International Conference «Computer Sciences and Information Technologies» (CSIT'2015), Львів, Україна 2015, IEEE International Conference «Computer Sciences and Information Technologies» (CSIT'2016), Львів, Україна 2016; Free/Libre and Open-Source Software (FOSS 2014), Львів, Україна, 2014, Free/Libre and Open-Source Software (FOSS 2015)), Львів, Україна 2015; 13th International Conference on Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) Львів – Поляна, Україна, 2015.

Матеріали дисертації регулярно доповідались та обговорювались на наукових семінарах кафедри інформаційних технологій видавничої справи Національного університету «Львівська політехніка» (2012 – 2017 рр.).

Публікації. Основні положення та результати дисертаційного дослідження викладено в 31 науковій публікації, серед них 6 статей у наукових фахових виданнях України з технічних наук; 2 статті у наукових фахових виданнях України, що включені до наукометричних баз даних; 1 патент

України на корисну модель; 1 колективна монографія (розділ 5); 21 публікація тез доповідей та матеріалів конференцій, з яких 5 у виданнях, які включено до міжнародних наукометричних баз даних.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаної літератури та додатків. Загальний обсяг дисертації – 189 сторінок, у тому числі 148 сторінки основного тексту, 64 рисунки та 6 таблиць, список використаних джерел налічує 176 бібліографічних найменувань на 19 сторінках. Дисертація містить 3 додатки, розміщені на 20 сторінках.

РОЗДІЛ 1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ФОРМУВАННЯ ЛАТЕНТНИХ ЕЛЕМЕНТІВ В ДРУКОВАНИХ ДОКУМЕНТАХ

У першому розділі проведено аналіз існуючих інформаційних технологій, розроблених моделей та засобів достовірності й ідентифікації друкованих документів, методів моделювання і виявлення латентних елементів. Детально проаналізовано сучасний стан інформаційних технологій, які забезпечують надійність документів в Україні, проведено аналіз теоретичних та прикладних засад побудови та впровадження інформаційних технологій для формування прихованих зображень.

1. Аналіз та порівняння формування латентних зображень

З кожним роком поява нових документів, які потребують захисту зростає у співвідношенні до кількості підробки та методів фальсифікації. Все частіше документи, які перебувають в обігу у приватному секторі піддаються частковій чи повній підробці. Банкноти, ЦПДСО, векселі, акцизні марки, бюлетні – документи, які потребують захисту через МЗ. Для складності здійснення підробок такого виду документ повинен мати спеціальні захисні ознаки. На сьогоднішній день методи ЗДП класифікуються за етапами їх реалізації. Особливо потрібно звернути увагу на методи та засоби захисту, які відбуваються під час додрукарської підготовки. Тому виникає потреба ЗДД. У роботах авторів [21 - 23], коли прихований елемент представлено двома зображеннями, використовуються поняття «латентне зображення» (latent image), що представляє із себе заповнений елемент з метою виявлення при певних змінах в зображенні.

В дисертаційній роботі, для позначення зображень, що містять приховану інформацію у вигляді іншого зображення використовується термін «латентне зображення» - ЛЗ. До ЛЗ відносяться зображення, основною

властивістю яких є зміна видимості елементів ТЗ при зміні умов спостереження або способу реєстрації основного зображення.

В даний час ЛЗ широко застосовуються в різних сферах для захисту документів від копіювання. Разом з тим не існує універсального способу виявлення латентних зображень в друкованих документах, в зв'язку, з чим також є дорогим процес виявлення підробки.

Для виявлення латентного зображення використовуються оптичні методи контролю, засновані на здатності прихованого зображення стати видимим під кутом або з використанням ІЧ чи лазерних променів за допомогою спеціальної техніки [24 - 26].

Латентні зображення - це група зображень, що мають одну спільну властивість, а саме зміну видимості певних частин ТЗ при зміні кута видимості. Латентні зображення створюються різними способами: за допомогою засобів голографії, з використанням явища поляризації, із застосуванням спеціальних фарб і покриттів, за рахунок певного методу формування елементів зображення, що можна віднести до графічних засобів захисту. [1-8]

Метод формування латентних зображень об'єднують три відмінні риси. По-перше, приховані зображення невидимі, по-друге вони невіддільні від зображення, в яке вмонтовані, тому вони не можуть бути видалені, коли латентне зображення перетворять або частково замінюють. По-третє, зображення піддаються тим же перетворенням, що дає можливість дізнатися, які зміни відбувалися [10-14]. Таким чином, латентні зображення можуть застосовуватися для вирішення наступних завдань:

1. Ідентифікація. Закон про авторське право встановлює певні права законного власника оригіналу. Оригінал відрізняється від копії певними характеристиками, які притаманні тільки при формуванні документу з латентними зображеннями. Якщо документ скопійовано, то ці характеристики мають нижчі показники параметрів. Щоб визначити оригінальне зображення вбуддовується приховане зображення. Завдяки

невидимості і невіддільності прихованого зображення від документу є можливість ідентифікації оригіналу та копії під час кадрування [9].

2. Відстеження копій. Дане завдання передбачає можливість в разі встановлення факту створення копій відстежити, що документ є підробкою. Впровадження латентних зображень містять унікальне для кожної копії приховане зображення, яке спотворюється та дозволяє з втратами візуальної якості і порушення художньої композиції помітити фальсифікацію.
3. Аутентифікація. Для вирішення завдань визначення цілісності зображень, що передається зазвичай використовуються захисні ознаки [15]. Аналогом захисних ознак можуть служити латентні зображення. В даному випадку є можливість визначити, яка саме область зображення була змінена, а не тільки дізнатися про факт такої зміни.
4. Контроль копіювання. Дане завдання передбачає неможливість копіювання зображення в цілому або його частин. Латентні зображення можуть служити сигналом для копіювального пристрою про неможливість копіювання. Обмеженість такого рішення очевидне, оскільки немає закону, який би зобов'язував постачати всі пристрої відтворення необхідними детекторами латентних зображень [17]. Однак в ряді областей дані методики знайшли широке застосування. Прикладами таких систем є Сузір'я Евріона [28], Advanced Access Content System [146].

Також, при копіюванні, на увазі технічних особливостей копіювальних пристроїв, приховане зображення або стає видимим на копії, або не відтворюється на копії [29-33]. Згідно ГОСТу [114] при виготовленні захищеної поліграфічної продукції всіх вищих рівнів захищеності: "А", "Б", "В" обов'язкова наявність трьох різних ГР захисту продукції, під які потрапляють, в тому числі і латентні зображення. Таким чином, під латентним зображенням можна розуміти ТЗ, що містить приховану інформацію у вигляді іншого зображення, під яким розуміється вбудовування не тільки графічної інформації, а й у якого елементами виступають як ТЗ.

1.1. Аналіз методів графічного захисту друкованих документів

Для підвищення ЗДД з кожним роком розробляють та застосовують нові комбіновані способи та комплекси для безпеки та достовірності інформації в документах. Друковані документи відіграють значну роль у інформаційній безпеці держави. Потрібно розробляти та впроваджувати впроваджувати нові технології для підвищення рівня захищеності документів. Захист інформації в друкованих документах повинен відбуватись з урахуванням критеріїв надійності, ефективності та економічності, що дасть можливість розвинути захист в документах та підвищити його ступінь [47 - 50]. Захищений документ має декілька ступенів захисту, а саме перше - складність відтворення технологічних процесів, які були застосовані саме до цього виду графічного захисту, наприклад, глибокий чи металографічний вид друку; друге – використання певного типу матеріалів та обладнання, наприклад, спеціальні фарби і покриття, захисні ламінати, голограми – хоча такі способи є дорогими та економічно невигідними; третє - це закритий доступ та новизна використаних методів та засобів формування нових ГР або застосування спеціального обладнання чи матеріалів із фізичними чи хімічними властивостями [18-20].

На даному етапі існує широке коло вчених, які займаються захистами у різних сферах, а також досліджують та публікують свої досягнення. Одними з провідних вчених є М.В.Шовгенюк та Л.А. Дідух – це науковці з Інституту фізики конденсованих систем НАН України, які розробили спосіб захисту цінних паперів ГКЗ, основна задача якого це кодоване зображення (друк з одного боку), ключ друкується з іншого боку, а при накладанні отримано декодер з відображенням [16]. Розроблені нові методи цифрової обробки зображень на основі дискретного ДВП Адамара для сучасних технологій захисту цінних паперів та документів (М.В.Шовгенюк, М.П.Козловський, Т.Є.Крохмальський, Т.В.Фітьо, Л.А.Дідух) [137-139]. На основі використання

ортогональних матриць Адамара розроблено методи та алгоритми кодування зображень, запропоновано принципово новий тип ГЕ захисту цінних паперів - ЕЦП, що складається із кодованого зображення та його ключа, які виготовляються за допомогою спеціалізованої програми “ГрафіКод 4”.

Дурняк Б. В. та Пашкевич В.З. розробили інформаційну технологію формування графічних засобів захисту документів, де запропоновали метод формального опису графічних засобів захисту, який дозволяє визначати базові параметри, які характеризують стійкість захисту документів, розробили математичну модель в межах якої можна було б досліджувати графічні засоби захисту, оперативно змінювати їх рівень захисту та забезпечити просту і ефективну ідентифікацію документів в системі документообігу.[37, 38, 100 - 102].

У своїй праці Коншин А.А. «Захист поліграфічної продукції від підробки» [62] піднімає основні питання захисту, а саме те що захист продукції повинен забезпечити не 100% гарантію від принципової можливості будь якої фальсифікації, а нерентабельність правдоподібної підробки. У своїй роботі Коншин А.А. виділяє 5 рівнів контролю достовірності:

1. Візуальний і сенсорний контроль, який здійснюється користувачем чи експертом візуально без використання апаратних засобів.
2. Низькотехнологічний приладовий контроль передбачає використання найпростіших загальнодоступних приладів контролю.
3. Високотехнологічний приладовий контроль потребує спеціальне устаткування та спеціаліста в даній області.
4. Професійний технологічний контроль – це контроль, який повинен бути забезпечений приладами для визначення оригінальності та повинен відповідати професійній підготовці експерта.
5. Лабораторний контроль здійснюється високотехнологічними експертними програмами та пристроями у поєднанні з компетентністю експерта.

По роботі Коншина А.А. можна зробити висновок, що використавши не правильний вид захисту чи не забезпечивши документ сукупністю декількох захистів, можна нанести значиних фінансових збитків державі. А також вартує зауважити, що виготовлення видів захисту мають бути максимально економічно невигідними для фальсифікації і повинні проходити на різних рівнях контролю.

Сучасні інформаційні технології, які формують захищені документи, розвиваються швидкими темпами. Є потреба створювати нові види ЗДД, оскільки засоби та методи фальсифікації стають все поширенішими. Сьогодні фальсифіковані документи створюються новими більш технологічними методами, які максимально близькі до методів виготовлення оригіналу. З кожним роком технічні характеристики копіювальних пристроїв стають більш досконалими, тому потрібно розробляти нові методи ЗДД. Одним з ефективних, економічних та надійних способів захисту є ГСЗ документів.

Проаналізувавши ОІД друкованого документа щодо видів захисту досліджено, що захищений документ створюється [120, 122, 124]:

1. На етапі додрукарської підготовки (гільйошні елементи, гравюри, мікротекст, латентні зображення, мікроплекс, мультиплекс, ГКЗ, анімація);
2. На основі особливостей паперу: використанні нових технологій створення паперу; водяні знаки; захисні кольорові волокна; металізовані смужки; планшетки; флюоресцентні частинки і т.д.
3. На основі особливих фарб (фарби “овіай”, флюоресцентні фарби);
4. На основі використанні особливих технології друку (високий друк, глибокий друк, ірисовий друк, орловський друк та ін.);
5. На етапі післядрукарських процесів (ламінуванняб перфорація, введення мікрочіпів, біометричні елементи).

Група графічних захистів ґрунтується на тонких графічних елементах: сітки, розетки, віньєтки, приховані елементи та мікрографіки. Труднощі

відтворення пов’язані зі складною геометричною структурою і мінімально можливою товщиною ліній елементів тонкої графіки. Навіть для найдосконаліших цифрових технологій достовірна підробка тонкої графіки чи мікрографіки залишається недоступною [82 - 85].

1.2. Аналіз математичних моделей і методів формування та контролю зображень, що містять приховану інформацію

На сьогоднішній день існує багато різноманітних математичних апаратів та методів, котрі застосовуються науковцями для ідентифікації документів [121, 125]. Наступним крок - це аналіз моделей, котрі найактивніше вдосконалюються сучасними дослідниками.

1.2.1. Формування зображень

Сучасний підхід до формування латентних зображень передбачає вбудовування прихованих зображень в певні області зображень, зміна яких може призвести до значного візуального спотворення вихідного зображення [132, 133].

При впровадженні прихованого зображення слід враховувати особливості сприйняття кожної з цих характеристик окремо, а також їхнє поєднання щоб уникнути передчасного виявлення прихованого зображення людським оком і великих видимих деформацій вихідного зображення. Виділяють наступні властивості [40-41]:

1. Великі зміни яскравості областей, що володіють малою і середньою яскравістю, призводять до помітних спотворень зображення [34].
2. Об'єкти червоного кольору є найбільш помітними в порівнянні з об'єктами інших кольорів. Об'єкти синього кольору - найменш помітні.
3. Частотна чутливість горизонтальних і вертикальних елементів вище, ніж діагональних.

4. Періодична структура, що складається з чорних штрихів і прогалин однакової ширини нерозрізнена при візуальному полі зору між центрами двох штрихів менш 1'30" [35]. Таким чином, мінімальна відстань D_{min}, з якого періодична структура стає помітною визначається за формулою:

$$D_{min} = \frac{T}{2} tg0.0125, \tag{1.1}$$

де T - відстань між штрихами.

При перегляді зображення з відстані 40 см і більше, що є нормальною відстанню перегляду зображень, відстань між штрихами періодичної структури, для забезпечення нерозрізненості, має бути не більше 0.175мм.

У поліграфії для періодичних растрових структур використовується поняття лініатури растру, яка дорівнює $1/T$, що вимірюється в лініях на дюйм (lpi) [136]. Таким чином, для забезпечення нерозрізненості поліграфічного зображення з відстані 40см, зображення повинно бути растроване з лініатурой не менше 150 lpi.

Зображення притягують більше уваги, ніж інші об'єкти. На сьогоднішній день не існує точного математичного опису системи людського зору, тому об'єктивна оцінка якості латентного зображення, з урахуванням всіх особливостей сприйняття, також неможлива [42].

Для визначення спотворень зображення в порівнянні з вихідним використовуються наступні підходи [86-87]:

1. візуальна оцінка латентного зображення і його зорове зіставлення з оригіналом та копією. Тільки такий підхід, незважаючи на його суб'єктивність, дозволяє враховувати всі основні відмінностей в зображеннях [140, 142].
2. Обчислення міри СКО (1.2) або її модифікації - ПОСШ (1.3) для півтонового латентного зображення або для кожної з колірних компонент зображення:

$$\text{СКО} = \frac{1}{N}\sum_{i=1}^{N}(x_i - x_i')^2, \tag{1.2}$$

де N - число пікселів в зображенні, x_i, $x_i^{'}$ - значення пікселів вихідного і латентного зображення.

$$\text{ПОСШ} = 10log_2\frac{N255^2}{\sum_{i=1}^{N}(x_i - x_i')^2}, \quad (1.3)$$

Практично всі вивчені методи формування латентних зображень, за винятком способу [36], припускають впровадження бінарного прихованого зображення $S(x, y)\ \varepsilon\ \{0,1\}$ в півтонове вихідне зображення або в один з каналів кольорового зображення. Як відомо, людське око має найбільш низьке сприйняття синього кольору. З огляду на цю особливість, а також те, що з математичної точки зору, повнокольорове зображення в системі RGB являє собою сукупність з трьох матриць однакового розміру, з однаковими діапазонами значень $\{0,1, ..., 255\}$, вбудовування зазвичай проводиться в синій канал.

1.2.2. Просторові методи формування цифрових зображень, які містять приховану інформацію

Формування та виявлення зображень, що містять приховану інформацію виробляється цифровими пристроями, а передача здійснюється виключно по цифрових каналах зв'язку.

З огляду на те, що передача даного класу зображень відбувається виключно по цифрових каналах зв'язку, рівень їх надійності визначається стійкістю до руйнівних процесів такої передачі, а також неможливістю виділення вихідного і прихованого зображення в первісному вигляді. В якості основних прикладів деструктивних впливів на цифрове зображення можна назвати стиснення, масштабування, поворот.

На сьогоднішній день відомо дуже багато алгоритмів для вбудовування даних у зображення, проте лише обмежений набір методів дозволяє використовувати в якості впроваджуваної інформації інше зображення.

Просторові методи впроваджують приховане зображення за рахунок перетворення яскравості вихідного зображення $l(x, y)\ \epsilon\ \{1, ..., L\}$ або колірних

складових червоного $r(x, y) \in \{0, ..., 255\}$, зеленого $g(x, y) \in \{0, ..., 255\}$, і синього $b(x, y) \in \{0, ..., 255\}$.

Метод найменшого біту [46]. Даний метод не відноситься до числа надійних, проте є показовим для просторових методів і застосовується в ряді інших методів. Кожен елемент матриці $I(x, y)$ представляє напівтонове зображення, яке можна представити у вигляді 8-бітного значення 0bXXXXXXXX. У такому вигляді матрицю можна розділити на 8 бітових площин, кожна з яких буде відповідати одному з розрядів двійкових значень:

$$I(x,y) = b_1(x,y) + b_2(x,y) * 2 + \dots + b_k(x,y) * 2^{k-1}, \quad (1.4)$$

де $b_k(x,y) = \{0,1\}, k = 8$.

Виявлення прихованого зображення, сформованого за допомогою даного методу, зводиться до розкладання латентного зображення на бітові площини і їх відсікання з 2 по 7. Для впровадження прихованого зображення можуть бути використані також інші бітові площини, проте заміна бітових площин, відповідних більш високими розрядами, призводить до великих спотворень латентного зображення.

Метод квантування зображення [45]. Даний метод заснований на міжпіксельній залежності. Розмірність впроваджуваного зображення, на увазі специфіки методу, менше вихідного $I(x, y)$ на один піксель по горизонталі або вертикалі, тобто $S(x-1, y)$ або $S(x, y-1)$відповідно. Алгоритм формування будується таким чином:

1. Формується матриця з різниць між сусідніми пікселями, наприклад, по горизонталі:

$$\varepsilon(k,m) = I(x,y) - I(x+1,y) \quad (1.5)$$

2. Формується ключ $B(\varepsilon,b)$, що представляє матрицю, з відповідним для кожного з можливих значень різниць ε матриці $\varepsilon (k,m) \in \{-255, ..., 255\}$ випадкового значення $b \in \{0,1\}$.
3. Генерується латентне зображення L(x,y) шляхом поелементного зіставлення матриці різниць ε (k,m) та ключа B(ε,b) і впроваджуваного

зображення S(x-1, y). Якщо значення b, відповідного елементу ε (k,m), дорівнює значенню елемента S(x-1, y), то значення відповідного елемента L(x,y) заповнюється з вихідного. Інакше підбирається найближче значення ε, якому відповідає значення b дорівнює значенню елемента S(x-1, y) і значення елемента L(x,y) заповнюється з I(x, y) зміненого таким чином, щоб виконувалася умова I(x, y)- I(x+1, y)= ε.

Виявлення латентного зображення *L(x,y)* такого типу здійснюється шляхом зіставлення ключа *B(ε,b)* з матрицею різниць латентного зображення $\varepsilon_{L(x,y)}$.

Метод Дармстедтера [43]. Істотним недоліком даного методу при створенні латентних зображень є обмеження у виборі прихованого зображення, яке повинно бути, як мінімум, в 8 разів менше вихідного.

Алгоритм формування латентного зображення методом Дармстедтера:

1. Початкове зображення розбивається на блоки 8 * 8 пікселів, в кожному з яких формуються дві групи пікселів з приблизно однорідною яскравістю l_1 *і* l_2. При цьому середня яскравість першої групи є меншою ніж у другій $l_1 < l_2$.
2. Кожна з груп пікселів ділиться на дві категорії, згідно ключа *B(8,8)*, представленого матрицею з нулів і одиниць, де 0 позначає приналежність до першої категорії (A), 1 - до другої (B). Таким чином, блок розбивається на 4 групи, де $l_{1A} < l_{2A}$, $l_{1B} < l_{2B}$.
3. Для впровадження пікселя прихованого зображення *S(x-1, y)є{0,1}* кожен блок вихідного зображення модифікується таким чином, щоб дотримувалися така умова:

$$S(x,y) = \begin{cases} 1, \begin{cases} l'_{1A} > l'_{2A}, \\ l'_{1B} > l'_{2B}, \end{cases} \\ 0, \begin{cases} l'_{1A} < l'_{2A}, \\ l'_{1B} < l'_{2B}. \end{cases} \end{cases} \quad (1.6)$$

При цьому яскравість кожної категорії пікселів для забезпечення одномірності повинна змінюватися однаково. Алгоритм виявлення прихованого зображення вимагає наявності ключа використаного при впровадженні, який

обернений алгоритму впровадження.

Метод Лангелара [44]. Даний метод застосовується для прихованих зображень як мінімум в 8 разів менше вихідного. Алгоритм впровадження наступний:

1. Початкове зображення розбивається на блоки $I_b(x,y)$ розміром 8×8 пікселів, в кожному з яких формуються дві групи пікселів згідно ключа $B(8,8)$, представленого матрицею з нулів і одиниць, які формуються випадковим чином.
2. Для кожної групи пікселів обчислюються середні значення яскравості l_0 та l_1.
3. Для впровадження пікселя прихованого зображення $S(x,y)$ ϵ $\{0,1\}$ вибирається деякий поріг α і кожен блок вихідного зображення модифікується таким чином, щоб виконувалась умова:

$$S(x,y)=\begin{cases}1, l'_0-l'_1>\alpha,\\ 0, l'_0-l'_1<-\alpha.\end{cases} \quad (1.7)$$

Алгоритм виявлення прихованого зображення вимагає наявності ключа, який використовується при впровадженні. Латентне зображення розбивається на блоки, на підставі ключа блоки діляться на групи.

Метод формування латентного зображення з впровадженням зображення [37].

Латентні зображення, побудовані з використанням даного методу нестійкі до руйнівних процесів, пов'язаних з передачею, проте перевагою даного методу є можливість впровадження повноколірного прихованого зображення. Даний метод працює таким чином:

1. Приховане зображення $S(x,y)$ раструється з використанням декількох растрових структур з отриманням матриці $S_r(x,y)$сумарно з $S(x,y)$ матрицею:

$$S_r(x,y)=k_1\,S(x,y)+k_2R_i\,(x,y), \quad (1.8)$$

де $R_i\,(x,y)$ - набір растрових структур; k_1, k_2- додатні константи.

2. Матриця $S_r(x,y)$ об'єднується з інвертованою копією прихованого зображення $S_{inv}(x,y)$, в результаті чого утворюється матриця $S_{pre}(x,y)$:(

$$S_{pre}(x,y)=k_1\,S_{inv}(x,y)+k_2S_r\,(x,y), \quad (1.9)$$

3. Матриця $S_{pre}(x,y)$ перетворюється у матрицю $S_{adj}(x,y)$. через використання коефіцієнта α:

$$S_{adj}(x,y) = \alpha\, S_{pre}(x,y) \tag{1.10}$$

4. Формується латентне зображення L(x,y) шляхом об'єднання основного зображення I(x, y) і зображення зі зміненим контрастом $S_{adj}(x,y)$:

$$L(x,y)=k_1\, I(x,y)+k_2\, S_{adj}\,(x,y), \tag{1.11}$$

Математична модель формування латентного зображення даними методом представлена наступною системою рівнянь:

$$\begin{cases} S_r(x,y) = k_1 S(x,y) + k_2 R_i(x,y), \\ S_{pre}(x,y) = k_1 S_{inv}(x,y) + k_2 S_r(x,y), \\ S_{adj}(x,y) = \alpha S_{pre}(x,y), \\ L(x,y) = k_1 I(x,y) + k_2 S_{adj}(x,y), \end{cases} \tag{1.12}$$

1.2.3. Частотні методи формування зображень, що містять приховану інформацію

Метод Жао [45]. Даний метод застосовується тільки для прихованих зображень як мінімум в 8 разів менших вихідного. Алгоритм формування латентного зображення з використанням даного методу передбачає наступне:

1. Початкове зображення розбивається на блоки $I_b(x,y)$ розміром 8×8 пікселів, після чого кожен блок піддається (ДКП) з отриманням матриці коефіцієнтів $D_b\,(u,v)$.
2. Із кожної матриці випадковим чином $D_b\ (u,v)$ вибираються два коефіцієнти $D_b\,(u_1,v_1)$ і $D_b\,(u_2,v_2)$ з середніми частотами. Із координат цих пар коефіцієнтів будується ключ B.
3. Для впровадження пікселя прихованого зображення $S(x,y)$ ε {0,1} вибирається деякий поріг α і кожна матриця $D_b(u,v)$ модифікується таким чином, щоб виконалась умова:

$$S(x,y) = \begin{cases} 1, |D_b(u_1,v_1)| - |D_b(u_2,v_2)| > \alpha, \\ 0, |D_b(u_1,v_1)| - |D_b(u_2,v_2)| < -\alpha. \end{cases} \tag{1.13}$$

4. Виконується зворотня декомпозиція кожної матриці $D_b(u,v)$ в результаті

чого утворюється латентне зображення. Алгоритм виявлення прихованого зображення вимагає наявність ключа B, який був сформований при впровадженні. Латентне зображення розбивається на блоки, проводиться ДКП кожного блоку, на підставі ключа вибираються коефіцієнти $D_b'(u_1,v_1)$ і $D_b'(u_2,v_2)$. За різницею між цими коефіцієнтами визначається значення біта прихованого зображення.

Метод Хсу [51]. Даний метод має реалізацію тільки для прихованих зображень, які є щонайменше в два рази менші вихідного. Узагальнений алгоритм формування латентного зображення з використанням даного методу передбачає наступне:

1. Приховане зображення $S(x,y)$ піддається вибірковій перестановці, в результаті чого виходить матриця $R_S(x,y)$.
2. Початкове зображення $I(x,y)$ розбивається на блоки $I_b(x,y)$ розміром 8×8, матриця $R_S(x,y)$ розбивається на блоки $R_{Sb}(x,y)$ розміром 4×4.
3. Матриці блоків $I_b(x,y)$ перетворюються та отримуємо матриці $D_b(x,y)$, з матриць отриманих коефіцієнтів вивантажуються 16, які належать середнім частотам та формують нові блоки $D_{mb}(x,y)$ розмірністю 4×4.
4. Обчислюються матриці $P_b(x,y)$ є {0,1}, які є різницею сусідніх блоків $D_{mb}(x,y)$ і $D_{mb+1}(x,y)$. У зазначених матрицях значенням 1 будуть відповідати позитивні різниці, а 0 - негативні і рівні нулю.
5. Створюються модифіковані матриці полярностей $P_{b'}(x,y)$ шляхом складання по модулю 2 матриць $P_b(x,y)$ і $R_{Sb}(x,y)$.
6. Кожна матриця $D_{mb}(x,y)$ модифікується таким чином, щоб дотримувалося рівність $P_{b'}(x,y) = P_b(x,y)$. На виході отримаємо матрицю $D_{mb'}(x,y)$.
7. Середньочастотні коефіцієнти кожної з матриць $D_b(x,y)$ замінюються на відповідні $D_{mb'}(x,y)$.

Латентні зображення формуються як зворотні матриці $D_{mb'}(x,y)$ та їх об'єднання.

Для виявлення прихованого зображення необхідна наявність вихідного

зображення. Алгоритм виявлення прихованого зображення полягає в ідентифікації вихідного і отриманого зображеннь і знаходженні різниці між ними. Подібно до процесу формування на основі полярності різниць середніх частот визначається біт прихованої інформації. На підставі вивантажених бітів будується відповідна матриця прихованого зображення.

Огляд існуючих методів показав, що вони не дозволяють впроваджувати зображення, які приховуються, за винятком методу, представленого в роботі [37, 141, 164], однак, в сформованих цим методом латентних зображеннях проявляється додаткова структура, тому необхідна розробка таких моделей формування латентних зображень, які дозволяли б отримати більш якісні зображення.

1.3 Методи впровадження прихованих зображень

Особливістю методів впровадження прихованих зображень в ДД є вимога стійкості таких зображень до ЦАП і АЦП [14]. Виявлення здійснюється за допомогою аналогового пристрою або спеціалізованого ПЗ [50].

1.3.1 Методи засновані на використанні різно-орієнтованих растрових структурах

Для впровадження прихованого зображення за допомогою методів, заснованих на використанні різно-орієнтованих растрових структур [51], вибираються дві растрові структури зі схожими або однаковими частотними характеристиками та з різним орієнтуванням. Зазвичай для формування даного типу зображень вибираються лінійні растри. Впровадження прихованого зображення відбувається в однорідні області вихідного зображення. Значні біти зображення раструються за допомогою однієї растрової структури, а решта застосовуються – іншою структурою. Приклад такого зображення представлений на рисунку 1.1.

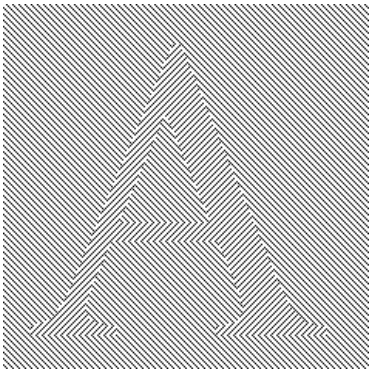


Рисунок 1.1. Латентне зображення з різно-орієнтованими структурами

Методи і технології формування латентних зображень даного типу є у доробку фірм багатьох країн, що займаються випуском захищеної поліграфічної продукції: Multicolor Latent Image, OeBS, LIFT - De La Rue та інші [53, 147-152].

1.3.2. Методи, засновані на використанні різних лініатур растра

Для побудови латентного зображення, за допомогою методів, заснованих на використанні різних лініатур растра [54], вибираються дві різні лініатури зі значеннями, що перевищують поріг розрізнення (> 150 lpi).

Впровадження прихованого зображення відбувається в однорідні області вихідного зображення. Значні біти прихованого зображення раструются з одною лініатурою, а інша область впровадження - іншою. Приклади таких зображень представлені на рисунку 1.2.

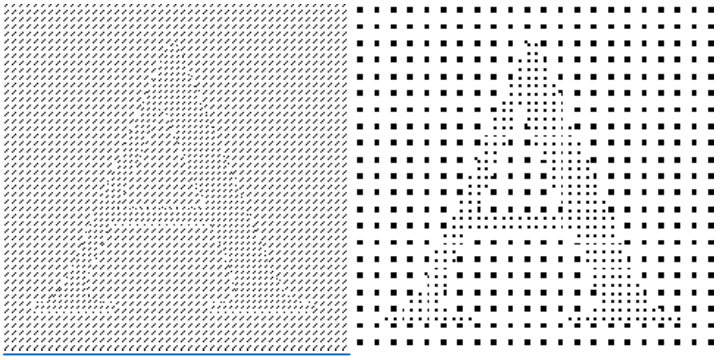


Рисунок 1.2 - Латентні зображення, з растрами різних линиатур

Виявлення прихованого зображення відбувається за рахунок появи частотного розрізнення періодичних структур. Приховане зображення також може проявитися після сканування або копіювання латентного зображення внаслідок анізотропії скануючих і друкуючих пристроїв. При копіюванні латентного зображення, побудованого растуванням з лініатурами 170 і 190 lpi, при максимальній РЗ принтера і сканера в 180 lpi, можна отримати ідентичну копію тільки частини зображення, растрованого з лініатурою 170 lpi, інша частина зображення змінить свій контраст [55-57].

1.3.3. Методи засновані фазовому зсуві растрових структур

За допомогою методів, заснованих на фазовому зсуві растрових структур [58], впровадження прихованого зображення відбувається в однорідні області вихідного зображення. Початкове зображення раструється, потім для вбудовування потрібного біта прихованого зображення відбувається зміна растрової точки в деякому напрямку із кроком меншим періоду растрової структури. Найпростіший приклад такого зображення представлений на рисунку 1.3.

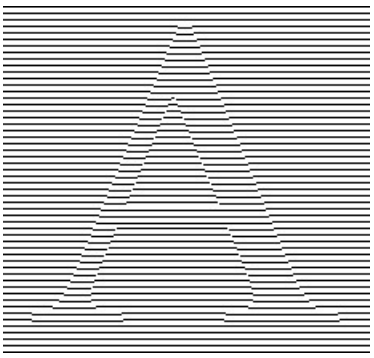


Рисунок 1.3. Латентне зображення, із зсувом фази растрових структур

Виявлення прихованого зображення відбувається при накладенні фільтра з періодом при растуванні вихідного зображення. При цьому відбувається посилення контрасту в ділянці прихованого зображення (рисунок 1.4).

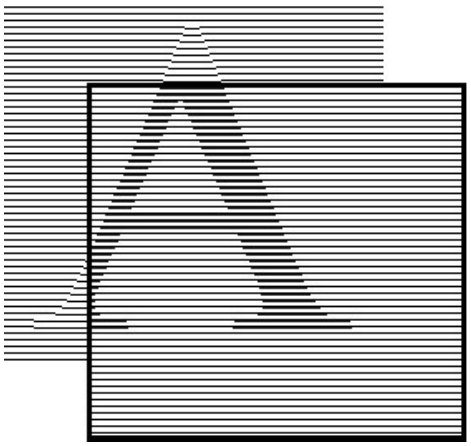


Рисунок 1.4. Виявленя прихованого зображення

Приховане зображення також може проявитися після сканування або копіювання латентного зображення внаслідок анізотропії скануючих і друкуючих пристроїв.

1.3.4. Фізико-хімічні методи впровадження і контролю прихованої інформації

Формування фізико-хімічних латентних зображень відбувається безпосередньо на поверхні, що захищається при нормальних умовах навколишнього середовища, які проявляються при певному фізичному впливі або наносяться спеціальними способами, що забезпечують видимість прихованого зображення під певним кутом. Виявлення таких зображень здійснюється за допомогою спеціальних пристроїв при зміні умов спостереження.

Поляризаційні плівки з прихованим зображенням – це група способів виявлення фальсифікації [60, 61, 161, 162], яка передбачає формування прихованих зображень накладенням виготовленої спеціальним чином прозорої поляризаційної плівки на вихідне латентне зображення. Поляризаційна плівка створюється з прозорих полімерів з нанесенням термічних, хімічних або радіаційних способів, яка додається до зображення, що візуалізується при перегляді через поляризатор.

Поляризатор являє собою пристрій з джерелом поляризационного світла і поляризаційним фільтром. При накладенні поляризатора на латентне зображення через світлофільтр стає видимим приховане зображення [64 - 65].

Поляризаційні латентні зображення мають високу стійкість до підробок із досить високим рівнем захисту від копіювання. Однак висока вартість виготовлення і вимога до наявності спеціального поляризатора для контролю даного виду латентних зображень є суттєвими факторами, що визначають їх не високе поширення.

Водяні знаки. Латентне зображення із впровадженим водяним знаком в ДД для окремих ділянок якої характерні різні значення щільності [63]. Нанесення водяного знака здійснюється за рахунок зменшення або збільшення товщини паперу, на якій нанесено вихідне зображення, таким чином, щоб ділянки зі зміненою товщиною паперу представляли образ прихованого зображення. Контроль зображень, що містять водяний знак, здійснюється просвічуванням носія, в результаті чого приховане зображення стає видимим. Зображення у вигляді водяного знака можуть бути однотонові, двотонові, багатотонові [143 - 145]. Однотонові приховані зображення утворюються за рахунок або зменшення, або збільшення товщини паперу. Двотонові приховані зображення припускають, як збільшення, так і зменшення товщини паперу. Впровадження багатотонових прихованих зображень здійснюється з використанням різних ступенів потовщення паперу. Комбіновані латентні зображення містять кілька тонових видів прихованих зображень [71].

Документи ЗПП водяними знаками мають досить високий рівень захисту і отримали широке поширення за рахунок простоти контролю. Однак технологічний процес створення водяних знаків є занадто складним і вимагає спеціального дорогого обладнання. А також водяні знаки мають технічне обмеження у вигляді поверхні нанесення, що робить їх непридатними для вирішення ряду завдань захисту друкованих документів – ЗДД [72].

Голограми. Голограми є особливим класом зображень, що наносяться на фотографічну пластину за допомогою лазера, що відображають собою образ тривимірного об'єкту зі збереженням можливості зміни перспективи при зміні точки спостереження [93]. Зображення на голограму наноситься у вигляді ряду ліній, що представляють тонкі поглиблення на поверхні, при цьому відстань між ними має бути порівнянна з довжиною світлової хвилі. Технологія передбачає, що на одному міліметрі поміщається до декількох десятків таких ліній [98].

Собівартість виробництва голографічних зображень, з причини високої вартості обладнання є досить висока і може бути виправдана тільки при виготовленні невеликого формату зображень. При цьому, на думку експертів, найближчим часом, широкого поширення даного виду латентних зображень не передбачається [69].

Захисні фарби. На сьогоднішній день захисні фарби знайшли широке застосування як засіб технологічного ЗДП. Завдяки складному вмісту, зображення, нанесені цією фарбою, стають видимими або змінюють свій колір залежно від умов освітлення і спостереження. У звичайних умовах ці фарби є безбарвними. Після нанесення прихованого зображення на будь-яку поверхню, включаючи друковану продукцію, за допомогою захисних фарб, візуальний образ, який створюється, визнається латентним зображенням [88].

1.4. Аналіз програмного та апаратного забезпечення для впровадження латентних зображень в документи та їх контроль

Наявне ПЗ призначене для масового споживача вельми обмежене і представлено програмними продуктами CERBER компанії SecureSoft [94, 123], що створює латентні зображення з використанням гільоширних візерунків з фазовим зрушенням прихованого зображення, і BBS Designer компанії GuardSoft [95], що створює латентні зображення за власною технологією Ghost

on Duty. Для виявлення зображень, сформованих за технологією Ghost on Duty, компанія GuardSoft пропонує спеціальні оптичні ключі.

Пристрої формування представлені ЕДП, що підтримують технології Glossmark, SafePaper, TrustMark і DataGlyphs [165 - 172]. Дані технології передбачають спеціальні методи растрування, реалізовані безпосередньо апаратною частиною. Для виявлення прихованих зображень, сформованих за технологіями SafePaper, TrustMark і DataGlyphs потрібен спеціальний оптичний ключ. Для виявлення зображень Glossmark досить змінити кут огляду надрукованого латентного зображення [85].

Виявлення прихованого зображення відбувається при повороті латентного зображення, за рахунок появи частотних відмінностей проекцій растрових структур. Приховане зображення також може проявитися після сканування латентного зображення внаслідок анізотропії РЗ скануючих пристроїв. Програмні засоби для виявлення латентних зображень, такі як Regula Video Scope [66], дозволяють тільки візуалізувати латентні зображення.

При впровадженні прихованих зображень в документи враховуються не тільки властивості людського зору, але і спеціальне устаткування – сканери та принтери, які здійснюють передачу латентних зображень в документи [67, 68]. У випадках, коли факт наявності прихованої інформації в друкованій продукції не визначається візуально при зміні кута огляду латентного зображення, оперативний контроль такої продукції неможливий і потрібен індивідуальний спеціальний алгоритм для виявлення кожного типу латентного зображення. Розробка методів контролю з меншою обчислювальною складністю контролю прихованої інформації дозволить забезпечити можливість автоматизації процесу контролю латентних зображень.

1.5. Обґрунтування вибору напрямку досліджень та постановка наукового завдання

Зі всього вищезазначеного випливає, що для вирішення головного завдання розроблення методів формування та ідентифікації латентних зображень дозволить збільшити надійність контролю, а також скоротити число помилкових спрацьовувань пристроїв контролю, що дозволить вирішити ряд локальних завдань, зокрема:

1. Провести аналіз моделей та методів формування захищених графічних елементів для забезпечення надійності та достовірності документа, а також встановити переваги та недоліки графічних способів.
2. Розробити метод формування латентних зображень для забезпечення достовірності документа.
3. Розробити моделі побудови графічних елементів на основі формування фракталів, які при копіюванні здійснюють часткове чи повне спотворення об’єктів.
4. Вдосконалити метод формування елементів тонкої графіки в інформаційній технології, які завдяки їх побудови із врахуванням умов друку унеможливлять несанкціоновану модифікацію документа.

Висновки до розділу 1

У дисертаційній роботі, для позначення зображень, що містять приховану інформацію у вигляді іншого зображення використовується термін «Латентне зображення». До латентних зображень відносяться зображення, основною властивістю яких є зміна видимості елементів зображення при зміні умов спостереження.

Наведений огляд літературних джерел показав, що існуючі методи впровадження прихованої інформації не враховують всіх особливостей. Тому необхідно розробити такі методи формування латентних зображень, які б найбільш повно враховували властивості, що дозволять забезпечити підвищення візуальної якості латентного зображення.

Дослідження друкованих документів з використанням латентних зображень дозволяє забезпечити їх захист без порушення візуальної композиції зображення, проте існуючі методи формування латентних зображень доступні тільки для кваліфікованих фахівців в даній області.

У випадках, коли факт наявності прихованої інформації в друкованих документах не визначається візуально при зміні кута огляду латентного зображення, оперативний контроль такої продукції неможливий і потрібен індивідуальний спеціальний алгоритм для виявлення кожного типу латентного зображення.

РОЗДІЛ 2 МЕТОДИ І АЛГОРИТМИ ФОРМУВАННЯ ЛАТЕНТНИХ ЗОБРАЖЕНЬ

У другому розділі розроблено методи моделювання латентних зображень і моделі формування латентних зображень з впровадженням їх в документ.

На відміну від відомих методів [21, 36] в дисертаційній роботі пропонується за допомогою розробленої математичної моделі формувати латентне зображення не тільки за рахунок комбінації різних растрових структур, що утворюють основне зображення, області яких визначаються на основі взаємно зворотних позитивної і негативної масок впроваджуваного зображення, але і за рахунок комбінації двох низькочастотних аперіодичних структур.

2.1. Метод моделювання латентного зображення

Існуючі методи формування латентних зображень розділяють на дві групи: просторові і частотні. Суть просторових методів полягає в перетвореннях яскравості вихідного зображення або однієї з його колірних складових. Частотні методи передбачають зміну вихідного зображення таким чином, щоб при частотному розкладанні отриманого латентного зображення приховане зображення виявилося в локалізованій частотній області, як правило, низькочастотній.

Діагональні лінії сприймаються людським оком як низькочастотний сигнал [73]. З огляду на те, що частотна чутливість діагональних структур нижче, ніж у горизонтальних і вертикальних [74], можна припустити, що незначні перетворення в діагональних структурах не приведуть до серйозних візуальних спотворень зображення. Людський зір нерозрізняє періодичні структури, що складаються з штрихів і прогалин однакової ширини, при куті зору між центрами двох штрихів [80, 81], тому впровадження повинно відбувається в структурі з мінімальними товщинами ліній і пробілами між ними.

Побудова математичної моделі латентного зображення здійснюється шляхом комбінації різних структур на основі створення позитивної й негативної маски [78].

Приймемо, що $G(x, y, z)$ − основне зображення, де x, y, z – інтенсивність кольору поточних пікселів в системі RGB, тоді $G_{inv}(x,y,z)$ – приховане зображення з інвертованою маскою. Нехай L – кількість шарів. Процес формування латентного зображення полягає у тому, що створюється приховане зображенння з інвертованою копією $G_{inv}(x,y,z)$ основного зображення $G(x,y,z)$;

$$G\_inv\ (x,y,z)=(2^L- 1)-G(x,y,z).$$

Основне зображення $G(x,y,z)$ формується з видаленням непарних діагональних ліній, утворюючи першу низькочастотну аперіодичну структуру $R_1\ (x_i,y_j,z_k)$:

$$R_1(x_i, y_j, z_k) = F_{R1}(G(x_i, y_j, z_k))|_{i=1,...,N;\ j=1,...,M;\ k=1,2,3},$$

де F_{R1} – функція растрування низькочастотної аперіодичної структури, k - колірна компонента в системі RGB: k=1–червоний, k=2–зелений, k=3– синій; i, j – координати пікселя; N, M – відповідно ширина і висота зображення в пікселях.

Інвертована копія зображення $G_{inv}(x,y, z)$ формується видаленням парних діагональних ліній, утворюючи другу низькочастотну аперіодичну структуру $R_2(x_i,y_j,z_k)$:

$$R_2(x_i, y_j, z_k) = F_{R2}(G_{inv}(x_i, y_j, z_k))|_{i=1,...,N;\ j=1,...,M;\ k=1,2,3.}$$

Створюється маска $H(x,y,z)$ шляхом об'єднання аперіодичних структур $R_1(x, y, z)$ й $R_2(x, y,-z)$:

$$H(x,y,z)= R_1\ (x,y,z) + R_2\ (x,y,z)$$

Латентне зображення $L(x,y,z)$ формується dбудовуванням основного зображення $G(x,y,z)$ та інвертованої копії – додаткового шару і маски $H(x,y,z)$.

Початкове зображення раструється, потім відбувається зміщення растрової точки в певному напрямку з кроком меншим періоду растрової структури. Метод створення латентних зображень формується шляхом утворення двох прихованих зображень, які накладаються. Визначають елементи рельєфу для

кожного прихованого зображення, що передається відповідними лінійними структурами для утворення основного і допоміжного шарів. Елементи вбудовуються тільки в ті місця, де лінійні структури рельєфу першого і другого шару накладаються. Шар і приховане зображення буде відтворюватися при копіюванні в якості постійної сірої області.

Для впровадження прихованого зображення *G(x,y,z)* на основне зоображення *I(x,y,z)* пропонується об'єднати це зображення зі своєю растровою копією $I_R(x,y,z)$, на яку накладено маску прихованого зображення *G(x,y,z)*.

Для впровадження прихованого зображення *G(x,y,z)* в низькочастотну складову вихідного зображення *I(x,y,z)* здійснимо підготовлення прихованого зображення, в низькочастотний сигнал, що представляє собою впроваджуване зображення *H(x,y,z)*. Для цього об'єднаємо два зображення: приховане зображення *G(x,y,z)* і його інвертовану копію $G_{inv}(x,y,z)$, чергуючи діагональні лінії матриці яскравості зображень *G(x,y,z)* і $G_{inv}(x,y,z)$. Для реалізації такого об'єднання необхідно растувати приховане зображення, видаливши непарні діагональні лінії в *G(x,y,z)* і інвертовану копію, видаливши парні діагональні лінії в $G_{inv}(x,y,z)$. Розроблений метод моделювання процесу формування латентного зображення, з впровадженням прихованого зображення проілюстрований на рисунку 2.1.

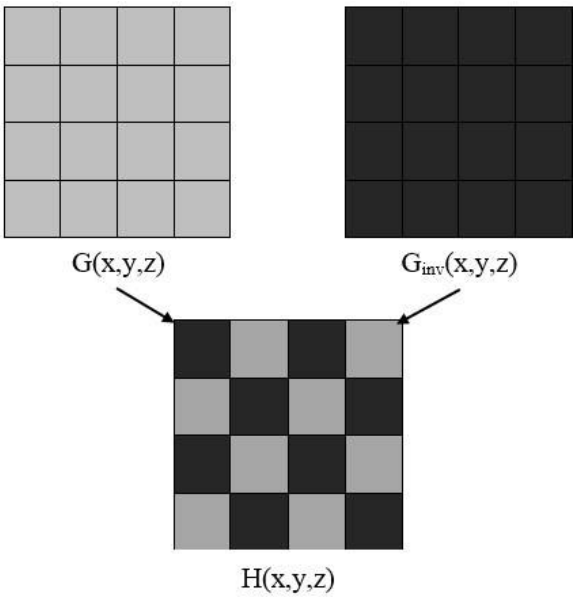


Рисунок 2.1 - Схема вбудованого латентного зображення

Алгоритм формування прихованого зображення:

Початкове зображення *I(x,y,z)* раструється, з видаленням непарних діагональних ліній, утворюючи першу низкочастотну аперіодичну структуру $R_1(x,y,z)$:

$$\begin{cases} R_1(x_i, y_j, z_k) = F_{R1}\left(I(x_i, y_j, z_k)\right), \\ R_1(x_{i+1}, y_{j+1}, z_k) = F_{R1}\left(I(x_{i+1}, y_{j+1}, z_k)\right), \end{cases} \Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \quad (2.1)$$

Копія вихідного зображення *I(x,y,z)* раструється з видаленням парних діагональних ліній, утворюючи другу низкочастотную аперіодичну структуру $R_2(x, y, z)$:

$$\begin{cases} R_2(x_i, y_{j+1}, z_k) = F_{R2}\left(I(x_i, y_{j+1}, z_k)\right), \\ R_2(x_{i+1}, y_j, z_k) = F_{R2}\left(I(x_{i+1}, y_j, z_k)\right), \end{cases} \Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \quad (2.2)$$

З першої аперіодичної структури $R_1(x,y,z)$ віднімається маска прихованого зображення *G(x,y,z)* в область застосування, з утворенням растрової структури прихованого зображення $R_{Gm}(x,y,z)$:

$$R_{Gm}(x,y,z) = G(x,y,z) * R_1(x,y,z) \quad (2.3)$$

Створюється впроваджуване зображення *H(x,y,z)* шляхом об'єднання растрової структури прихованого зображення $R_{Gm}(x,y,z)$ і аперіодичрої структури $R_2(x, y, z)$:

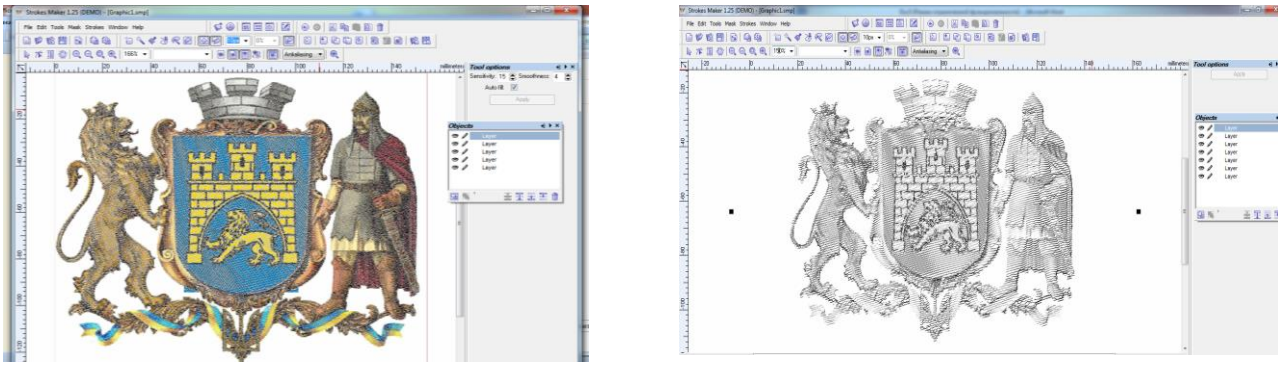
$$H(x, y, z) = R_{Gm}(x, y, z) + R_2(x, y, z) \quad (2.4)$$

Латентне зображення формується шляхом вбудовування вихідного зображення *I(x, y, z)* і впроваджуваного *H(x,y,z)* з коефіцієнтами *a i b* відповідно:

$$L(x, y, z) = aI(x, y, z) + \mathrm{b}H(x, y, z), \quad (2.5)$$

де *G(x,y,z)* - приховане зображення; *I(x,y,z)* - вихідне зображення; $R_1(x,y,z)$ - растроване вихідне зображення з видаленням парних діагональних ліній; $R_2(x,y,z)$ - растроване вихідне зображення з видаленням непарних діагональних ліній; $R_{Gm}(x,y,z)$ - растрова структура $R_1(x,y,z)$ з маскуванням прихованого зображення *G(x,y,z)*; *H(x,y,z)* - впроваджуване зображення; *L(x,y,z)* - латентне зображення.

Незважаючи на візуальну непомітність вихідного і латентного зображень, побудованого комбінованим методом, при великому збільшенні латентного зображення виразно проявляється растрова структура (рисунок 2.2).



а б

Рисунок 2.2 - Зображення: а - вихідне, б – латентне

При побудові моделі формування запропонованим методом моделювання непомітність сусідніх пікселів латентного зображення $H(x,y,z)$ шляхом усереднення яскравості сусідніх пікселів прихованого зображення $G(x,y,z)$ і його інвертованої копії $G_{inv}(x,y,z)$. Для збереження розміру зображення необхідно, щоб розмір растрової точки до і після растрування залишався незмінним. Перед об'єднанням матриць яскравості прихованого зображення $G(x,y,z)$ і його інвертованої копії $G_{inv}(x,y,z)$ виконаємо растрування цих зображень, що дозволяє забезпечити нерозрізненість сусідніх пікселів.

Передбачається, що мінімальним розміром растрової комірки, яка дозволяє забезпечити структурну відмінність є 2×1 або 1×2, об'єднаних в групи розміром 2×2. Інтенсивність одного з двох пікселів при раструванні, прирівнюється до середньої по растровому осередку. Інтенсивність іншого пікселя растрового осередку прирівнюється 0. Схематично процес растрування описаним способом представлено на рисунку 2.3, рівняння растрування представлено формулами 2.6 - 2.7.

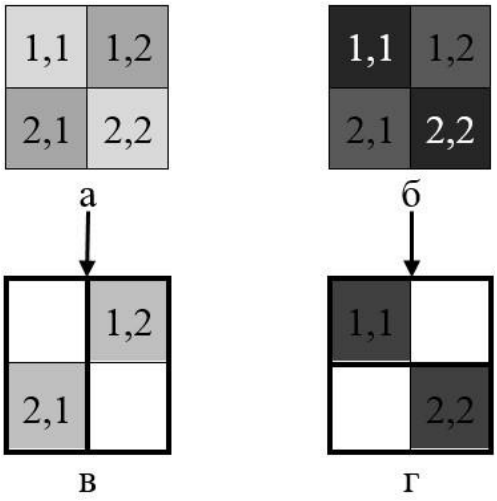


Рисунок 2.3. Групи растрових осередків: а, б - прихованого і інвертованого зображень; в, г - растрованого групою растрових осередків.

$$\begin{cases} R_1(x_i, y_j, z_k) = F_{R1}\left(\frac{1}{2}\left(I(x_i, y_j, z_k) + I(x_{i+1}, y_j, z_k)\right)\right), \\ R_1(x_{i+1}, y_{j+1}, z_k) = F_{R1}\left(\frac{1}{2}\left(I(x_i, y_{j+1}, z_k) + I(x_{i+1}, y_{j+1}, z_k)\right)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \quad (2.6)$$

$$\begin{cases} R_2(x_i, y_{j+1}, z_k) = F_{R2}\left(\frac{1}{2}\left(I(x_i, y_j, z_k) + I(x_i, y_{j+1}, z_k)\right)\right), \\ R_2(x_{i+1}, y_j, z_k) = F_{R2}\left(\frac{1}{2}\left(I(x_{i+1}, y_j, z_k) + I(x_{i+1}, y_{j+1}, z_k)\right)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \quad (2.7)$$

Розроблені методи моделювання латентних зображень дозволяють отримати моделі формування латентних зображень не тільки за рахунок комбінації різних растрових структур, що утворюють основне зображення, області яких визначаються на основі взаємно зворотних позитивної і негативної масок впроваджуваного зображення, як у відомих методах [103 - 106], а й на основі комбінації двох низькочастотних аперіодичних структур.

2.2. Математичні моделі формування латентних зображень

На основі запропонованого методу моделювання, побудована математична модель формування латентного зображення з впровадженням його у вхідне зображення.

У відому математичну модель додано рівняння растрування з видаленням діагональних ліній (2.2 - 2.3), що дозволило виключити з відомої моделі яскравості перетворення введені для приховання факту впровадження. Це призводять до суттєвих спотворень зображення.

Для отримання інвертованої копії прихованого зображення $G_{inv}(x,y,z)$ інтенсивність кожного пікселя зображення в координатах x,y,z обчислюється як різниця між максимальним діапазоном інтенсивностей зображення і відповідного пікселя прихованого зображення:

$$G_{inv}(x,y,z) = (2^L - 1) - G(x,y,z) \qquad (2.8)$$

Для отримання першої аперіодичної структури $R_1(x, y, z)$ прихованих даних з зображення $I(x,y,z)$ виділяють парні діагональні лінії, значення інтенсивності кожного пікселя непарних діагональних ліній, яке дорівнює середньому значенню інтенсивності відповідного пікселя прихованого зображення і сусіднього пікселя в тому ж рядку:

$$\begin{cases} R_1(x_i, y_j, z_k) = \frac{1}{2}\left(I(x_i, y_j, z_k) + I(x_{i+1}, y_j, z_k)\right), \\ R_1(x_{i+1}, y_{j+1}, z_k) = \frac{1}{2}\left(I(x_i, y_{j+1}, z_k) + I(x_{i+1}, y_{j+1}, z_k)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \qquad (2.9)$$

Для отримання другої аперіодичної структури $R_2(x,y,z)$ прихованих даних з копії вихідного зображення виділяють непарні діагональні лінії, значення інтенсивності кожного пікселя парних діагональних ліній, яке дорівнює середньому значенню інтенсивності відповідного пікселя копії вихідного зображення і сусіднього пікселя в тому ж стовпці:

$$\begin{cases} R_2(x_i, y_{j+1}, z_k) = \frac{1}{2}\left(I(x_i, y_j, z_k) + I(x_i, y_{j+1}, z_k)\right), \\ R_2(x_{i+1}, y_j, z_k) = \frac{1}{2}\left(I(x_{i+1}, y_j, z_k) + I(x_{i+1}, y_{j+1}, z_k)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \qquad (2.10)$$

Для отримання прихованого зображення аперіодичних структур $R_1(x,y,z)$ здійснюється віднімання по масці прихованого зображення $G(x,y,z)$ і отримане зображення об'єднується з другою аперіодичною структурою $R_2(x,y,z)$ шляхом

додавання інтенсивності кожного пікселя зображення в координатах *x, y, z*:

$$H(x,y,z) = G(x,y,z)*R_1(x,y,z) + R_2(x,y,z) \quad (2.11)$$

Для впровадження прихованих даних у вихідне зображення *I(x,y,z)* відбувається об'єднння прихованого зображення *H(x,y,z)* шляхом додавання інтенсивностей кожного пікселя зображень в координатах *x,y,z* з коефіцієнтами 1 і 0.1 відповідно:

$$L(x, y, z) = I(x, y, z)+ 0.1H(x, y, z) \quad (2.12)$$

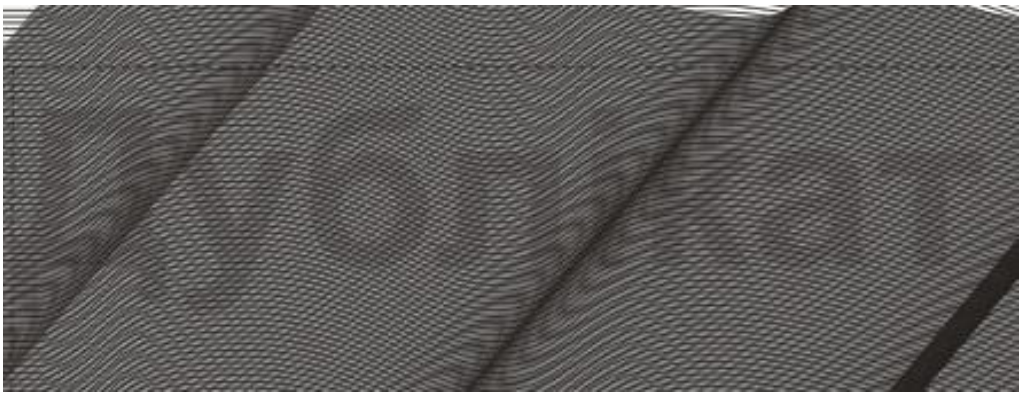
Отримана математична модель представлена системою рівнянь 2.13.

$$\begin{cases} \begin{cases} R_1\left(x_i, y_j, z_k\right) = \frac{1}{2}\left(I\left(x_i, y_j, z_k\right) + I\left(x_{i+1}, y_j, z_k\right)\right), \\ R_1\left(x_{i+1}, y_{j+1}, z_k\right) = \frac{1}{2}\left(I\left(x_i, y_{j+1}, z_k\right) + I\left(x_{i+1}, y_{j+1}, z_k\right)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \\ \begin{cases} R_2\left(x_i, y_{j+1}, z_k\right) = \frac{1}{2}\left(I\left(x_i, y_j, z_k\right) + I\left(x_i, y_{j+1}, z_k\right)\right), \\ R_2\left(x_{i+1}, y_j, z_k\right) = \frac{1}{2}\left(I\left(x_{i+1}, y_j, z_k\right) + I\left(x_{i+1}, y_{j+1}, z_k\right)\right), \end{cases}\Bigg|_{\substack{i=1,3,\ldots,N \\ j=1,3,\ldots,M \\ k=1,2,3}} \\ H(x, y, z) = G(x, y) * R_1(x, y, z) + R_2(x, y, z), \\ L(x, y, z) = I(x, y, z) + 0.1H(x, y, z), \end{cases} \quad (2.13)$$

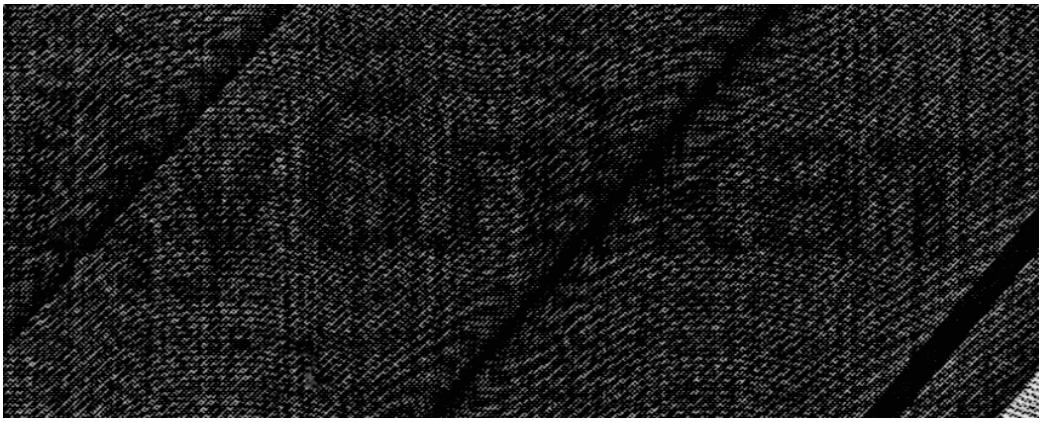
де G(x, y) - приховане зображення; R1(x, y, z) і R2(x, y, z) - підготовлені на основі вихідного зображення низькочастотні аперіодичні структури; H(x, y, z) - підготовлене впроваджуване зображення; L(x, y, z) - латентне зображення; x, y, z - координати колірних компонент в системі RGB; i, j - координати пікселя над яким виробляється перетворення; k - колірна компонента в системі RGB. k = 1-червона, k = 2-зелена,k = 3-синя; N - ширина зображення в пікселях; M - висота зображення в пікселях.

Використання латентних елементів для захисту документів відбувається за рахунок періодичних структур, які формують векторною графікою з заданими параметрами для кожного шару окремо. Для основного шару формують прихований елемент, наприклад слово “Дублікат”. Допоміжний шар формується за допомогою хвиль, які розпадаються при копіюванні за рахунок того, що були здійсненні у 10-60 мкм – це найменше можливе значення штихів лінії. Зверху накладається інший шар періодичної структури, яка формується

за принципом суперпозиції. На рисунку 2.3а показано векторне зображення з ефектом латентності. Це ж зображення було виведене засобами ксерографії та оцифроване (рисунок 2.3б). Навіть візуально спостерігається втрата якості та розмиття ліній сіток. На рисунку 2.3.б прихований напис не читається.



а



б

Рисунок 2.3. а) Приклад векторного зображення з латентністю
б) Скановане зображення на основі створеного векторного

2.3. Застосування розроблених моделей формування латентних зображень

Проведено порівняння візуальної якості латентних зображень, сформованих на основі розроблених моделей, з зображеннями отриманими на основі відомих методів. Для цього були розроблені моделі в системі MATLAB, що дозволяють автоматично формувати латентне зображення методом, запропонованим в роботі [70, 83] і розробленим методом.

Для оцінки результатів було сформовано латентне зображення відомим

методом, що дозволяє впроваджувати приховані зображення в документи [89-91].

Узагальнений алгоритм формування зводиться до наступного: приховане зображення дублюється; проводиться інвертування прихованого зображення; дубльоване приховане зображення раструється заздалегідь підготовленими растровими структурами; інвертоване приховане і растроване зображення об'єднуються; над отриманим прихованим зображенням здійснюють перетворення яскравості; основне і отримане приховане зображення об'єднуються, утворюючи латентне зображення.

До недоліків даного способу відноситься те, що технологічний процес запропонованого способу досить трудомісткий і вимагає спеціального дорогого ПЗ, а саме Adobe Photoshop.

В рамках дисертаційного дослідження розроблена модель на основі Adobe Photoshop [153 - 156], що дозволяє формувати латентне зображення способом, запропонованим в роботі [37] на основі вихідного і прихованого зображень. Передбачуване даними способом растрування здійснюється на основі растрового комірки n * n завантажується в програму у вигляді бінарного зображення, наприклад, як показано на рисунку 2.4.

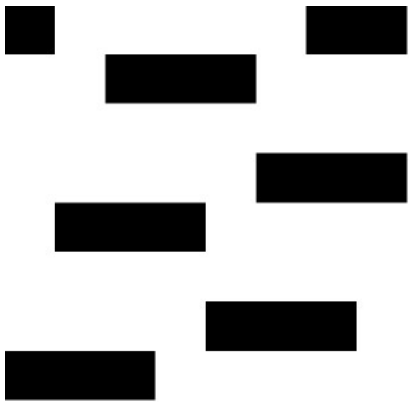


Рисунок 2.4 - Растрова комірка 8 * 8

Покроковий алгоритм створення латентного зображення: завантажується вхідне зображення; наступний крок це приховане зображення дублюється і інвертується; формується основний шар 60 - 75%; для створення растрової структури можна скористатися функцією, що створює матрицю з заданої

кількості копій вихідної матриці, для створення растрової структури сумарно з вихідним зображенням; отримана растрова структура є маскою, по якій проводиться растрування інвертованого прихованого зображення; формується додатковий шар 15 - 20%; отримуємо негатив маски растрової структури і накладаємо її на копію прихованого зображення і об'єднаємо отримане зображення з растрованим інвертованим; створюється ЗК та формується виворотка; для впровадження прихованому зображенні проведемо перетворення яскравості та зміну кольорів; відбувається накладання шарів; для безпосереднього впровадження прихованого зображення скористаємося командою, з коефіцієнтом для прихованого зображення 0.1, що відповідає прозорості 10%, що задається програмою Adobe Photoshop: L = imlincomb (0.1, G, 0.9, I); створюється шаблон; латентне зображення вмонтовується в документ; на завершення програма записує отримане латентне зображення в файл; формовується документ в Post Script файлі.

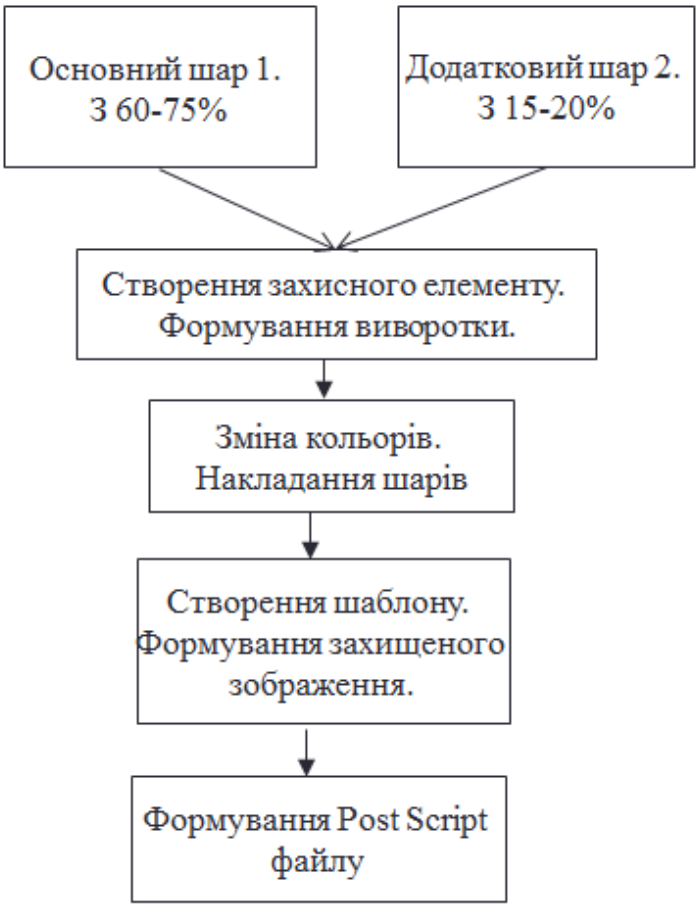


Рисунок 2.5 – Алгоритм побудови латентних зображень

В рамках дисертаційного дослідження розроблені моделі дозволяють формувати латентне зображення запропонованими методами на основі вихідного і прихованого зображень. Метод створення латентних зображень формується шляхом утворення двох прихованих зображень, які накладаються. Визначають елементи рельєфу для кожного прихованого зображення, що передається відповідними лінійними структурами для утворення основного і допоміжного шарів. Елементи вбудовуються тільки в ті місця, де лінійні структури рельєфу першого і другого шару накладаються. Шар і приховане зображення відтворюватимуться під час копіювання сірою ділянкою. Схему формування латентного зображення наведено на рисунку 2.6.

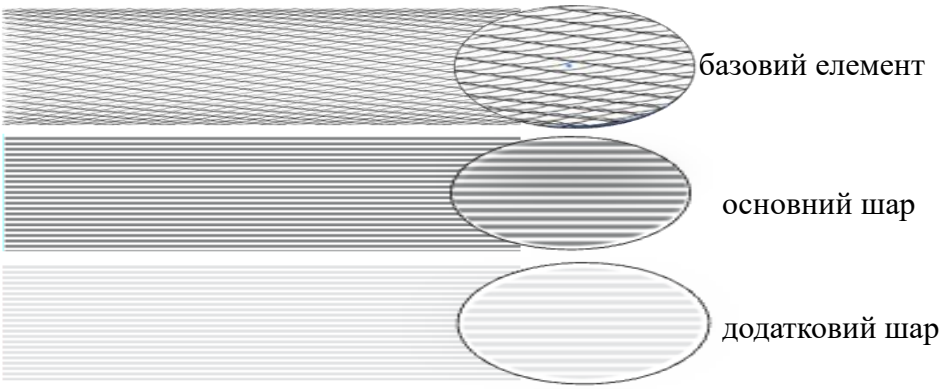
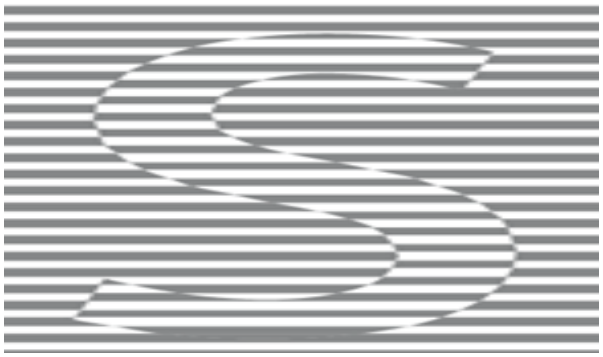


Рисунок 2.6. Формування шарів прихованого зображення

Запропоновано створення верхніх шарів хвилями з частотами, які відповідають значенню порядку 10 – 60 мкм із заданими градієнтними характеристиками інтенсивності кольору. А зверху накладаємо інший шар періодичної структури, який будуємо за принципом суперпозиції. Прихований елемент формують на основі двох рівномірних шарів, утворених лініями з однаковою лініатурою і відносною площею елементів. У першому полі встановлюємо 60 – 70% градацій сірого для ліній, а в другому 15 – 20%, та накладаємо на базовий елемент із відображенням темних ділянок на першому шарі й світлих ділянок на другому шарі. Суть цього методу полягає у створенні документа, який буде захищений прихованим елементом на основі шару

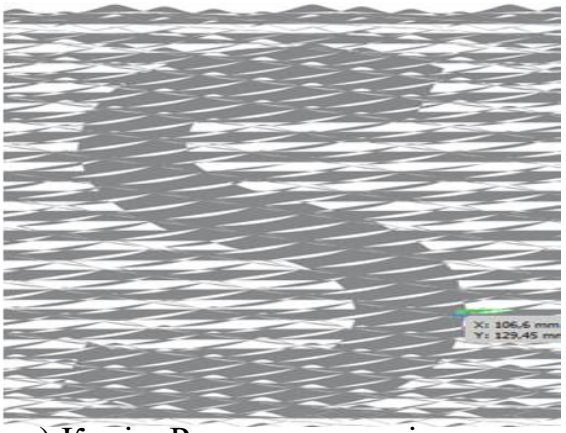
основного елемента із додаванням додаткового шару та базового елемента шаблона – маски. На наступному етапі генерується текстовий документ. Ідентифікують документ внаслідок дослідження документа та шаблона – маски. Якщо документ скопійовано, то оригінал чітко відрізняється від копії за захунок латентності, коли відбується розпад чи налипання ліній [107].

Приховане зображення стає видимим за рахунок унікального візерунка, який з'являється при копіюванні. Це дозволяє відрізнити справжність на рівні експертизи і розрізнити оригінал від підробки (навіть професійної якості). Схему ідентифікації прихованого елементу за допомогою шаблону наведено на рисунку 2.7.



а) перший шар з прихованим написом

б) другий шар з прихованим написом



в) Копія. Результати суміщення шарів і маски

Рисунок 2.7. Формування латентного елементу рисунок а і б та результати копіювання прихованого елементу на рисунку в

Отримані латентні зображення були розроблені методом виявлення і збереження отримані прихованих зображень. На основі використання основного та допоміжного шарів, а також маски, які формують латентне зображення з підвищенням захисних характеристик. Таким чином ЛЗ сформоване багатьма шарами важко сфальсифікувати, адже при копіюванні

воно змінює свою структуру за рахунок того що приховане зображення стає видимим і спотворює документ. На рисунку 2.8 а показано документ з латентним зображенням і на рисунку 2.8б показано копію цього документу, де латентні елементи стали видимими. Як видно, виявлені зображення повністю зберегли структуру прихованих зображень і, у випадку рисунку 2.8б приховане зображення, повністю стає видиме і показує, що документ є скопійованим.

а б

Рисунок 2.8. а) Вигляд захищеного документа; б) Скопійований вигляд документа з видимими латентними елементами

Для визначення чи документ є оригінальнимчи сфальсифікованим використовують візульну оцінку або використовують приладо-контрольоване устаткування залучаючи експерта в даній області. Також для визначення оригінальності документів використовують градієнті властивості латентних зображень, які визначаються друкарськими характеристиками, а саме розтискування фарби, оптична щільність, трепінг та інше, що можна обчислити за формулою Шеберстова-Мюррея-Девіса.

Таблиця 2.1.

Результати обчислення градієнтних властивостей латентних зображень

Градієнтні властивості друкованих плашок	Обчислені значення (метод Шеберстова-Мюррея-Девіса)	Експериментальні дані (розроблений метод)	Відносна похибка ΔR
20%	2.09	7.3	5.21
40%	5.05	9.9	4.85
60%	6.25	9.9	3.65
80%	7.4	11.9	4.5
100%	8.8	13.6	4.8
Середнє значення			4.24

Середнє значення відносної похибки оптичної густини ΔR за результатами вимірювання дорівнює **4.2%.**

Приховане зображення відображається візуально, що дозволяє відрізнити оригінал та копію. Як видно з рисунку 2.8, латентне зображення повністю виявляє структуру прихованих елементівпри та стає повністю повністю видимим. Латентне зображення є візуально помітним та дозволяє виявити фальсифікат. Таким чином, розроблені методи формування ЛЗ дозволили підвищити якість захисних характеристик друкованих документів. Отримані латентні зображення, також дали змогу проаналізовати виявлення прихованих зображень при копіюванні.

Висновки до розділу 2

1. Розроблено метод формування латентних зображень, на основі модифікації відомого методу, що полягає у використанні як частотних, так і просторових перетворень вихідного зображення.
2. Розроблено метод формування латентних зображень, у який додано рівняння векторизації з видаленням діагональних ліній та введено дані для приховання зображень, які стають видимими та призводять до істотних спотворень документів.
3. Впровадження латентного зображення відбувається в документ без втрати візуальних характеристик, що дозволяє поліпшити якість та допомагає виявляти зображення при копіюванні.
4. Розроблений метод створення латентних елементів у якому графічним елементом є зображення, яке складається з шарів з наперед заданими параметрами, що забезпечує підвищення точності побудови графічних елементів.

РОЗДІЛ 3 ФОРМУВАННЯ ПРИХОВАНИХ ЗОБРАЖЕНЬ НА ОСНОВІ СТВОРЕННЯ НОВИХ ГРАФІЧНИХ ЕЛЕМЕНТІВ

У третьому розділі реалізовано та розроблено метод моделювання елементів тонкої графіки на основі локального викривлення лінії сітки та деформації лінії на основі малих збурень. Також реалізовано метод формування латентних елементів на основі фракталів. Розроблено метод формування муару, що призводить до значних змін форми чи повної втрати елементів зображення на копії. Подано опис розроблених методів для розробленої інформаційної технології.

3.1. Алгоритм моделювання та розроблення елементів тонкої графіки

Лінії тонкої графіки, які формують елемент мають різні форми та виконані двома способами: позитивним, де товщина ліній є в діапазоні 40-80 мкм та негативним – 60-100 мкм. Основним елементом растрового зображення є точка. Якщо растрові точки з відстані розглядання зображення здаються досить дрібними, то через інтегруючу дію ока воно «розмивається», а, отже, сприймається растрове зображення як безперервне тонове. Чим більше растрових точок на одиницю площі, тим природнішим виглядає зображення [97]. Параметри растрування оригіналу залежать від методів, які застосовуються при раструванні, а відповідно, і від розміру растрої точки. Сітка ліній, яка накладається на оригінал зображення утворює елементарні комірки растру. Кількість ліній на дюйм носить назву лініатури растру та вимірюється частотою сітки [84]. Растрування залежить від оптичної густини, оскільки всі об'єкти описуються точками у координатній сітці певного розміру. Оскільки, растрова точка складається з окремих пікселів, кількість рівнів градації визначається розміром растрової комірки, всередині якої вони відтворюються, а також РЗ у крапках на дюйм (dpi – dots per inch), з якою можна позиціонувати окремі елементи. Відомо [108], що око людини при

спостереженні растрової структури з лініатурою, більше 60 лін/см (тобто 150 ліній на дюйм) з нормальної відстані, приблизно 30 см, перестає розрізняти окремі растрові точки. Багато друкарських машин друкують зображення з максимальною лініатурою растру 120-160 ліній на дюйм. Для того, щоб надійно захистити документ потрібно створити такі лінії, які добре друкує друкарська машина офсетного друку, та, які здаються розмитими людському оку. Тому з урахуванням значення тону «пробілу» (незадрукованої комірки), вважаємо, що всього в діапазоні від 0 до 100% можливо сформувати N + 1 рівень градації. Число градацій також залежить від оптичної густини, а саме від інтервалу оптичих густин g.

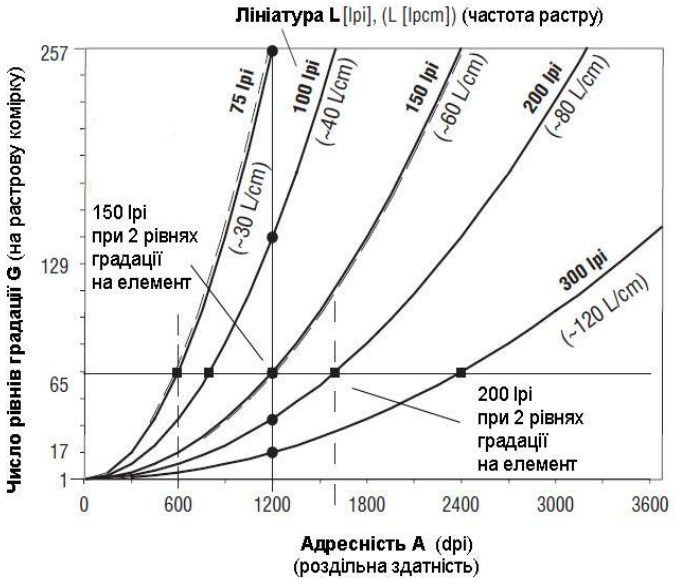


Рисунок 3.1. Зв'язок між лініатурою, адресністю та числом градацій при числовому раструванні та побудові зображення [137-139]

Для виведення якісних повноколірних зображень друкарська машина друкує зображення з лініатурою растру 300 lpi та РЗ 2400 dpi. Тому вважаємо, що для друку тонкої графіки потрібно, щоб друкарська машина відтворювала дрібні елементи з лініатурою растру 200 lpi та РЗ 1500 dpi та передачею 65 градацій. Отже, визначено значення мінімальної відтворюваності штрихів та мікротексту при офсетному друці, лініатуру растру 150 lpi, при якій зображення для спостерігача розмивається, та лініатуру 200 lpi, при якій тільки невелика кількість друкарських машин зможе якісно надрукувати зображення

[134, 135]. Цим забепечується додаткова надійність захисту на етапі друкування. Колір та відтінок ліній підбирають таким чином, аби під час копіювання та сканування лінії не відтворювалися. До інформаційних характеристик друкованого документу належать оптична густина, процент растрової крапки, рівномірність нанесення фарби, розтиснення, трепінг, які наведено в таблиці 3.1.

Таблиця 3.1.

Інформаційні характеристики друкованого документа

Інформаційні характеристики друкованого документа	Оригінал, %	Копія, %	Відносна похибка ΔE , %
Оптична густина	88 – 100	7 – 12	13
% растрової точки	85 – 100	9 – 15	15
Рівномірність нанесення фарби та розтиснення	82 – 100	8 – 10	12
Трепінг	80 – 100	6 – 9	10
Критеріальні ознаки порогових характеристик			10-15

Розв’язуючи обчислювальні задачі побудови розв’язків диференціальних рівнянь, які базуються для практичного вирішення задачі локальної апроксимації даних застосовуємо чисельні методи інтерполяції та наближення функцій. Таким чином, доводиться заміняти одну функцію $f(x)$, яка є відомою, на деяку близьку до неї функцію $\varphi(x)$, яка має визначені властивості. Нехай функція $f(x)$ задається таблицею значень $f(x_0)$, $f(x_1)$, …, $f(x_n)$ для деякої скінченної множини аргументів x_i і в процесі розв’язування задачі необхідно використовувати значення $f(x)$ для проміжних значень аргументу. Функцію $\varphi(x)$ будують таким чином, щоб в заданих точках $x_0, x_1, ..., x_n$ вона приймала значення, що збігаються зі значеннями $f(x_0)$, $f(x_1)$, …, $f(x_n)$, а в інших точках відрізка $[a, b]$, що належить області визначення $f(x)$, приблизно зображувала функцію $f(x)$ із тим чи іншим ступенем точності. Тоді під час розв’язування задачі замість функції $f(x)$ використовують функцію $\varphi(x)$. Задача побудови функції $\varphi(x)$ є інтерполяційною задачею.

3.1.1. Побудова зображень на основі локального викривлення лінії

Розглянемо площину майбутнього рисунка, як додатню першу чверть двовимірного декартового координатного поля $П^2$ у пікселях. Розмістимо початок координат точку *O(0,0)* у лівому нижньому куті рисунка, із горизонтальною віссю OX та вертикальною віссю OY. Тоді кожна точка рисунка матиме координати (x, y) у пікселях. Для побудови захисних сіток використаємо масив значень $B_N = \{(x_i, y_i), i = 1,\square, N\}$ графіка будь-якої кривої $f(x, y) = 0$ у звичайних декартових координатах площини R^2, N- кількість точок графіка. Побудову ліній тонкої графіки реалізовано за допомогою спеціального ПЗ, яке дозволяє побудувати довільну композицію ліній, наприклад: пропорційність, масштабність, динамічність, контраст і нюанс. Причому можна гарантовано забезпечити присутність зображення ліній у довільному потрібному пікселі координатного поля рисунку. При побудові ліній використовують паралельний перенос та поворот, що дозволяє здійснювати різні комбінації. Також можна створити симетричні та асиметричні зображення ліній, використовуючи різні закони композиції.

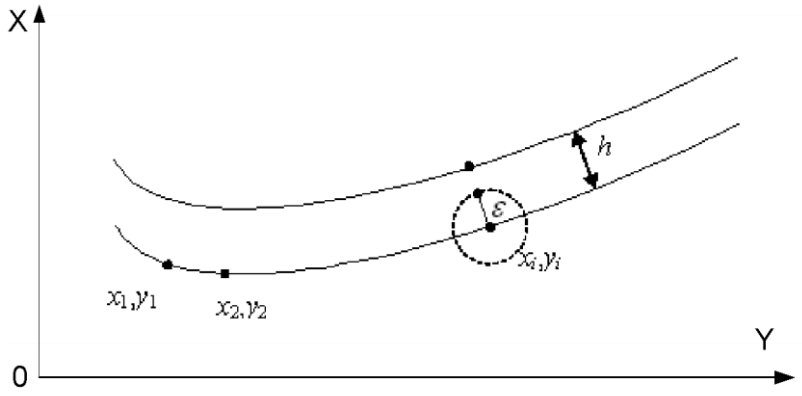


Рисунок 3.2. Фрагмент фонової лінії

Алгоритм побудови зображень на основі деформації ліній тонкої графіки, реалізований для побудови зображень на основі деформованих

фонових ліній для формування рисунку. Вводимо початкові дані: масив координат графічного елемента сітки B_N крок сітки h, розміри околу деформації ε, ($\varepsilon < h$), тип закону розмноження графічного елемента. Фрагмент ліній тонкої графіки представлений на рисунку 3.2, а алгоритм побудови зображення показано на рисунку 3.3. Будуємо масив пікселів $\{W_N \subset \Pi^2\}$, що відповідає точкам рисунка. Після цього формуємо масив D_N як перетин двох масивів S_N та W_N, $D_N = S_N \cap W_N$. Відповідно до вибраного розміру околу кожної точки масиву D_N проводимо деформацію ліній сітки в околі.

Запропоновано три різні методи локального викривлення ліній сітки S_N з метою отримання зображення у лініях сітки.

Метод зміщення. Точки $\{y_i\}$ масиву D_N знайденого зміщаємо на певну кількість пікселів $Y_i = y_i + C_i$, де C_i - величина зміщення, див. рисунок 3.3.

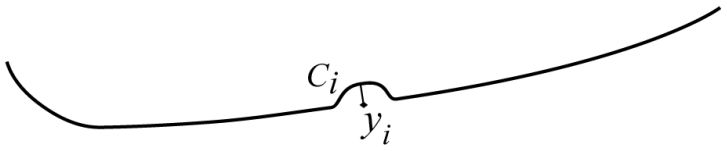


Рисунок 3.3. Деформація ліній сітки на основі згладжування

Таким чином утворюється новий масив $\overline{D}_N = \{Y_{i,}, y_{i,} \in \overline{D}_N\}$. А на кінцях зміщення проводимо згладження за допомогою методів згладження.

Метод малих збурень. У точках масиву D_N проводимо малі збурення графіка використовуючи тригонометричні функції.

Новий масив $\bar{D}_N = \{Y_{i,}, y_{i,} \in \bar{D}_N\}$ формуємо за законом:

$$Y_i = y_i + AL(\varphi x_i + \alpha), \tag{1.4}$$

де A- амплітуда коливань збурення лінії, φ – період збурень, α- зміщення, L- довільна періодична функція. Приклад зображення побудованого за даним методом показано на рисунку 3.4.

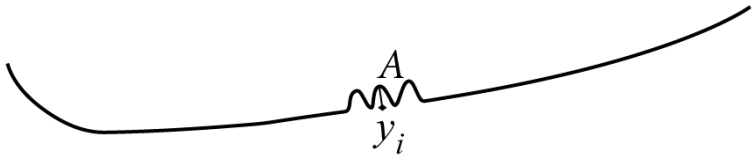


Рисунок 3.4. Деформація ліній сітки на основі малих збурень

За допомогою тонкої графіки реалізовано три різні способи утворення ліній. В залежності від вибору режиму збурення, лінія може підніматися на зображення.

Складність репродукції пов’язана зі складною геометричною структурою і мінімально можливою товщиною ліній елементів тонкої графіки. Складність відображення елементів тонкої графіки пов’язана зі специфічними технологічними умовами пристосування друкарських циліндрів і декелів друкарських машин для відображения такої графіки в області друкарських технологій.

Одним з можливих застосувань є створення захисного елементу в документі. ЗЕ виконано тонкими неперервними лініями, які мають властивість деформуватись та перериватись при копіюванні. Метод підвищує точність побудови захисних сіток та значно розширює можливості для захисту документів. Лінії тонкої графіки можна контролювати у кожній точці координатної площини, що дає змогу ідентифікувати документ. Крім того, обчислені значення у базі даних дають змогу будувати документи унікальної форми із функціями персоніфікації кожного документу. Лінії тонкої графіки є складними елементами, які переплітаються і становлять перешкоду для імітації їх цифровими копіювальними пристроями. Тонкі лінії, з яких складаються фонові сітки, тому їх скопіювати неможливо. На рисунку 3.5.відображено алгоритм побудови захисного латентного зображення на основі деформації ліній фонових сіток.

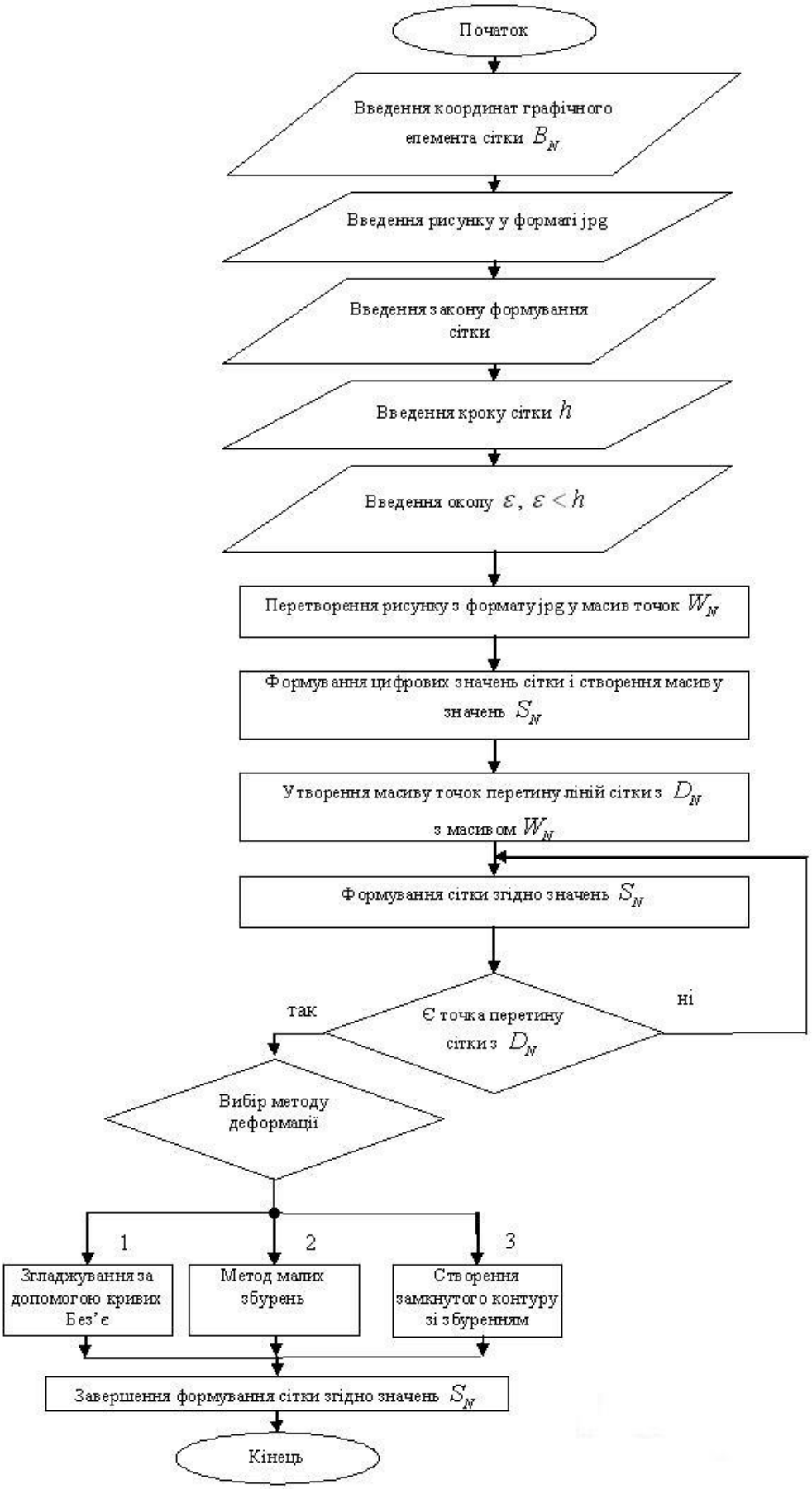


Рисунок 3.5. Алгоритм побудови зображення на основі деформації фонових сіток

Метод захисту друкованих документів за допомогою створення прихованих елементів дозволяє вибирати тип ліній зі створеної бази даних та будувати графічні композиції у векторному форматі, який забезпечує високу поліграфічну якість документа, що захищається. Вибір параметрів дає можливість отримати різні типи графіків, що дозволяє персоніфікувати кожен документ. Захищена КІ записується у PostScript-файл, який є прототипом формату Portable Document Format (PDF) [163]. Проведений аналіз структури PostScript-файлів дозволив запропонувати інформаційну технологію захисту документів. Для створення захисних елементів використовується програмування на мові PostScript і вбудовування потрібних елементів у відповідні місця PostScript-файлів. Таким чином, можна будувати не тільки захисні елементи, але і шифрувати, або приховувати необхідну інформацію.

Для побудови прихованого елементу, який накладаються на документ, розроблено технологію, що базується на точних математичних формулах. За цими формулами побудовано графічні примітиви на основі розробленого методу захисту з використанням PostScript технології.

Алгоритм методу, схема якого представлена на рисунку 3.6.

1. Вибирається документ, в який потрібно додати латентне зображення;
2. Формується одиничний графічнтй елемента використовуючи один з методів формування тонкої графіки;
3. Здійснюється конструювання захисної сітки. Здійснюється вибір алгоритму повторюваності ліній. При побудові захисної сітки можна змінювати колір, товщину та тип ліній.
4. Здійснюється формування програмного коду на мові PostScript, який реалізовуватиме вибраний дизайн прихованого елементу;
5. Здійснюється поєднання у єдиний файл прихованого елементу та документу. На цьому етапі формування документу є завершеним. Але у разі необхідності можна перетворити файл у формат PDF.

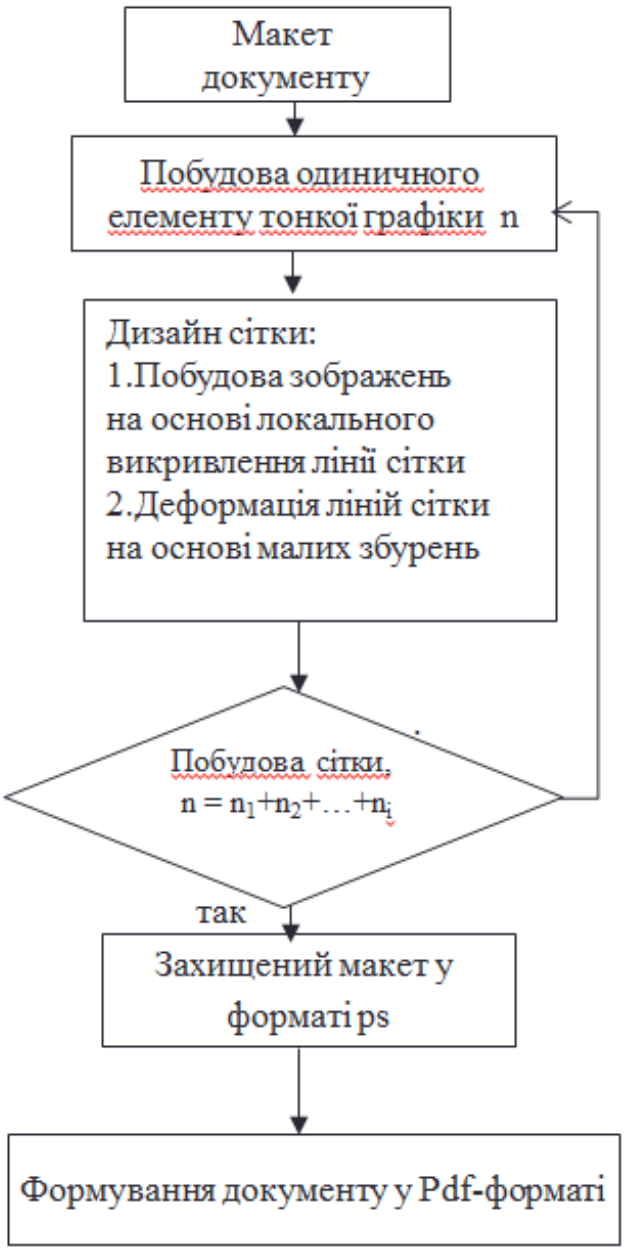


Рисунок 3.6. Алгоритм формування прихованого зображення на основі використання тонкої графіки у друкований документ

На рисунку 3.7. та 3.8 представлено сітку побудовану горизонтальними паралельними лініями методом побудови, які захищаються від НСД накладенням на документ захисних сіток унікальної будови.

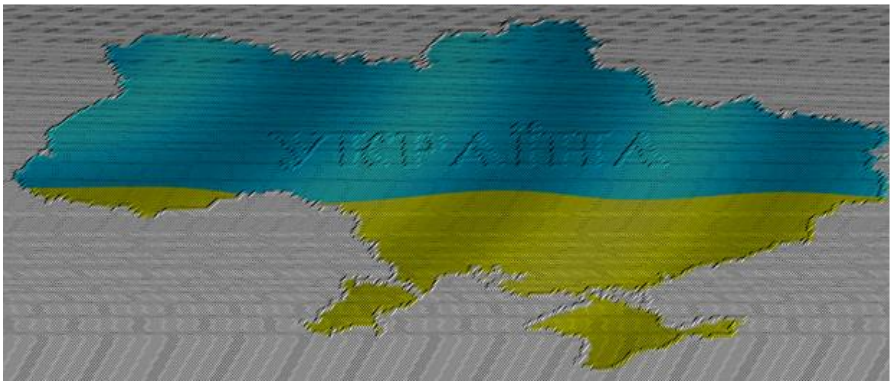


Рисунок 3.7. Карта України сформована методом «тонкої графіки»

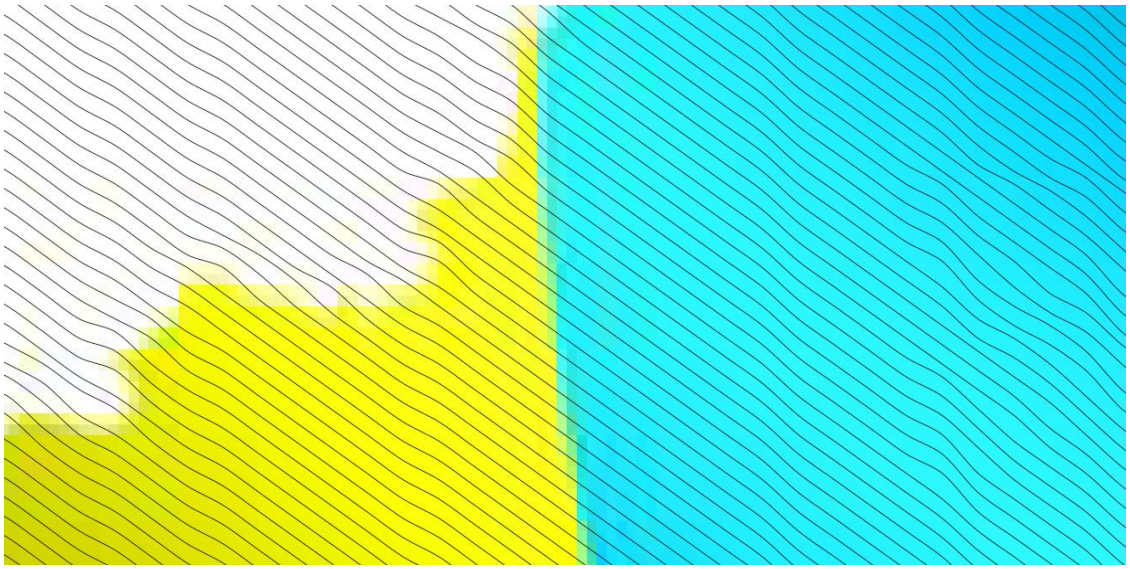


Рисунок 3.8. Редактор тонкої графіки при збільшенні зображення в 1600% показує на скільки є тонкими лінії, які покривають і прорисовують зображення.

При створенні контуру зображення, в основі лежать захисні сітки (за основу береться метод побудови векторного зображення, у якому контур зображення формується зміною координат; файли зображень перетворюються у масиви чисел, які порівнюються та видозмінюються).

На рисунку 3.9. представлено побудову прихованих елементів на основі синусоїди, яка створюється при перетворенні ліній за допомогою зміни амплітуди та періоду (до кривих застосовано інтерполяцію сплайнами, яка зробила їх гладкими, неперервними, без різких та гострих переходів). По відтворенню найдрібніших елементів можна розпізнати достовірність

документу. При спробі відсканування рисунку та його оцифрування однозначно втрачається якість, оскільки при таких діях лінії розпадаються на крапки. Тому при спробі фальсифікації можна за допомогою розробленої технології ідентифікаціївизначити спробу фальсифікації документа. Запропонований метод грунтується на створенні захисних елементів за допомогою тонких неперервних ліній, що дозволяє підвищити захист документів, які мають вбудовані латентні зображення створені методом тонкої графіки.

Рисунок 3.9. Формування прихованого елементу тонкою графікою методом деформація ліній сітки на основі малих збурень

3.2. Алгоритм моделювання та розроблення прихованих зображень на основі формування фракталів

Проаналізувавши кількість фальсифікацій за останні роки встановлено, що існує доцільність розроблення нових методів та засобів захисту документів, які зможуть забезпечити надійний та ефективний захист, але з іншого боку не потребують використання дорогих матеріалів та устаткування. Розроблено метод формування латентних зображень з використанням фракталів для підвищення рівня захищеності документів. За нормами Держстандарту [39 - 41] документ, який потребує захисту повинен бути в межах позитивного відтворення 40 – 50 мкм і негативного – 60 – 80 мкм. Щоб гарантувати високу якість друку та зменшити підробку величини мікроелементів, які мають бути в межах 200 – 250 мкм.

Одним з графічних способів захисту є формування латентних зображень за допомогою фрактальних елементів, які дозволяють впровадити засоби захисту з новими характеристиками, які відповідають вимогам технологічних процесів та використовуються для підвищення захисних характеристик документів.

3.2.1 Алгоритм моделювання прихованих зображень з викоористанням методу формування фракталів

У даному методі приховані елементи формуються на етапі додрукарської підготовки документів.

Латентні зображення можна створювати за допомогою вбудовування фракталів в зображення для підвищення рівня захищеності. Фрактал – це геометрична фігура, в якої один і той самий фрагмент повторюється за кожного збільшення масштабу. Фрактали, що володіють такою властивістю і що отримуються в результаті простої рекурсивної процедури (комбінації лінійних перетворень), називаються конструктивними фракталами [109-111].

Основною перевагою фракталів є те, що це самоподібні структури, а це означає, що фрактал являє собою об’єкт безкінечної складності. Існує декілька груп фракталів: перша – це алгебраїчні – фрактали, які створюються за рахунок нелінійних процесів; друга – це геометричні фрактали, які формуються ламаною-генератором, яка за один крок змінює ламану і створює новий фрактальний елемент; третє – це стохастичні фрактали, які будуються випадковими параметрами з різними ітераціями.

Для захисту документів на основі формування латентних елементів доцільніше використовувати групу геометричних фракталів. На рисунку 3.10. показано алгоритм формування латентного зображення на основі використання фракталів.

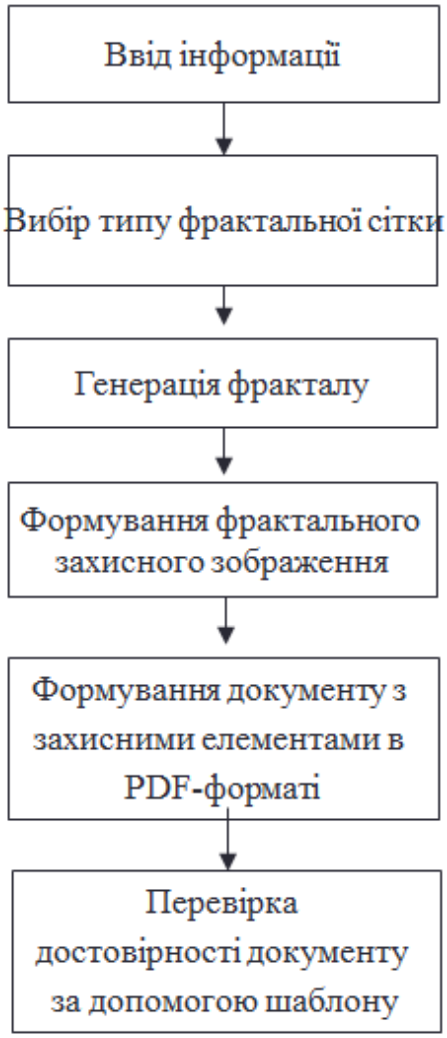


Рисунок 3.10. Алгоритм моделювання прихованого елементу в документі на основі методу формування фракталу

Побудований алгоритм демонструє процес генерування фрактального захисного зображення, яке вбудовується в документ. У вхідний документ після вибору фрактальної сітки вбудовують латентне зображення з фрактальним елементом, який додається як допоміжний шар.

Зображення формується таким чином, щоб елементи фракталу заповнили всю площину захисного зображення і таким чином за рахунок параметрів ліній, які відповідають параметрам тонкої графіки унеможливлюють копіювання документа офісною технікою, адже спотворення стають видимими візуально.

Товщина ліній задається з мінімальними параметрами, а колір задається в світлій тонові гаммі або з додаванням особливих фарб у процентному співвідношені до основної фарби, що забезпечує надійність та ефективність захисту. Метод захисту здійснюється у векторному форматі, тому генерація фрактальних сіток підвищує ефективність захисту, а генерація даного документу в pdf–файл надає додаткових захисних властивостей.

Змінюючи лише деякі характеристики, можна створити величезну кількість різноманітних фігур, для точного відтворення яких потрібно витратити значну кількість часу. Тобто даний спосіб формування ЛЗ з застосуванням фонових сіток на основі фракталів для захисту цінних паперів підвищує рівень захищеності документів, а при використанні спеціальних видів друку унеможливлює створення якісних фальсифікацій.

Фрактал формується таким чином, що кожна ламана є настільки подрібненою та сформованою певною кількістю ітерацій, що копіювання такого латентного зображення стає неможливим. Фрактальна сітка забезпечує захист за рахунок складності візерунку та створює захист завдяки наявності дрібних елементів та тонких ліній, що розташовані близько одна до одної. Приклади захисних сіток, що побудовані на саме основі геометричних фракталів, подані на рисунку 3.9.

Елементи фрактальної сітки для латентного зображення утворюють на допоміжному шарі, який накладається на зображення. Елементи фракталу

будують векторним способом генеруючи графічні елементи завдяки копіюванні, розмноженні та деформації лінії-генератора. Використовуючи рекурсивну процедуру фрактал здійснює роль генератора, що визначає площу захисного елемента, а ініціатор заповнює всю площину зображення.

3.2.2 Метод створення сіток на основі фракталів

Першим кроком є побудова сітки, яка здійснюється за рахунок задання параметрів фракталу. Коли відбулась побудова фракталу можна здійснити певну кількість видів фрактальної сітки за допомогою новоствореного фрак талу, при цьому потрібно змінити товщину лінії, кут нахилу, поворот, змінити кількість ітерацій. При спробі фальсифікації важко відтворити фрак тал, адже треба знати формулу та всі задані параметри для формування такого фракталу, тому це є часозатратно і невигідно. Вхідний документ в який буде вбудоване латентне зображення з фрактальною сіткою на верхньому шарі може містити будь яку інформацію, як графічну так і текстову.

На рисунку 3.9 зображено захисну сітку, побудовану на основі фракталу за методом Мінковського, яка заповнює усю площину документу без самопересічень.

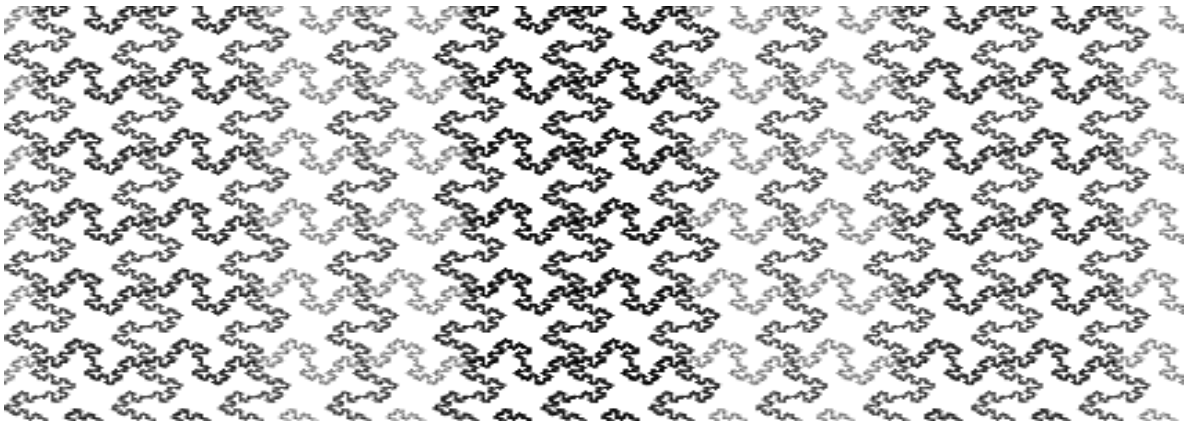


Рисунок 3.9. Захисні сітки на основі геометричних фракталів на основі кривої Мінковського

3.2.3. Метод створення сіток на основі фракталів, генератором яких є інший фрактал

Будується графічна сітка на основі фракталу, у якому додатково генерується інший фрактал. Даний метод дозволяє ускладнити фоновий візерунок, забезпечуючи велику кількість різноманітних варіантів заповнення фону та підвищує ефективність захисту. Даний спосіб дозволяє будувати ГСЗ заповнення документа захисною сіткою, зменшуючи одиничні елементи до межі відтворення поліграфічної техніки. На рисунку 3.10 зображено прихований елемент, побудований на основі фракталу за методом Серпінського, який заповнює усю площину документу.

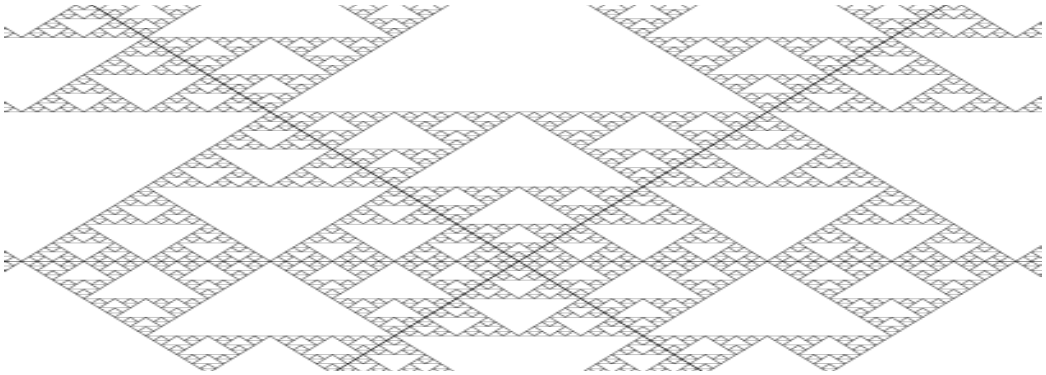


Рисунок 3.10. Прихованих елементів - геометричних фракталів на основі трикутника Серпінського, генератором яких є інший фрактал

3.2.4. Метод створення фракталів на основі паттерну

Заповнення площини документу відбувається на основі створення паттерну. При збільшенні кількості ітерацій кількість дрібних елементів патерну зростає, – відповідно зростає рівень захисних властивостей створеної сітки. Паттерн будують у будь-якому графічному редакторі і він стає основою при подальшій побудові. Основу копіюють, розмножують, здійснюють паралельне перенесення, поворот і таким чином заповнюють усю площину документу. Основу можна заповнити фракталом, який описаний в способі 1. Перевагою даного методу є те, що кількість елементів паттерну є скінченною, їх можна порахувати, кожен елемент паттерну обмежений певною границею,

кожен елемент паттерну є продовженням попереднього паттерну і між ними не існує проміжків та перекриттів. На рисунку 3.11 зображено захисну сітку на основі побудови фракталу Хартера - Хейтуэя, який генерується іншим фракталом Хартера - Хейтуэя, що забезпечує ефективніший захист друкованого документу.

Рисунок 3.11. Прихованих елементів - геометричних фракталів на основі паттерну

Застосування цих способів дозволило підвищити ефективність та надійність захисту на основі побудови сіток, що базуються на геометричних фракталах. Складність елементів, наявність надзвичайно тонких ліній у геометричних фракталах, а також оригінальність створених одиничних елементів забезпечують надійний та ефективний захист документів.

3.2.5. Метод створення прихованих елементів на основі формування фракталів

Метод створення фрактальних елементів базується на створенні захисної сітки, яку утворюють на основі фракталу у векторному форматі за допомогою рекурсивної процедури до генерування одиничного елементу з заданими параметрами дроблення. Фрактали будуються рекурсивною процедурою, де кожен одиничний ГЕ постає в ролі генератора, який задає величину захисного елемента. На растрові поля поміщають зображення, де буде вбудовано прихований елемент. Наступним кроком цей елемент буде вирізано, а дану область заповнюється растром зі зміщенням ліній растру на половину кроку.

Наступний крок це зміна кольору латентного елементу для створення маски. Для цього білі елементи залишаються білими, а темні елементи – прозорими. Потім розташовують маску на основному шарі, а на основі допоміжного шару формується маска для отримання прихованого елементу захисту. Тим самим забезпечується можливість перевірки достовірності документу з використанням оригінального шаблону. Для формування латентного зображення з'єднують основний та допоміжний шари та між ними поміщають прихований надпис, наприклад, «FALSE» (рис. 3.12, 3.13).

Рисунок 3.12. Основний шар з прихованим написом

Рисунок 3.13. Допоміжний шар з прихованим написом, що утворений зміщенням ліній

Також створюється шаблон-маска для перевірки достовірності документів (рис.3.14), яка містить сітку з лінійним растром частотою рівною лініатурі растру прихованого зображення з відносною площею растрових елементів 40-45%.

Рисунок 3.14. Шаблон-макса з відносною площею растрових елементів 40-45%

При спобі фальсифікації документу з таким латентним зображенням виникає різниця лініатури растру від оригінальної, тому при накладенні шаблону приховане зображення буде гірше читатися чим покаже, що документ було сфальсифіковано. На рисунку 3.15 - лініатура зображення менша від лініатури шаблону на 5%.

Рисунок 3.15. Ознаки фальсифікації

Для підвищення захисту розроблено фрактальні сітки, які ускладнюють копіювання та деформацію латентного зображення за рахунок складної геометричної структури. Фрактали – це само подібні структури, які не залежать від масштабу, але мають певні властивості форма зображення залежить від заданих параметрів; фрактальна сітка при збільшенні не змінює параметрів фракталу. За рахунок цих властивостей збільшується ефективність захисту. Параметри фракталу будуються на основі генерації ліній векторним форматом, для підвищення захисту використовують зміну тональності чи

кольору. Побудова фрак талу здійснюється двома фігурами – ініціатором і генератором.

Генератор – це ламана крива, що складається з *N* рівних відрізків довжиною *r*. Розмірність обчислюється за формулою *D = ln*N/ln*(1/r)*. За основу захисного елемента беремо геометричний фрактал, який зображений на рисунку 3.9. Генератор складається з восьми рівних частин. Параметри фрактала: *N = 8*; *r = 1/4; D = 1.26.*

Побудова відбувається згідно наступного алгоритму. Створюється відрізок, який приймають за основу та який є ініціатором, тоді замінюють його на генератор за рахунок чого відбувається побудова кривої, при цьому враховується, що кожний наступний етап генератора був ініціатор на попередньому етапі. Таким чином вибудовується захисна фрактальна сітка.

Рисунок 3.16. Основний шар з фрактальною сіткою, яка зміщена на лінію растру

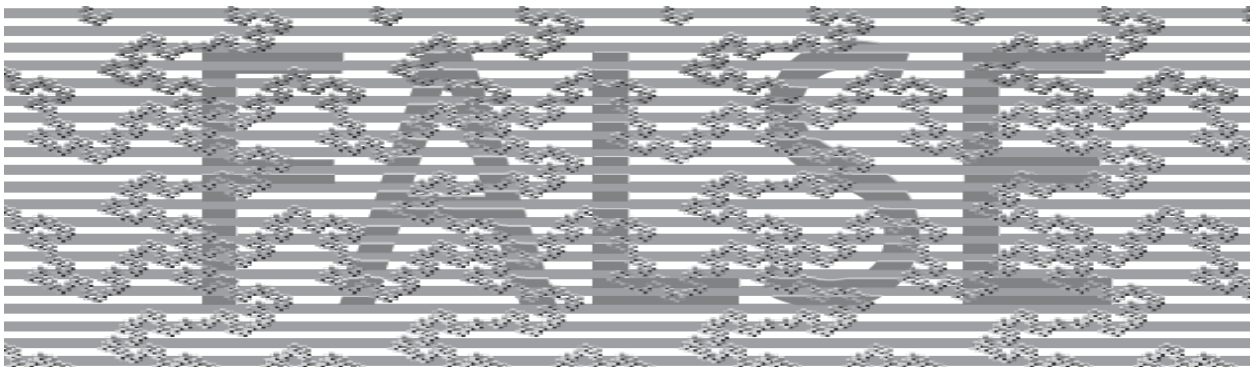


Рисунок 3.17. Додатковий шар з фрактальною сіткою, яка зміщена на лінію растру

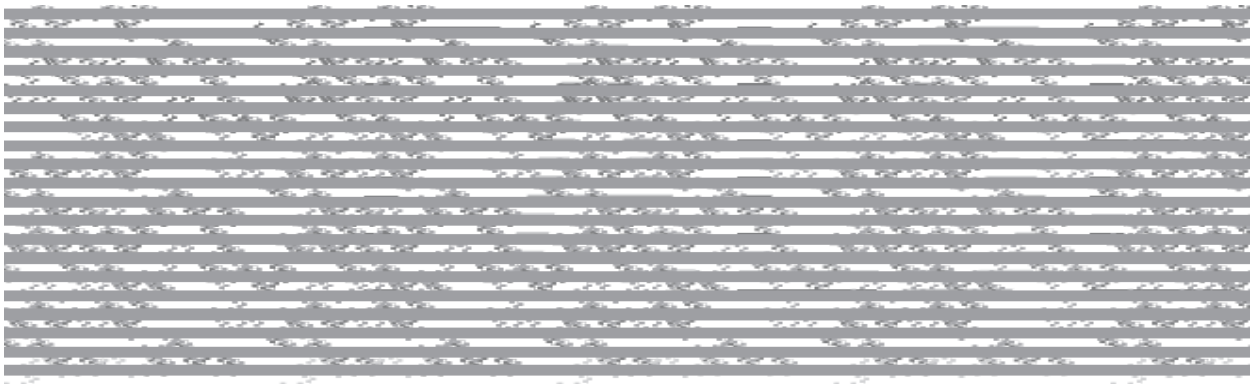


Рисунок 3.18. Шаблон- маска з відносною площею фрактальної сітки

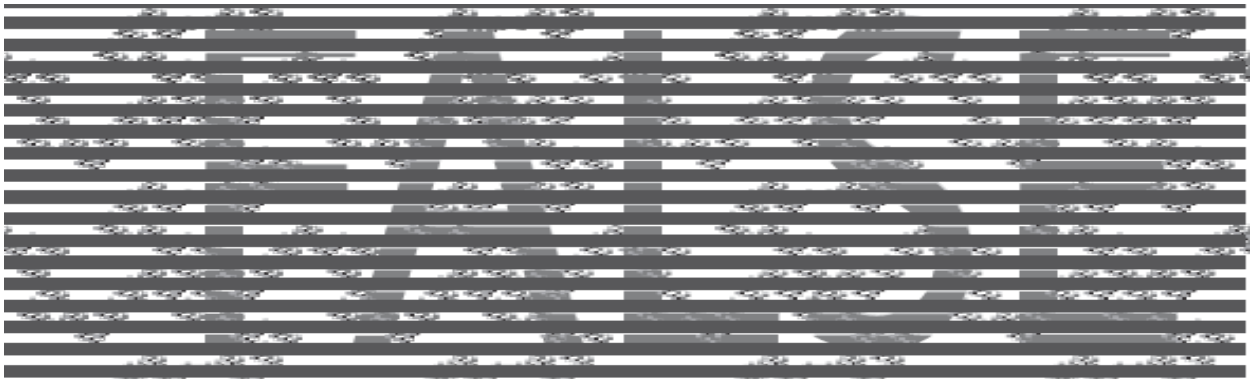


Рисунок 3.19. Ознаки фальсифікації – фрактальна сітка не співпадає з періодом на шаблоні-масці

На рисунках 3.16 - 3.18 показано реалізацію розробленого методу. На рисунку 3.19 представлено приклад визначення підробленого документу. Створений метод захисту документів з використанням фрактальних елементів, які вбудовані в латентне зображення, що підвищує рівень захисту документів та візуально допомагає виявити фальсифікацію. Оскільки впровадження та реалізація методу не вимагає великих фінансових затрат, то розроблений метод може широко використовуватись для захисту документів.

3.3. Загальна характеристика формування муару

Приховані елементи відображатимуться з ефектом муару при копіюванні, а отже таким чином фальсифікація стане помітною. Муар виникає при використанні декількох шарів, а саме коли базовий шар із зображенням поверхні періодичної структури у вигляді непрозорих та прозорих паралельних смуг зазнає змін.

3.3.1. Загальна структура моделей формування графічних пасток на основі муару

Метод формування муару полягає у створені тонких паралельних ліній, з шириною 0.25мм та частотами повторень, які кратні цілому числу частоти відтворюючого пристрою і відрізняються від частоти копіювання/сканування на величину муароутворення менше 0.25мм, що візуально не можливо розпізнати без використання спеціальних оптичних пристроїв. Документ із прихованими елементами містить хоча б одне латентне зображення, котре складається з великої кількості видимих і окремо надрукованих елементів, які, в свою чергу, складають захисний об'єкт, утворених з кривих ліній та фрагментів.

При споробі копіювання документу формуються муар, а за рахунок зміни латентного зображення чи часткового спотворення чи втрати певних елементів на копій стає легко відрізнити оригінал та фальсифікат.

Основна ідея методу полягає в тому, що для прихованих елементів формують зміщення частини ліній муару на половину величини кроку лінії. Рисунок 3.20 ілюструє основний принцип методу створення маурного прихованого елементу, використовуючи періодичні лінії. На рисунку 3.20а *об'єкт А* формується за допомогою паралельних ліній та завантаженого об'єкту трикутника.

На рисунку 3.20б зображено *об'єкт В*, який сформовано паралельними лініями з зміщенням на пів кроку. Об'єкт набуває видимості і зафарбовується в сіре на основі накладання об'єктів у яких ліній співпадають, що представлено на рисунку 3.20в. Паралельні лінії, які формуються зі зміщенням на половину періоду, спричиняє висвітлення форми трикутника, проте зовнішня форма змінює колір до сірого відтінку, що показано на рисунку 3.20 г. Основний та допоміжний шари будуть друкуватися як сіра область при копіюванні. Розмір растрових точок відозмінюється від найменщого відтінку сірого до найбільшого відтінку чорного, залежно від методу перетворення у півтони.

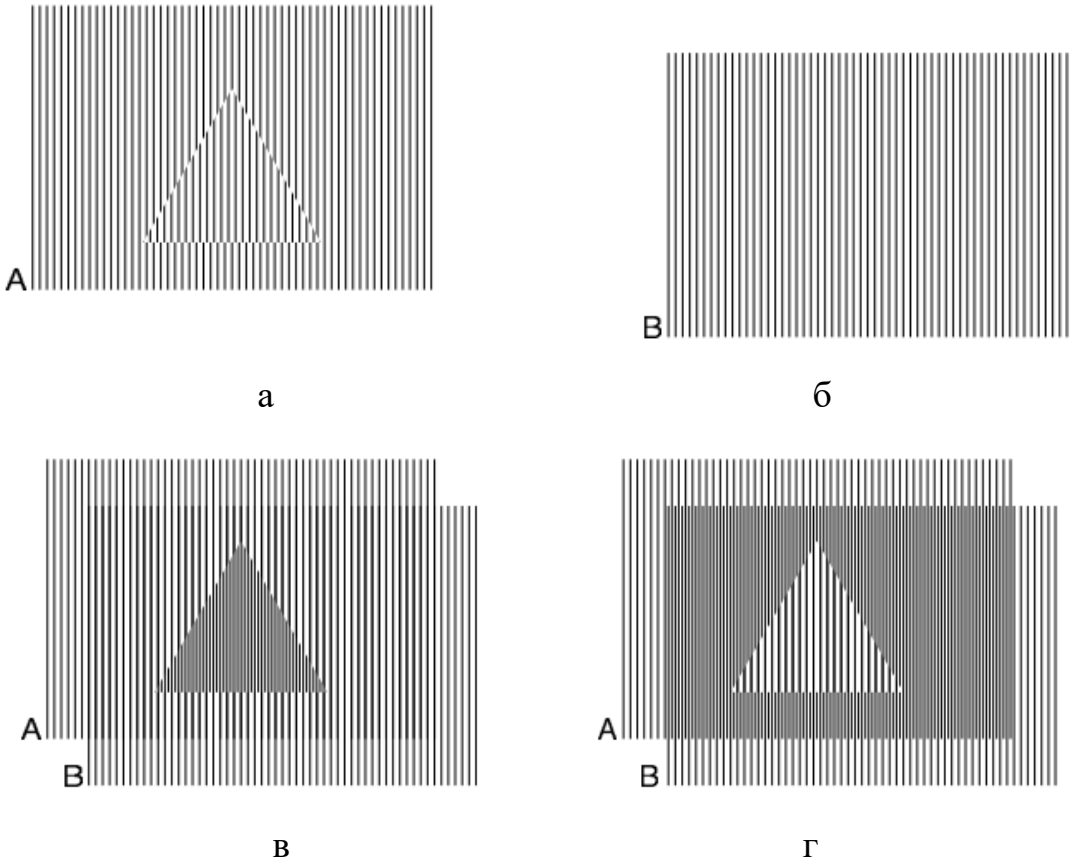


Рисунок 3.20. Ефект муару за допомогою ліній

Зображення може набувати повного чорного чи білого кольорів, оскільки приховане зображення є невидиме. Для приховуваання декількох різних зображень можна використовувати розроблений метод кольорового друку із застосуванням блакитних, пурпурного, жовтих і чорних напівтонів для всієї площини документа.

Муар відображається, коли кут зменшується, тим чином чіткіше відображається спроба фальсифікації документів [173-176]. Іншим варіантом є поворот ліній на кут, наприклад, 45^0 при створенні. В результаті цього, контур зображення шляхом розбивання прямих ліній за рахунок зміни ширини лінії в залежності від щільності сірого кольору оригінального зображення. Якщо ж у рівновіддалених лініях змінювати кут нахилу, то можна спостерігати муар у вигляді решіток, які змінюватимуть нахил. Нижче подано рисунки з кутами нахилу в 5^0, 15^0, 45^0. Важким для фальсифікації є метод створення муару при певному куті формування ліній, так як при копіюванні повністю неможливо

виділити та забрати муар. Таким чином в даному способі ми будемо вибирати не аналогові всім відомі кути повороту, а деформовані, як наприклад 43^0, 57^0 , 99^0, та ін. На рисунку 3.21. - муар, який відбувася за рахунок паралельних рівновіддалених ліній, які уворились при накладанні двох решіток.

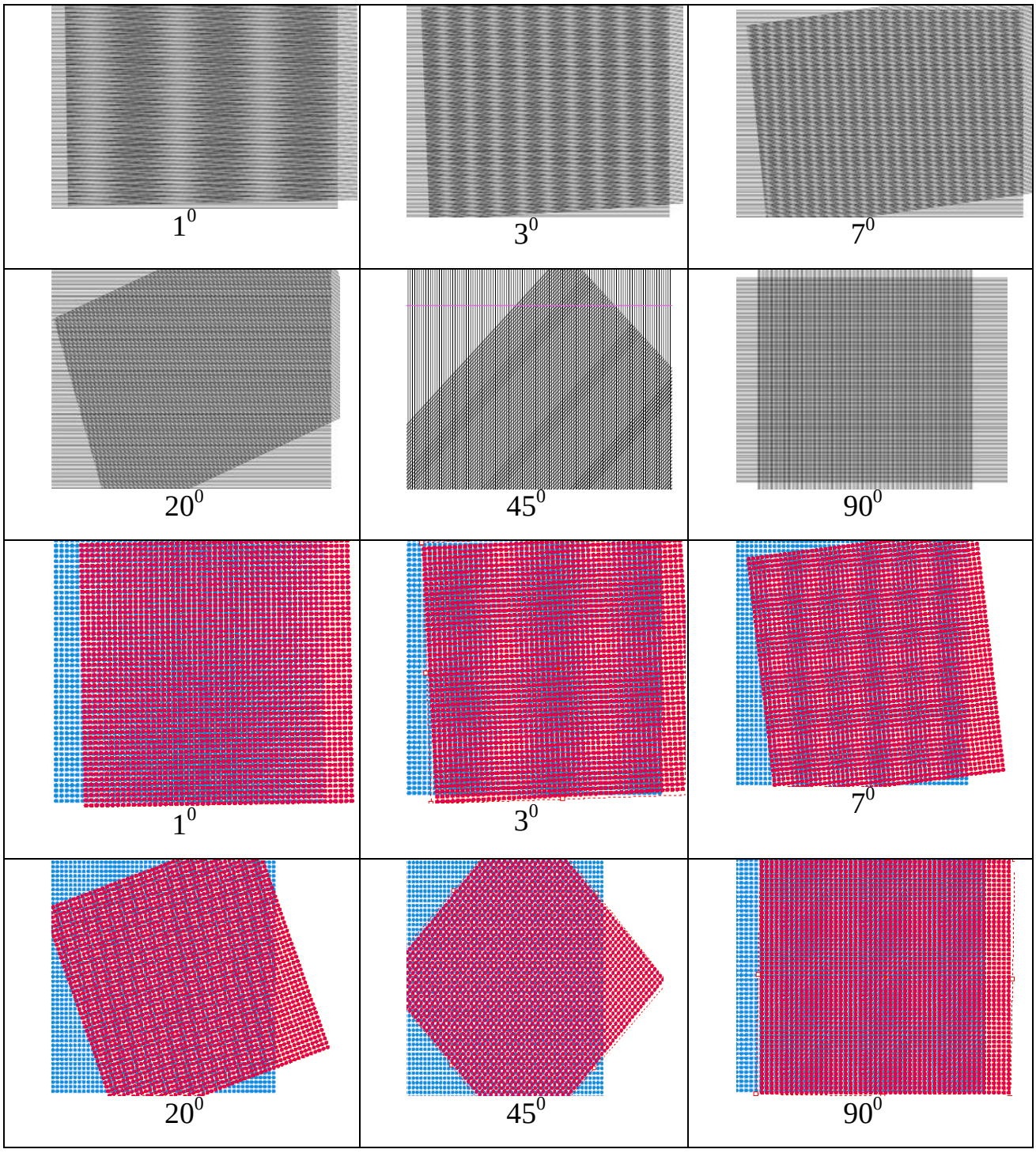


Рисунок 3.21. Виявлення муару при різних кутах нахилу.

Щоб зменшити кількість фальсифікацій, а також для підвищення рівня виявлення фальсифікації документу потрібно використовувати більше двох сіток, при умові що частота другої сітки кратна частоті першої, а частрота наступної – попередній. Таким чином вдається досягнути вищий рівень захисту і захистити документ від копіювання, адже муар буде проявлятись

3.3.2. Математична модель створення захисту на основі муарних елементів за допомогою ліній

За допомогою математичної моделі створюється сітка, яка формується паралельними лініями у співвідношенні ширини і відстаннями між лініями, які розташовані у певній послідовності. Модулюється відстань і ширина ліній так, щоб їх співвідношення відповідало заданому розрахованому параметру. Потім трансформуються прямі лінії в лінії іншої форми для відтворення геометричних зображень. За рахунок цього забезпечується можливість утворення ЛЗ з підвищеним рівнем захисту. Технологічний прогрес в області фотокопіювальної техніки і сканерів призвів до того, що з появи кольорових фотокопіювальних машин з дуже високими технічними характеристиками виникло завдання створення зон, що дають муаровий ефект при цифровому копіювання, наприклад, за допомогою кольорового фотокопіювальних пристрої для копіювання документів. Цей муаровий ефект спотворює оригінальне зображення і вказує на те, що це копія.

Муаровий ефект з'являється, коли зчитування інформації порушується і оригінальне зображення спотворюється, зокрема, отримують нерівномірні зміни відтінків і кольорів. Появу таких муарових ефектів складно передбачити, оскільки це залежить від технічних характеристик і регулювання використовуваного для відтворення обладнання.

Спосіб характеризується тим, що послідовно:

1. а) створюють однорідний фон, утворений прямими паралельними ліній, позначений проміжком d_0 між двома лініями, і шириною l_0 ліній, визначаючи таким чином постійне співвідношення $r_0 = l_0/d_0$;

2. б) змінюють фон, модифікуючи проміжок d_0 між лініями в залежності від попередньо обраних параметрів генерації;
3. в) ширину лінії l_n і проміжку d_n змінюють таким чином, щоб між першою та другою лініями було співвідношення $l_n/d_n = r_0$.

Перевагами способу є те, що параметри модифікації розподілу ліній можуть вибиратися в залежності від фотокопіювальних пристроїв і сканерів, від яких намагаються знайти захист, і, з іншого боку, те, що ці зміни не спотворюють оригінального зорового аспекту зображення, при огляді неозброєним оком, завдяки тому, що співвідношення ширини лінії і відстані між двома послідовно розташованими лініями залишається постійним.

Різні варіанти створення муарних елементів, перетворенням прямих ліній в лінії іншої форми, наприклад, синусоїди, концентричні кола, замкнуті й незамкнуті вигнуті лінії і т.д., дозволяють підвищити рівень захисту.

Іншим варіантом здійснення графічних пасток на основі муару є лінії фону можуть бути частково або повністю повернені на певний кут, або можуть бути обернуті на цей кут тільки певні сегменти ліній, що знаходяться всередині контуру, що обмежує зміни в латентних зображеннях.

За іншим варіантом здійснення зображення та з метою створення малюнка згадані лінії "розрізають", тобто вони є переривчастими всередині контуру, що обмежує зображення. Сукупність прямих паралельних ліній, причому відстань між двома послідовно розташованими лініями постійно і дорівнює d_0, ширина по всій довжині лінії дорівнює l_0, а співвідношення $r_0 = l_0/d_0$ є незмінною.

Змінюючи відстань між двома лініями t_n+1 досягається, що $d_n = d_0 + d_1 + \ldots + d_k$ причому проміжок d_n є параметром лінійної модуляції. Нехай r_0 – це співвідношення ширини лінії і відстані від першої лінії до другої, яке змінюють на l_n таким чином, що $l_n = l_0 + l_1 + \ldots + l_k$ щоб співвідношення l_n/d_n завжди дорівнює r_0, причому є параметром модуляції ширини лінії. Формується однорідне зображення, яке створить муар при копіюванні за рахунок налипання фарби між лініями. Відстань між лініями задається по

формулі $d_n = d_0 + i^{\wedge}(1 + sin(2^{\wedge}h/N)$. N виступає періодом модуляції. Таким чином, ми отримуємо зображеннгя, де відстань між двома лініями формується синусоїдально.

Наступнипм етапом буде зміна форми лінії за рахунок модифікації ширини лінії, які утворимо у формі хвилі чи синусоїда та перетворимо в криві за формулою:$l_n = l0 + i^{\wedge}(1 + sin2^{\wedge}n/N)$.

Іншим варіантом є поворот ліній на кут, наприклад, 45^0, в результаті цього, контур зображення створює ефект рельєфу шляхом розбивання прямих ліній. Можемо змінювати ширину ліній в залежності від щільності сірого кольору оригінального геометричного зображення. На рисунку 3.22 зображено накладання шарів латентного зображення з різними кутами нахилу.

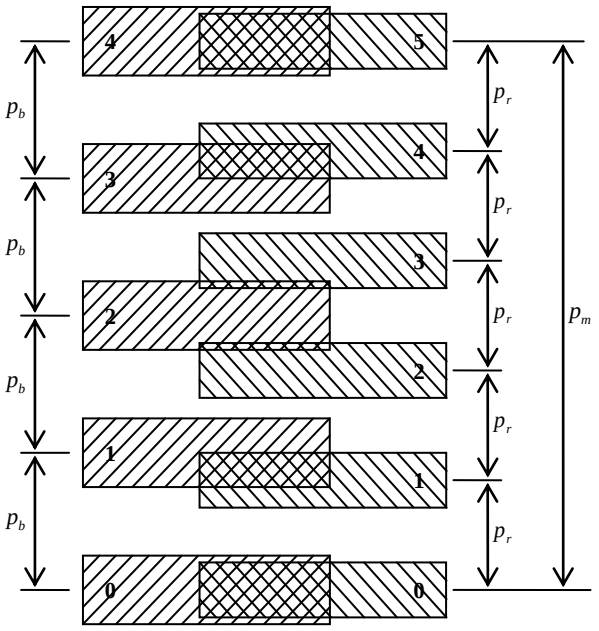


Рисунок 3.22. Накладання муарових шарів в під різним кутом нахилу та різною розмірністю

Ефект муару є візуальне явище і виникає унаслідок неточного накладання двох шарів, які містять комбінацію прозорих та непрозорих елементів. Муар у перекладі означає мерехтіння і створюється унаслідок інтерференції між двома рівномірними структурами. Математичне представлення ефекту муару є тривіальним та може бути довільно описаним.

Розглянемо дві побудови з паралельних вертикальних.

Будуємо два зразки з вертикальними лініями. Нехай першу побудову зразка здійснюємо з кроком p (рисунок 3.23.), а другу з кроком $p+\delta p$, де вибираємо δ у межах $0<\delta<1$. Якщо лінії двох зразків накладаємо один на один на лівій частині рисунка, зсув між лініями збільшується унаслідок іншого кроку повторення (рисунок 3.23б). Здійснивши декілька перетворень вертикальні лінії стануть протилежність ліній наступного зразка.

Якщо розглядати конструкцію із накладеннння ліній одного типу, то відбудеться заповнення зони утворюючи білий проміжок між рядками, і темної зони, якщо лінії будувались у протилежному напрямі. Зявиться рівномірна гратка з певним кроком повторення якщо під однаковим кутом накласти однакові лінії (рисунок 3.23г). Середина першої темної зони зі зсувом рівна $p/2$. На n-ій лінії друга зразок посувається на n_p

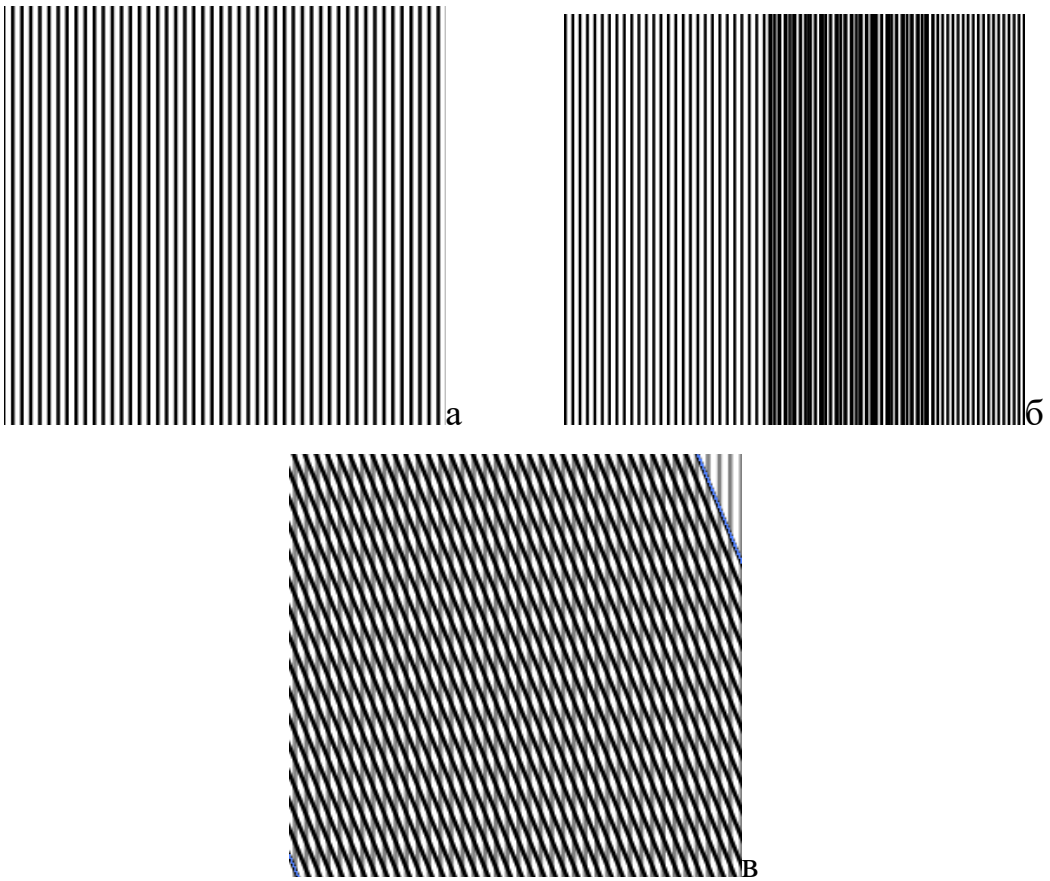


Рисунок 3.23. а – зразок з вертикальними та рівновіддаленими лініями;
б – явище муару при накладанні рівномірних паралельних ліній,
в – явище муару при накладанні паралельних ліній під кутом

Явище муару створюється якщо відстань між лініями першого зразка p_b, а відстань між лініями другого зразка p_m при накладанні їх відношення еквівалентне з відстанню плюс 1.

$$\frac{p_m}{P_b} = \frac{p_m}{P_b} + 1 \tag{3.1}$$

Муар спостерігається коли у рівновіддалених лініях змінюється кут нахилу.

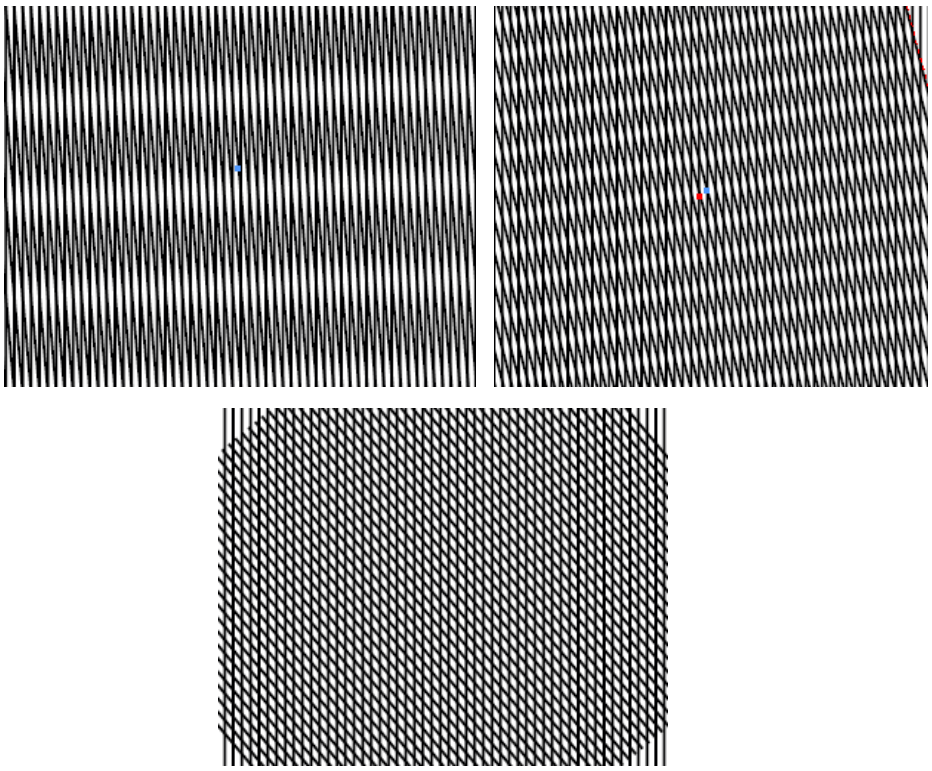


Рисунок 3.24. Муарові решітки з кутами нахилу в 5^0, 15^0, 45^0 відповідно

Використані періоди T_b -період базового шару, T_r - період верхнього шару, and T_m - період муару, можна обчислити за такими формулами :

$$T_b=p_b*\cos\alpha_b,\ T_r=p_r*\cos\alpha_r, T_m=p_m*\cos\alpha_m.$$

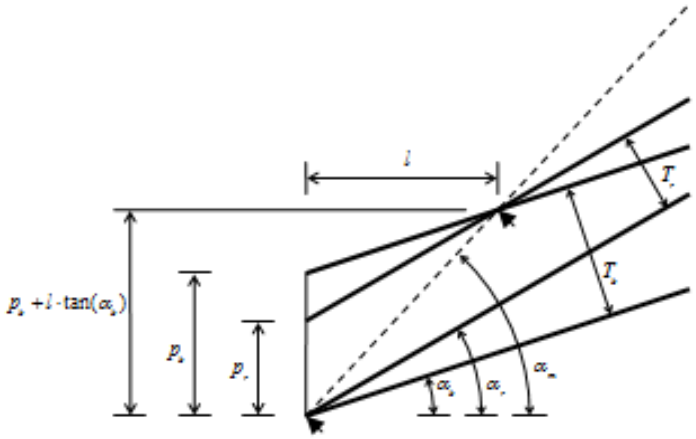


Рисунок 3.25. Змінам нахилу кута ліній базового шару

З рисунку 3.25 отримуємо наступні два рівняння:

$$\begin{cases} \tan\alpha_m = \dfrac{p_b + l\cdot\tan\alpha_b}{l} \\ \tan\alpha_r = \dfrac{p_b - p_r + l\cdot\tan\alpha_b}{l} \end{cases} \tag{3.2}$$

З цих рівнянь отримуємо рівняння для обчислення нахилу муара ліній залежно від схильностей базового шару і виявлення ліній рівня:

$$\tan\alpha_m = \frac{p_b\cdot\tan\alpha_r - p_r\cdot\tan\alpha_b}{p_b - p_r} \tag{3.3}$$

Для базового шару нахилу прикріплений до 30 ступеня, з періодом базового шару. Крива рисунку 3.26 являє собою ступінь нахилу лінії муара залежно від виявлення шару нахил лінії. Дві інші криві відповідають випадкам, коли базовий шар нахилу дорівнює 20 і 40 градусів відповідно.

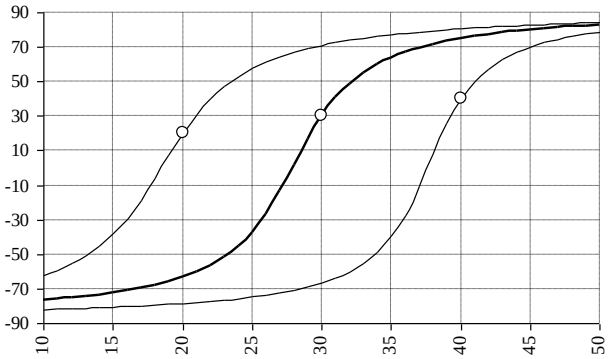


Рисунок 3.26. Муар лінії нахилу для базового рівня ліній нахилення дорівнює 30^0

Використані періоди T_b, T_r, та T_m можна обчислити за такими формулами:

$$T_b = p_b \cdot \cos \alpha_b ,$$
$$T_r = p_r \cdot \cos \alpha_r ,$$
$$T_m = p_m \cdot \cos \alpha_m \qquad (3.4)$$

Використовуючи рівняння (3.4) виводимо відому формулу для кута муара ліній:

$$\alpha_m = \arctan\left(\frac{T_b \cdot \sin \alpha_r - T_r \cdot \sin \alpha_b}{T_b \cdot \cos \alpha_r - T_r \cdot \cos \alpha_b} \right) \qquad (3.5)$$

За допомогою тригонометрії виводимо наступні формули:

$$\cos \alpha = \frac{1}{\sqrt{1 + \tan^2 \alpha}}$$
$$\cos(\alpha_1 - \alpha_2) = \cos \alpha_1 \cdot \cos \alpha_2 + \sin \alpha_1 \cdot \sin \alpha_2 \qquad (3.6)$$

З рівнянь (3.5) і (3.6) маємо:

$$\cos \alpha_m = \frac{T_b \cdot \cos \alpha_r - T_r \cdot \cos \alpha_b}{\sqrt{T_b^{\,2} + T_r^{\,2} - 2 \cdot T_b \cdot T_r \cdot \cos(\alpha_r - \alpha_b)}} \qquad (3.7)$$

З рівнянь (3.1) і (3.4) отримуємо:

$$T_m = \frac{T_b \cdot T_r}{T_b \cdot \cos \alpha_r - T_r \cdot \cos \alpha_b} \cdot \cos \alpha_m \qquad (3.8)$$

З рівнянь (3.7) і (3.8) виводимо другий формулу для періоду муару ліній:

$$T_m = \frac{T_b \cdot T_r}{\sqrt{T_b^{\,2} + T_r^{\,2} - 2 \cdot T_b \cdot T_r \cdot \cos(\alpha_r - \alpha_b)}} \qquad (3.9)$$

З тригонометрії випливає, що:

$$T_m = \frac{T}{2 \cdot \sin\left(\frac{\alpha_r - \alpha_b}{2}\right)} \tag{3.10}$$

Можна припустити, що всі кути по відношенню до лінії основного шару рівні і рівняння (3.3) буде виглядати наступним чином:

$$\alpha'_m = \arctan\left(\frac{\sin \alpha'_r}{\cos \alpha'_r - 1}\right) \tag{3.1}$$

З тригонометрії випливає, що:

$$\tan \frac{\alpha}{2} = \frac{1 - \cos \alpha}{\sin \alpha}$$

$$\tan(90° + \alpha) = -\frac{1}{\tan \alpha} \tag{3.12}$$

А з формул (3.11) і (3.12):

$$\alpha'_m = 90° + \frac{\alpha'_r}{2} \tag{3.13}$$

Використовуючи рівняння (3.2) використаємо відому формулу в [1] для кута муару ліній, графічне представлення якої показано на рисунку 3.27:

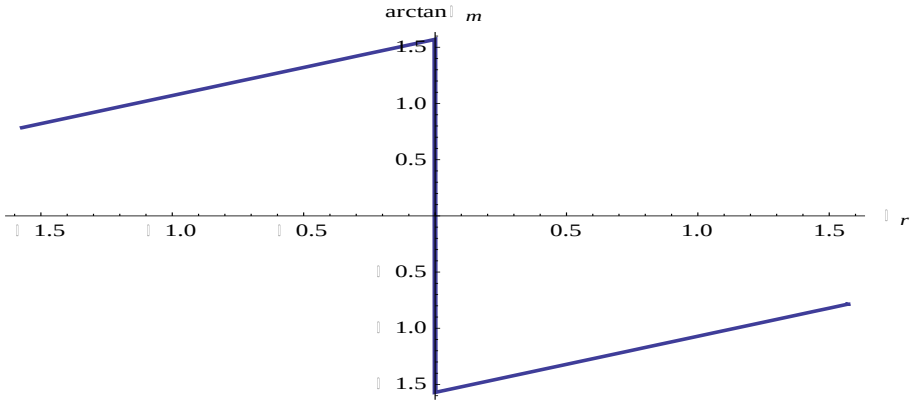


Рисунок 3.27. Зміна кута нахилу муару від кута верхнього шару α_r

На рисунку 3.27 показана залежність зміни кута нахилу муару α_m від зміни кута нахилу верхнього шару α_r при α_r в межах від 0 до π при зміні частоти повторів ліній верхнього шару T_r. Зміна частоты повторів ліній базового шару є постійною та рівною T_b=0.5, T_r в межах від 0.01 до 0.5.

Муар з'являється, коли зчитування інформації порушується та оригінальне зображення спотворюється, та, зокрема, отримують нерівномірні відтінки кольорів та шарів. Появу таких муарових ефектів тяжко передбачити, поскільки це залежить від технічних характеристик та налаштування обладнання, яким виконують зчитування інформації.

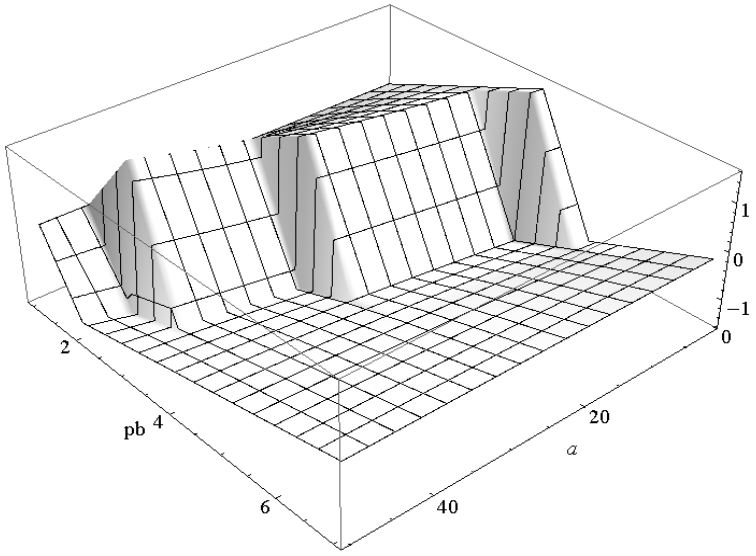


Рисунок 3.28. Залежність зміни кута нахилу муара від зміни кута нахилу верхнього шару та частоти повторень верхнього шару

3.3.3. Формування муару на основі ідентичності побудови

Базовий та допоміжний шари побудовані однаково, отже їхні періоди співпадають, тобто $T_b = T_r$. Якщо дві решітки є ідентичними, то обґрунтуємо формування муару коли базовий та допоміжний шар решіток зміщується під певним кутом, а отже їхні періоди співпадають, тобто $T_b = T_r$.

Розглянемо випадок коли дві однакові сітки, які будемо повертати під певним кутом. На кут α_r змістили першу сітку, а наступну на α_b. Якщо сітки є одинакові, то їх період повторення є також однаковим, звідки $T_b = T_r$.

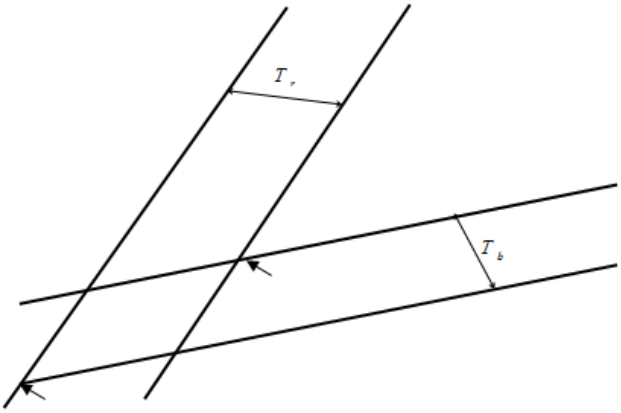


Рисунок 3.29. Дві решітки є ідентичними, $T_b = T_r$

З формули (3.4) отримуємо

$$T_m = \frac{T_b^{\,2}}{\sqrt{2T_b^{\,2} - 2 \cdot T_b^{\,2} \cdot \cos(\alpha_r - \alpha_b)}} \tag{3.14}$$

Отримуємо:

$$T_m = \frac{T_b}{\sqrt{2 \cdot (1 - \cos(\alpha_r - \alpha_b))}} \tag{3.15}$$

$$T_m = \frac{T_b}{\sqrt{2 \cdot (\cos\alpha_r \cos\alpha_b + \sin\alpha_r \sin\alpha_b)}} \tag{3.16}$$

Якщо прийняти, що $\alpha_r = 0$, то $\cos\alpha_r = 1$

$$T_m = \frac{T_b}{\sqrt{2 \cdot \cos\alpha_b}} \tag{3.17}$$

З формули 3 при $\alpha_r = 0$, $T_b = T_r$ випливає:

$$\alpha_m = \arctan\left(\frac{\sin\alpha_r}{\cos\alpha_r - 1}\right) \tag{3.18}$$

Побудуємо з формули 3.18 залежність кута муарної решітки α_m від кута нахилу базової решітки α_r. При α_r=0 решітки співпадають, муар не відтворюється. На рисунку 3.30 введено α_r, яке змінюється в межах від *-π/2* до *π/2*. Побудуємо залежність зміни періоду муарної решітки у випадку коли періоди базового та основного шару сіток ідентичні. Ця залежність описана формулою 3.17.

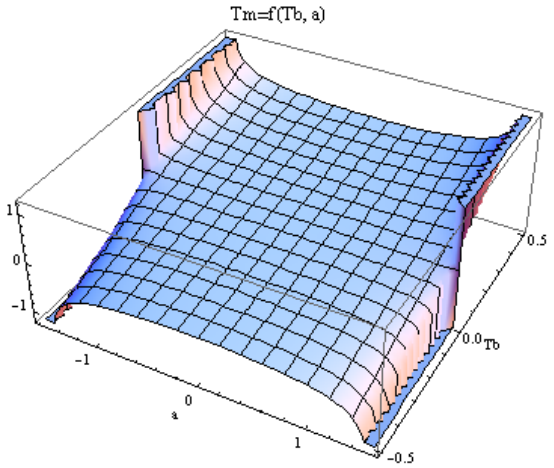


Рисунок 3.30. Залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару T_b.

На рисунку 3.30 показано залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару T_b. З рисунку випливає, що у випадку малих змін кута нахилу базового та основного шару муарна решітка різко змінює свій період. На рисунку 3.31 проведена залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару $T_b \in [0..0{,}01]$.

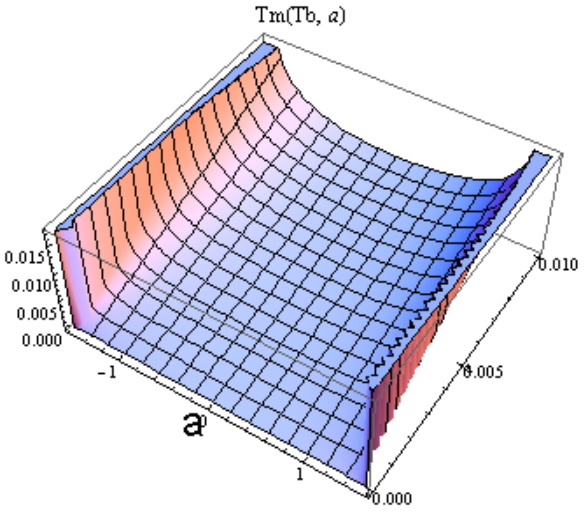


Рисунок 3.31. Залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару $T_b \in [0..0{,}01]$.

З графіка випливає, що чим менший період решітки базового шару, тим величина муарної решітки є помітніша та більша, що проілюстровано на рисунку 3.31. Тому для подальших досліджень було обрано період зміни ліній базового шару $T_b \in [0..0{,}01]$.

3.3.4. Формування муару на основі змінних періодів у шарах

Базовий шар має у k-разів більший період за допоміжний шар, отже $T_b = kT_r$. Якщо одна з решіток має період в *к*-раз більший за іншу решітку, то один з шарів буде зміщено на певну траєкторію та буде повернуто під кутом, α_r, а другий на α_b.

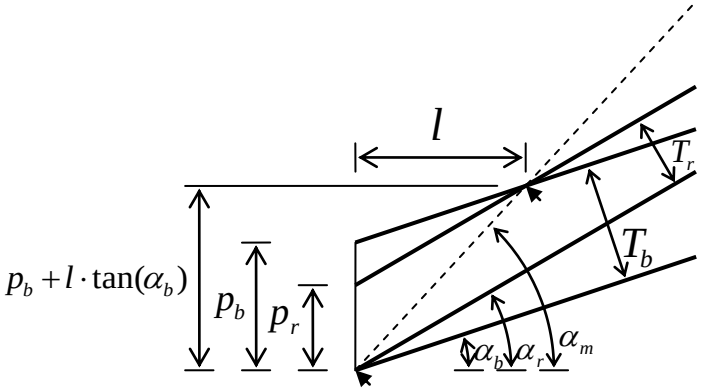


Рисунок 3.29. Базовий шар у *k*-разів менший за період допоміжного шару

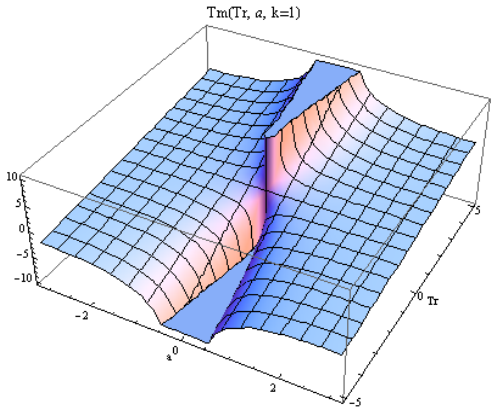
З формули (3.4) отримаємо:

$$T_m = \frac{kT_r^{\,2}}{\sqrt{k^2 T_r^{\,2} + T_r^{\,2} - 2 \cdot kT_r^{\,2} \cdot \cos(\alpha_r - \alpha_b)}} \qquad (3.19)$$

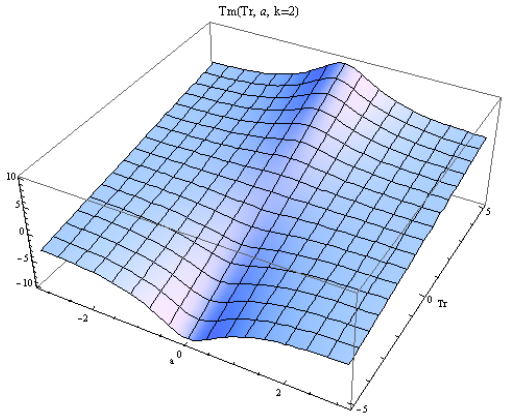
Після перетворень випливає:

$$T_m = \frac{kT_r}{\sqrt{k^2 + 1 - 2k\cos(\alpha_r - \alpha_b)}} \qquad (3.20)$$

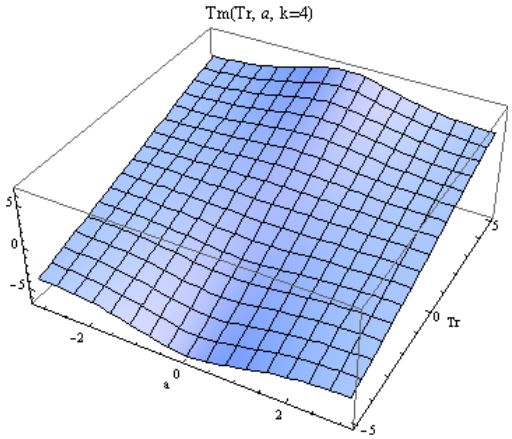
Побудуємо залежності кута повороту базового та допоміжного шару решіток, періоду допоміжного шару від періоду зміни муарної решітки T_m. Отримані залежності представлено на рисунку 3.32. Експерименти було здійснено для випадків коли базовий шар був у один, два, чотири та вісім разів більший за допоміжний. Отримано залежність періоду муарної решітки T_m від кута нахилу α_b та періоду допоміжного шару T_r для кожного з чотирьох досліджень.З рисунку 3.32.*а* випливає, що при *k = 1* різко збільшується муар, якщо кут нахилу 5^0. Доведено, що T_m змінюється від -20^0 до $+20^0$, що показано на рисунку 3.32.*а* та 3.32.*б*.На рисунку 3.32.*в* та 3.32.*г* показані випадки зміни періоду базового шару коли *k= 4 та k=8*. Таким чином період муарної решітки стає меншим.



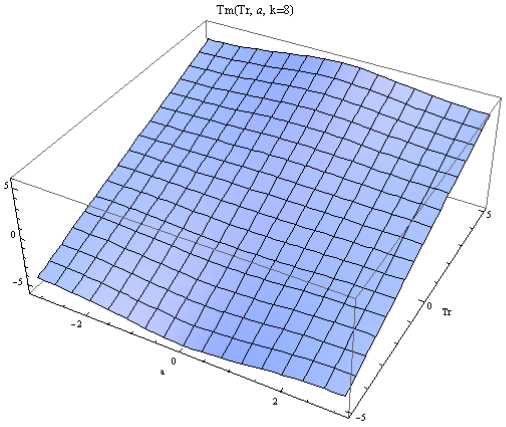
а



б



в



г

Рисунок 3.32. Залежність періоду зміни муарної решітки T_m від кута нахилу α_b

3.3.5. Формування муару на основі зміни товщини ліній

Товщина ліній базового шару на l* більша за товщину допоміжного шару, отже $T_b = T_b + l^*$.

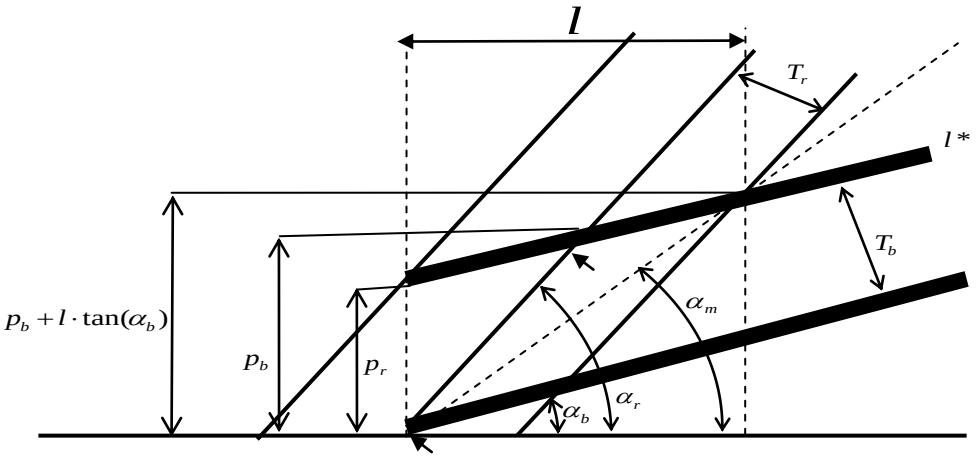


Рисунок 3.33. Товщина ліній одного шару на l* більша за інший.

З формули (3.4) випливає:

$$\tan \alpha_m = \frac{(T_b + l^*) \cdot \sin \alpha_r - T_r \cdot \sin \alpha_b}{(T_b + l^*) \cdot \cos \alpha_r - T_r \cdot \cos \alpha_b} \tag{3.22}$$

З формули (3.1) отримуємо:

$$p_m \cdot = \frac{p_b \cdot p_r}{p_b - p_r} . \tag{3.22}$$

Звідси:

$$T_m \cdot = \frac{(T_b + l^*) \cdot T_r \cdot \cos \alpha_m}{(T_b + l^*) \cdot \cos \alpha_r - T_r \cdot \cos \alpha_b} \tag{3.23}$$

Підставивши в формулу (3.6) отримуємо:

$$\cos \alpha_m = \sqrt{\frac{(T_b + l^*) - T_r}{(T_b + l^*)(\cos \alpha_r - \sin \alpha_r) - T_b}} \tag{3.24}$$

Звідси випливає, що:

$$T_m \cdot = \frac{(T_b + l^*) \cdot T_r \cdot \sqrt{\frac{(T_b + l^*) - T_r}{(T_b + l^*)(\cos \alpha_r - \sin \alpha_r) - T_b}}}{(T_b + l^*) \cdot \cos \alpha_r - T_r} \tag{3.25}$$

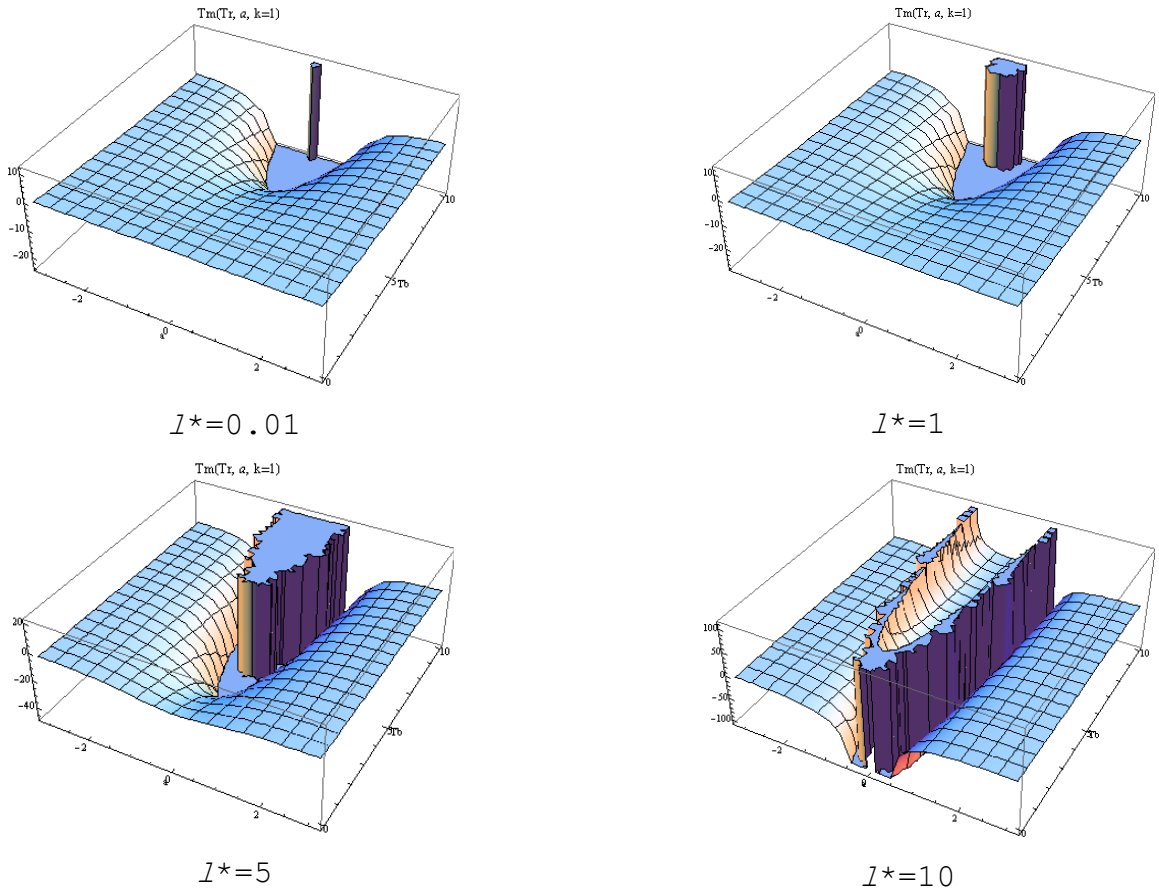


Рисунок 3.34. Залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару $Tb \in [0,10]$

Для даного способу проведено експериментальні дослідження для T_m - період зміни муарної решітки , α_b - кут нахилу решітки та періоду базового шару Tb при значеннях *l*=0.01, l*=1, l*=5, l*=10*, див. рисунок 3.34. Доведено, що чим більший період базового шару, тим більш помітним є муар. Тому використовуючи збільшення товщини однієї з ліній досягаємо збільшення видимості муару. Таким чином здійснюється підвищення захисту документів з використанням цього способу формування та винекнення муару утворюючи ГП в документах чим підвищують рівень захищеності.

Приховані елементи утворюються на основі використання ефекту муару, який утворюється двома структурами паралельних ліній. Ще більш складнішими для підробки, а отже і більш надійними є елементи, утворені суміщенням двох паралельних структур ліній зі зміною кутів нахилу. Утворені приховані елементи під час фальсифікації стають видимими і таким чином

можна визначити підробку. Розроблений метод формування графічних пасток на основі муару є ефективним і складним для підробляння, у процесі створення копії документу муар стає видимим і візуально спотворює документ. Результати роботи можна використовувати для захисту друкованих документів, що потребують ефективного захисту та подальшу ідентифікацію.

Висновки до розділу 3

1. Для реалізації процесів формування прихованих зображень, представлених у розділі 3 розроблені відповідні алгоритми і методи їх формування. Розроблена система формування прихованих зображень, на основі запропонованих методів дозволяє представити процеси з моменту формування до визначеності захищеного документа.
2. Розроблено та реалізовано метод тонкої графіки, призначений для моделювання збурень ліній. Вдосконалено векторний метод для захисту друкованих документів, що ґрунтується на використанні математичного апарату, який створює захисні елементи на основі формування тонкої графіки. На основі даного методу видано пат. «Спосіб захисту друкованих та електронних документів».
3. Вдосконалений метод формування латентних елементів на основі фракталів для побудови математичної моделі на основі змін дозволяє підвищити захисні характеристики документу та зменшити кількість фальсифікацій. Вперше розроблено метод формування фрактальних елементів, в яких вибір параметрів генерації фракталу залежить від ступеня необхідного захисту: створення сіток на основі однотипних фракталів; створення сіток на основі двотипних фракталів; створення сіток на основі патерну.
4. Враховуючи всі особливості методу муароутворення, для вирішення поставлених в дисертаційній роботі завдань за основу було вибрано класичний метод формування муру, оскільки він підходить для переважної більшості випадків виявлення спотворень в зображеннях та є відносно простим. На основі розроблених методів запропоновано систему формування зображень з прихованим муаром, що дозволяють виявляти деформацію в латентному зображенні.

РОЗДІЛ 4 ІНФОРМЦІЙНА ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ ЛАТЕНТНИХ ЗОБРАЖЕНЬ В ДОКУМЕНТАХ

У четвертому розділі створено інформаційну технологію розроблення та ідентифікації латентних зображень в документах. Здійснено експериментальний збір та дослідження зразків оригіналу та копії для проведення експериментів. Були проведені та описані експерименти для тестування зібраних зразків на різних видах паперу, зокрема показано результати визначення параметрів оригінальних документів та копій; визначено коефіцієнти ефективності захисту документів; здійснено порівняльні характеристики додрукарських процесів на різних видах паперу відносно оригіналу та підробки (копії).

4.1. Розроблення методу ідентифікації латентних зображень в документах

Для підвищення захисту документів потрібно не тільки розробити захисні елементи, а також здійснити ідентифікацію цих елементів за певними критеріальними ознаками чи експертними оцінками. На даному етапі ідентифікації документів можна запровадити певні автоматизовані процеси, коли система сама може визначити чи документ оригінальний чи підроблений. Таким чином зможемо уникнути неточності визначення оригінальності документа використовуючи лише знання експерта. Для ідентифікації використовується захищене латентне зображення, яке відтворюється репографічними засобами без спотворень та спотворене зображення, яке виникло в процесі оцифровування (частина зображень є видозміненою).

З метою ефективного впровадження та тестування розробленої інформаційної технології аналізу та прогнозування підробки документів, було розроблено модель контролю латентних зображень в документах.

Розроблено метод виявлення прихованої інформації, який реалізує перетворення латентного зображення і дозволяє, на відміну від відомих методів, виявити приховане зображення незалежно від конкретної моделі

формування, на основі запропонованої математичної моделі виявлення прихованої інформації в латентних зображеннях. Запропонована модель скоротила обчислювальну складність виявлення прихованої інформації, що дозволило підвищити контроль латентного зображення, незалежно від способу впровадження прихованої інформації [99].

На основі запропонованих методів розроблено технологію формування та ідентифікації латентних зображень, що дозволяє, здійснити процес від моменту формування до визначення автентичності захищеного документа, що відрізняється від відомих тим, що передбачений контроль латентних зображень, як при відомому, так і при невідомому методах впровадження прихованих зображень [96].

Для виявлення латентних зображень використовуються методи, засновані на Фур'є-аналізі, методах фільтрації зображень, а також методи перетворення зображення, засновані на способах впровадження прихованих зображень [112, 113, 116-119].

Для розробки методу ідентифікації, який не буде залежати від конкретного способу формування латентних зображень, сформованих різному орієнтованими структурами або утворених структурами, що формуються на основі описаних методів та моделей в розділі 2 та 3.

Поставлене завдання вирішується за допомогою того, що для оперативного контролю якості застосовуються денситометри, тобто виконується непряма кількісна оцінка критеріїв відтворення кольору. В якості таких критеріїв рекомендується вибирати баланс по сірому і колориметричні показники, інакше буде важко отримати передбачуваний результат.

Спектрофотометрична система порівнює координати вимірюваного і еталонного документів, відображаючи процес порівняння у вигляді графіка, а значення оптичної щільності розраховується математичною формулою. Програмне забезпечення таких систем включено в бази даних стандартних (наприклад, з ISO 12647) [157 - 160] колірних координат. При вимірі завжди враховуються колірні координати паперу, адже і оригінальний і

фальсифікований документ створено з використанням одного виду паперу, але з різними інформативними характеристикамим, які відрізняються на оригіналі та копії.

Колірні характеристики документу поелементно перетворюються в кольоровому просторі *RGB*, потім в *Lab*, що відповідає етапами процесу кольоровідтворення [126-128].

Використовуючи модель репродукційного процесу здійснюємо перетворення колірної інформації. Нехай X – координати елементів зображення, тоді O – набір координат пікселів зображення, $v = \left\{\Phi_i^j, \Psi_i^j\right\}$ - це профілі пристроїв, що відображаються як Φ_i^j і Ψ_i^j, а також здійснюють пряме й зворотне перетворення між колірними просторами *i*-го пристрою для *j*-ої мети передачі кольору; нехай ε – похибка колірних градієнтів; тоді приймемо, що U – градаційні перетворення - кольорокорекція; а спектральні характеристики та колірні координати точки білого УФ позначено як С; припустимо, що M – характеристики фарби та паперу $M = (M_1, M_2)$; позначимо F – оператор, що описує технологічний процес; та параметр Q буде визначати оцінку якості кольоровідтворення.

Формула може бути представлена у вигляді наступних співвідношень:

$$S = < X, O, v, \varepsilon, U, C, M, F, Q > \tag{4.1}$$

$$\begin{cases} X = F(O, v, U, C, M), \quad X = \{L_i, a_i, b_i\}_{i=1,\ldots,m} \\ O = \{R_i, G_i, B_i\}_{i=1,\ldots,n} \\ v = \{v_i\}_{i=1,\ldots,k}, \quad v_i = \left\{\Phi_i^j, \Psi_i^j\right\}_{j=1,\ldots,3} \\ M = (M_1, M_2), \quad M_1 = \left\{\hat{X}_{т.б.}, \hat{Y}_{т.б.}, \hat{Z}_{т.б.}\right\}, \quad M_2 = \{\beta(\lambda_i)\}_{i=1,\ldots,N} \\ C = (\tilde{C}, \overline{C}), \quad \overline{C} = \left(\bar{x}(\lambda), \bar{y}(\lambda), \bar{z}(\lambda)\right), \quad \tilde{C} = \left\{C_j\right\}_{j=1,..,N}, \text{ де } C_j = \{S_i(\lambda)\}_{i=1,\ldots,34} \\ Q = P(X, X^*) \to \min\limits_X \end{cases}$$

Для досягнення поставленої мети в роботі запропоновано створення технології, яка включає методи і алгоритми, які повинні задовольняти ряд вимог щодо швидкодії та точності. Розв’язання задач ідентифікації інформації

визначається розробленням технологій обробки, аналізу і розпізнавання різних видів зображень.

Розроблений метод ідентифікації полягає у наступному: збільшується різкість границь захисних елементів, здійснюється приведення до єдиного масштабу, зображення бінаризується, здійснюється ідентифікація шляхом порівняння з еталонною моделлю. За допомогою спектрофотометра та денсометрометра порівнюються координати колірного простору *RGB* і координати *Lab*, що на основі тестової шкали представляє собою вибірку з колірного простору пристрою, які занесені в базу даних створених латентних елементів.

У метричному просторі *Lab* колірну відмінність ΔE_{00}^{12} (CIEDE2000) – відстань між двома зразками $\left\{L_i^* a_i^* b_i^*\right\}_{i=1}^2$ визначено як:

$$\Delta E_{00}^{12} = \sqrt{\left(\frac{\Delta L'}{k_L \cdot S_L}\right)^2 + \left(\frac{\Delta C'}{k_C \cdot S_C}\right)^2 + \left(\frac{\Delta H'}{k_H \cdot S_H}\right)^2 + R_T \left(\frac{\Delta C'}{k_C \cdot S_C}\right) \cdot \left(\frac{\Delta H'}{k_H \cdot S_H}\right)}, \qquad (4.2)$$

де $\Delta L', \Delta C', \Delta H'$ – різниця між зразками за оптичною щільністю, процентом розтиснення фарби та растрової точки;

Визначення залежності між колірними характеристиками *RGB* і *Lab* для всіх точок відповідності може бути сформульована наступним чином: нехай визначено набір *N* залежностей від $\{R_i, G_i, B_i\} \in RGB$, $i=1,\ldots,N$, отриманих у процесі вимірювання, і відповідний набір від зразків $\{L_i, a_i, b_i\} \in Lab$, $i=1, \ldots, N$.

Знаходимо аналітичну залежність, що описує пряме перетворення $\Phi: RGB \to Lab$ і зворотне перетворення $\Psi: Lab \to RGB$:

$$\begin{cases} L = \varphi_L(R,G,B) \\ a = \varphi_a(R,G,B), \\ b = \varphi_b(R,G,B) \end{cases} \qquad \begin{cases} R = \psi_R(L,a,b) \\ G = \psi_G(L,a,b). \\ B = \psi_B(L,a,b) \end{cases} \qquad (4.3)$$

Для зворотнього перетворення $\Psi : Lab \to RGB$ вирішується задача побудови формування та порівняння даних $R = \psi_R(L,a,b), G = \psi_G(L,a,b), B = \psi_B(L,a,b)$. Через різницю у формі колірних точок визначається процент спотворення зображення і таким чином експерт може з0робити висновок чи документ є оригінальним чи це фальсифікат.

Нехай x – множина абсциз сканованого зображення $x = \{x_1, x_2, x_3, ..., x_N\}$, тоді $y = \{y_1, y_2, y_3, ..., y_N\}$ – множина відповідних ординат, а $\bar{y} = \{\bar{y}_1, \bar{y}_2, \bar{y}_3, ..., \bar{y}_N\}$ – множина відповідних ординат еталону. Вважаємо що y - це скановане зображення, тоді еталоном буде $\bar{y}$.

Ідентифікація здійснюється при при порівнянні еталону з отриманим документом. На етапі розпізнавання латентного зображення, яка вимагає верифікація зображень. Нехай P_i P_j - це міри подібності двох зображень, тоді метрику $\mu(P_i\ P_j)$ в просторі зображень G з полем зору D. Визначення міри $\mu_0 = \mu(P_0,\ P_j)$ у випадку збіжності зображень, використаний кореляційний критерій означає знаходження перетворення $g \in G$, для якого $|\ \mu_0,\ \mu_g| < \varepsilon$. Класичною мірою ідентичності є визначення максимуму функції:

$$\mu_g = \frac{\sum\limits_{(x,y)\in D} P(x,y)P_0(x,y)}{\sqrt{\sum\limits_{(x,y)\in D} P^2(x,y)}\sqrt{\sum\limits_{(x,y)\in D} P_0^2(x,y)}} \to \max_{g\in G} \quad (4.4)$$

Припустимо, що P_0 позначення еталонного зображення, тоді P_g міра зображенням позначатимемо μ_g.

Для визначення подібності використовується класична задача пошуку кореляційного максимуму $\mu_g \to \max$. Тоді міра подібності визначатиметься метрикою

$$\rho_g = \left|\left|\mu_g\right| - 1\right| \quad (4.5)$$

При значенні коефіцієнта кореляції рівним

$$\mu_g = \frac{\sum_{i=1}^{N} y_g(x_i) y_0(x_i)}{\sqrt{\sum_{i=1}^{N} y_g^2(x_i)} \sqrt{\sum_{i=1}^{N} y_0^2(x_i)}}, \qquad (4.6)$$

де $y_g(x_i) y_0(x_i)$ – ординати точки з абсцисою x_i вхідної та еталонної кривої відповідно, $x_i \in [0; 2\pi]$, N – розмірність простору ознак.

Результатом роботи П буде результат у вигляді відсотків, який визначається за міра подібності ε між значеннями μ_0 і μ_g еталонного та сканованого зображень:

$$k = \left|1 - \frac{\varepsilon}{\mu_0}\right| \bullet 100\% = \left|1 - \frac{|\mu_0 - \mu_g|}{\mu_0}\right| \bullet 100\% . \qquad (4.7)$$

Такий метод ідентифікації використовується для попіксельного порівняння даних в документах для розпізнавання інформація, яка була спотворена чи сфальсифікована. На даному етапі є проблема визначення достовірності документів, тому запропоновано використовувати метод повного попіксельного порівняння зображень. Нехай $P_0(x, y)$ це оригінальне зображення, тоді $P(x, y)$ буде спотворене зображення. Приймемо, що зображення є розміром $m_p n_p$ пікселів. $MaxP$ – максимальна кількість градацій сірого. Коефіцієнт PSNR визначить чи зображення оригінальне чи ні, що обчислюється за формулою

$$PSNR = 10 \log_{10} \frac{MaxP^2 m_p n_p}{\sum_{x=1, y=1}^{m_p n_p} \left(P(x, y) - P_0(x, y)\right)^2}, \qquad (4.8)$$

Даний метод ідентифікації за допомогою PSNR дозволяє програмі попіксельно визначити чи документ підроблено та дати висновок щодо латентного зображення.

4.2. Інструментальні засоби розроблення та встановлення достовірності

З метою перевірки та визначення якисних показників розробленої інформаційної технології ідентифікації документів було проведено експериментальні дослідження. На основі розроблених методів запропонована система формування і контролю латентних зображень.

Сукупність методів і алгоритмів, що дозволяють впровадити одне зображення в інше являє собою структурну схему інформаційної технології.

Розроблено програмний модуль формування латентного зображення, що дозволяє на основі двох зображень: вихідного і прихованого створити латентне зображення. Програмний модуль розроблений на основі алгоритму, представленого на рисунку 4.1, побудованого на основі моделі, описаній в розділі 2 дисертаційного дослідження.

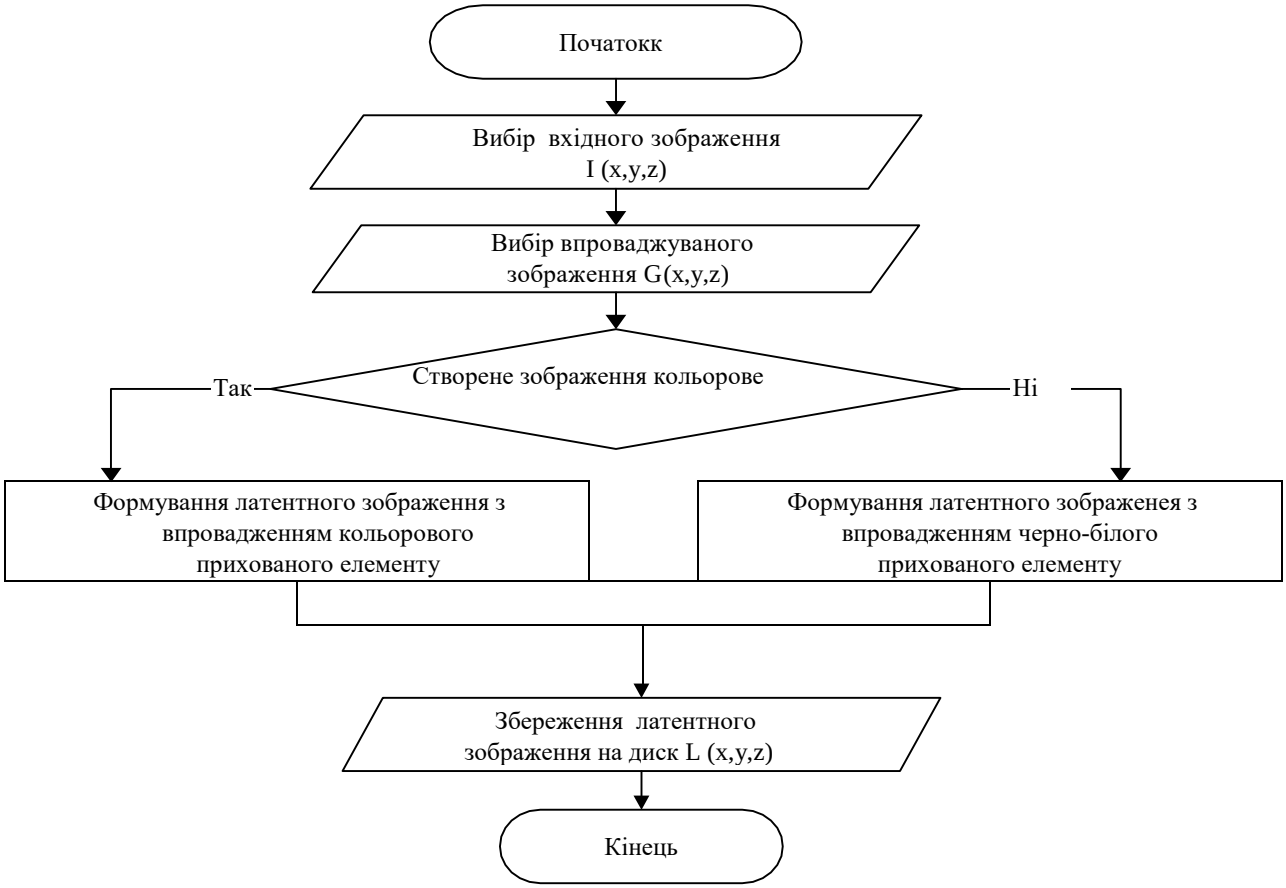


Рисунок 4.1 – Алгоритм формування латентного зображення

Прямими перетвореннями є перетворення, які не залежать від попередніх трансформацій. До таких перетворень відносяться: процес формування латентного зображення; перетворення латентного зображення в ході передачі; процес виявлення прихованого зображення - способом не залежним від способу формування. Під зворотним перетворенням розуміється перетворення, що описує процес виявлення прихованого зображення на основі способу зворотного способу формування латентного зображення. Під формуванням латентного зображення за допомогою системи розуміється процес прямого графічного перетворення.

Створено та реалізовано інформаційну технологію розроблення ЛЗ та ідентифікації цих елементів для підтвердження достовірності друкованих документів. Розроблена технологія передбачає, що кожному документу, який потребує захисту надаються захисні ознаки в залежності від рівня захищеності документа. Розроблена модель передбачає захист документів, які перебувають в обігу. Розроблено нові методології формування латентних зображень з використанням тонкої графіки, фрактальних захищених елементів, створення муару для захисту документів від фальсифікації. Для побудови захисних елементів, які накладаються на документ, розроблено інформаційну технологію, що ґрунтується на сумісному використанні розроблених моделей та методів формування латентних зображень за допомогою графічних елементів. На рисунку 4.2 зображено структуру інформаційної технології формування та ідентифікації латентних зображень в документах.

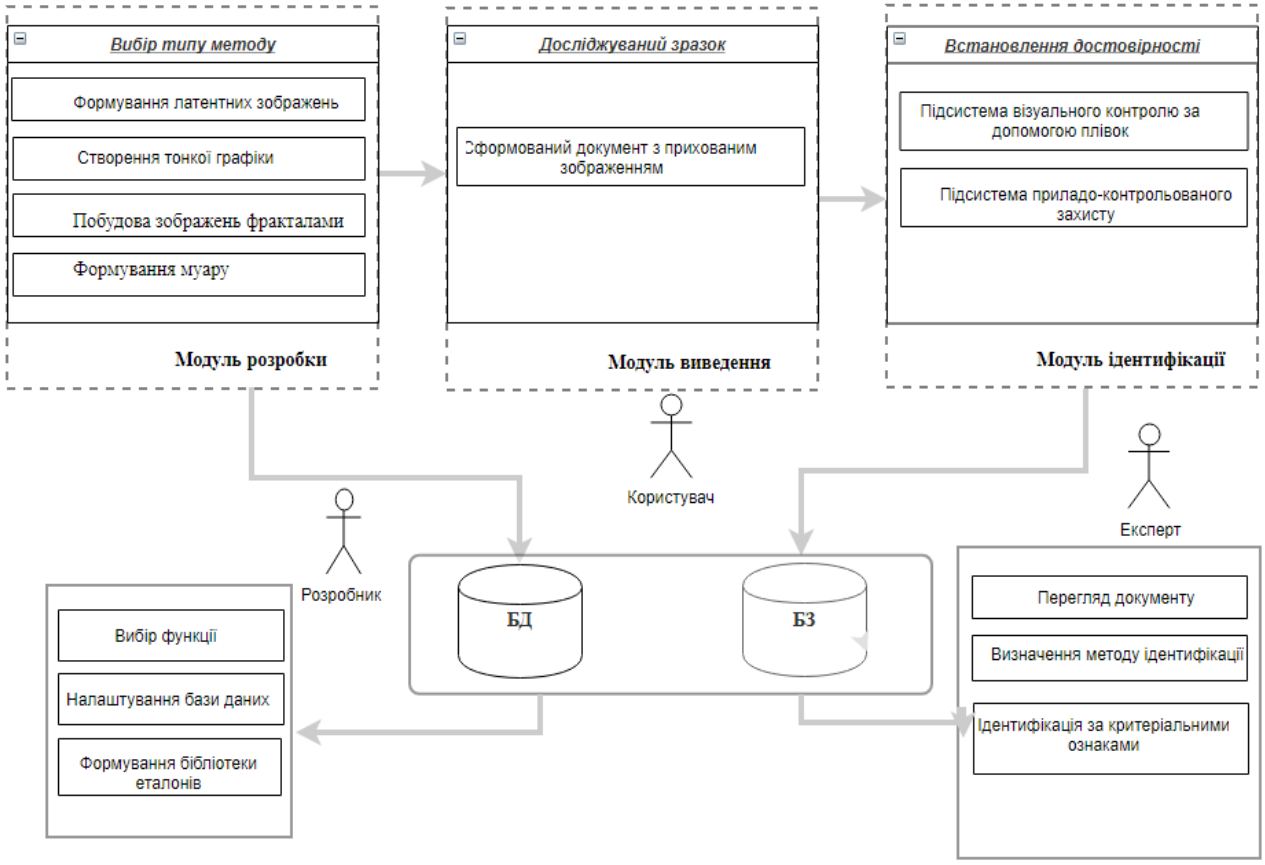


Рисунок 4.2. Структурна схема інформаційної технології розроблення та ідентифікації латентних зображень

Розроблена інформаційна технологія надає документам додаткових властивостей, базується на ролевій моделі керування доступом до даних, розрізняє рівні атрибутів документів, забезпечує цілісність даних, що дозволяє зменшити можливості підробки документів. Кожен з методів виступає критерієм підсистеми для визначеності ефективності розроблення інформаційної технології.

Алгоритм: розробник отримує вхідний документ, з якого зчитує текстову, табличну і графічну інформацію; розробник вибирає функцію захисту та генерує прихований одиничний елемент на основі методів тонкої графіки, латентних елементів, муаротворення та фракталів, врахувавши критерії вхідного документа. Розроблене приховане зображення заносить до бібліотеки еталонів та записує до бази даних; Формується приховане зображення, де поєднано в єдине ціле документ та прихований елемент.

Враховується формат та наповнення документа, а також розміщення прихованого зображення; Документ видруковується та надходить в обіг; Оригінальність документу підтверджує експерт з використанням плівок чи приладо-контрольованого пристрою. Експерт переглядає документ, визначає метод ідентифікації та за критеріальними ознаками встановлює оригінальність документа на основі невідповідності графічних елементів. Невідповідність між зображеннями значно полегшує визначення оригінальності, що дозволяє підвищити точність та пришвидшити процес ідентифікації. Розроблений метод ідентифікації документів було додано до існуючої бази з можливістю викликати необхідні функції оброблення даних прогнозування та ідентифікації прихованих зображень, а також було додано метод попіксельного порівнняння зображень на основі методу PSNR [129-131].

Для побудови захисних елементів, які накладаються на документ, розроблено технологію, що ґрунтується на основі сумісного використання графічних елементів та структурних характеристик латентних зображень. За цим принципом побудовано графічні елементи з нерегулярною структурою прихованих елементів, що становить серйозну перешкоду для імітації їх цифровими копіювальними пристроями. Розроблена технологія передбачає, що кожному документу, який потребує захисту надаються персоніфікуючі ознаки в залежності від рівня захищеності документа.

Розроблена інформаційна технологія надає документам додаткових властивостей, розрізняє рівні атрибутів документів, забезпечує цілісність даних, що дозволяє зменшити можливості підробки документів.

Структура інформаційної технології реалізована на основі графічних елементів для друкованих документів основне призначення яких забезпечити високу поліграфічну якість для документів та застерегти від фальсифікації. Для здійснення досліджень моделювання було розглянуто декілька найвідоміших середовищ комп’ютерного імітаційного моделювання, що дають змогу створювати оригінали та копії документів будь-якого типу з актуальними на сьогодні пристроями, а також такі, що дають можливість генерувати зразки

фальсифікації й можливість її виявлення. Реалізовано метод виявлення часткової підробки документів відбувається зміна кольору у області документа, де було здійснено зміни. Виявляється підробка для випадку здійснення фальсифікації документу. При візуальному спостереженні документа спостерігають такі дефекти: лінії пропадають; лінії у виходять грубими з нерівними краями; відбувається викривлення ліній; лінії налипають одна на одну і стають ширшими; лінії розпадаються.

Для реалізації процесів формування та контролю латентних зображень, представлених в структурній схемі інформаційної технології аналізу та ідентифікації документів, розроблені відповідні алгоритми та програмні комплекси, описані в розділі 4.

Очевидно, що інформаційна технологія ідентифікації документів з використанням графічних елментів дуже проста та дуже зручна для запрограмовування. Крім того, не потребує великої кількості вихідних даних, що означає, що програмна реалізація цього структурної схеми матиме високу швидкодію.

4.3. Експериментальне дослідження достовірності документа

У цьому підрозділі з метою проведення оцінювання ефективності розробленого методу формування та ідентифікації латентних зображень було здійснено порівняння результатів розробленого методу формування прихованих елементів, отриманих за допомогою методу латентності.

Сучасні методи контролю якості друку вимагають використання відповідної контрольно-вимірювальної техніки: денситометрів і спектрофотометрів. Для оцінки кольору найбільш об'єктивним є спектрофотометричний контроль, тому що він заснований на вимірюванні колориметричних координат на відбитках, у той час як денситометрично метод оцінює оптичні щільності барвистих шарів.

Одним зі спеціальних інструментів для визначення ідентифікації та

достовірності документа було використано денситометр та спектрофотометр ***x-rite spectroeye,*** який досліджує якість друкованої продукції та визначає оптичну щільність, чіткість відтворення, рівномірність розподілення фарби на відбитку та розтиснення.

Досліджувалися такі взірці паперів: CANSON калька Tracing Paper, 4CC з шовковими волокнами, 4CC каландрований, Sirio Pearl oyster shell, Самоклейка Optima, Folia 300 г Fotokarton, Папір картковий тиснений, Калька-Canson, Fedrigoni constellation jade riccio, Constellation ivory, Папір двостороннього крейдування Art-Tech Gold, Stardream peridot, Canon Plus Glossy II PP-201, Star Dream Moon Stoo.

4.3.1.Експериментальні дослідження застосовані до різних способів друку

Експеримент та обчислення були проведені за допомогою розробленого документу в якому було вбудовано прихований елемент. Зразки для проведення цього експерименту були отримані шляхом, описаним у попередньому підрозділі (елементи зображення методом тонкої, методом латентних елементів, методом створення фрактальних елементів та захисту на основі муароутворення). Ці елементи були поміщені на форму А4 формату. Було надруковано кожен документ на 14 взірцях паперу, опис яких приведено вище. Із оригіналів відбитків було здійснено копії. Копії були оцифровані та збережені в базі як фальсифікат, а оригінали поміщені у розряд еталонів.

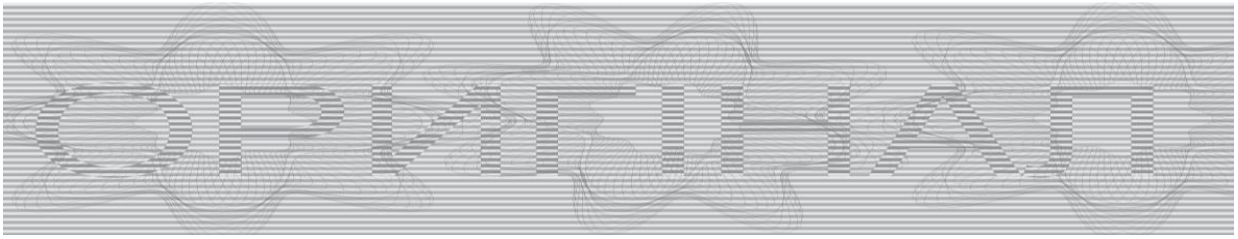
Провівши експериментальні дослідження було виявлено, що метод попіксельного порівняння оригінального документу та фальсифікату на основі використання програмного продукту, описаного в розділі 4.1 підвищив рівень ідентифікації від 10 до 40%.

4.3.2.Екперементальні дослідження з використанням спеціалізованого обладнання

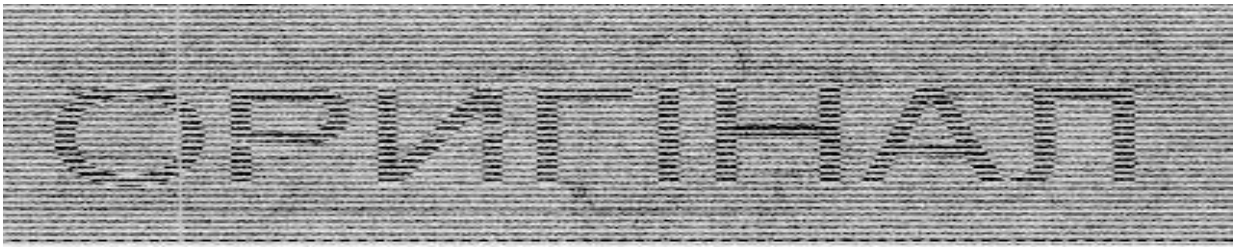
Досліджено друкований документ щодо оригінальності виведення на матеріальний носій інформації спектрофотометром SpectroEye, який поєднує в собі високу точність вимірювань. Ідентифікація показників досягається за допомогою вимірювань щільності, розтискування, площі растрової точки, треппінгу, контрасту. SpectroEye включає в себе колориметричні функції CIE *L*a*b** (за сертифікатом ISO 13655) [159] для точного контролю і вимірювання кольору, а також денситометричної функції.

Для оцінювання точності відтворення зображень часто застосовується візуальний контроль, що дозволяє одержати певні якісні характеристики. Тому виникла потреба у розробці інформаціної технології для оцінки якості кольоровідтворення й ідентифікації оригіналів та копій з точностю репродукування латентних зображень. Ідентифікацію документів було виміряно та експериментально досліджено спектрофотометром x-rite spectroeye. Проведено порівняльну характеристику латентних елементів. Пропонований спосіб забезпечує високу ступінь унікальності результату і дозволяє визначати наявність прихованого візерунка і відсутність ознак, характерних для підробки.

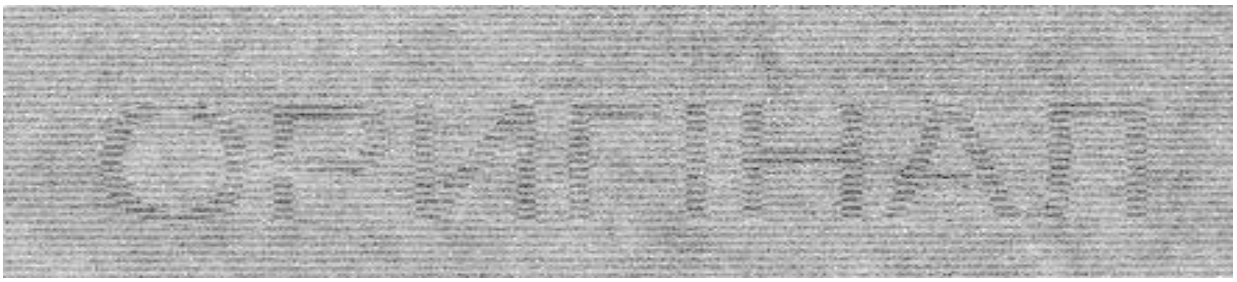
1. Оригінальний документ – еталон **I**.



2. Копія $\mathbf{I_1}$ – Еталон №7 (Folia 300 г Fotokarton)



3. Копія $\mathbf{I_2}$ – Еталон №11 (Constellation ivory)



4. Копія $\mathbf{I_3}$ – Еталон №13 (Stardream peridot)

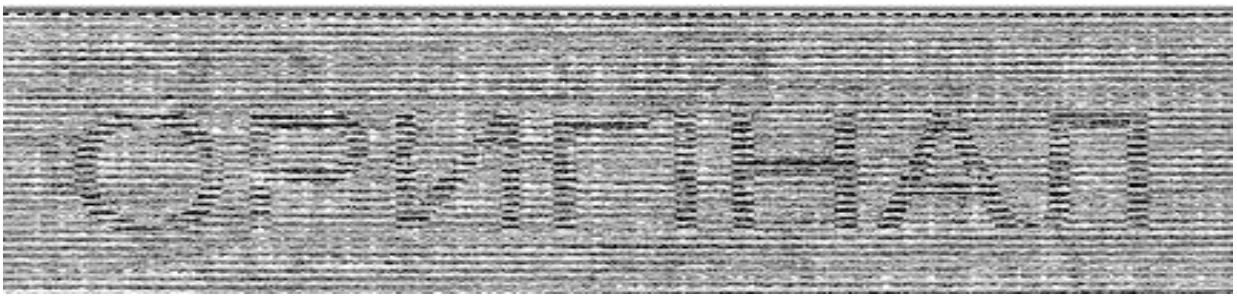


Рисунок 4.3. Приклади експерементальних зразків

В процесі растрування зображень формується регулярна растрова структура , в якій координати і величина кожного растрового елемента по заданій формулі зв'язуються з базовими величинами: кутом, лініатурою і тональною градацією, а також з додатковими величинами, які визначаються нестандартними змінами у куті, лініатурі та формі точок. Серед додаткових

величин можуть бути як постійні, що визначають лінійні спотворення по всьому зображенню, так і змінні, або випадкові, викликають складні і неоднорідні геометричні спотворення в різних його ділянках. В якості додаткової величини може використовуватися тональна градація відповідної ділянки зображення або інший інформаційний масив. В цьому випадку кінцеве зображення здатне містити й однозначно передавати додаткову приховану інформацію. Величина кожної точки визначається тональною градацією зображення і максимальною площею, яку вона може зайняти (визначається лініатурою). Тому геометричні спотворення лініатури проявляють себе освітленням або затемненням основного фону. При растуванні багатоколірних зображень для різних шарів встановлюються різні кути растрування, однакові базові (відповідно до правил растрування звичайних кольорових зображень) і всі додаткові величини.

В експерименті використано захисні елементи, а саме сформовані латентні зображення, які роздруковані на різних типах паперу для проведення дослідження. Результати експериментів приведені в таблиці 4.1., 4.2., 4.3., 4.4., а також представлено порівняльна характеристика растрової точки, трепінгу, оптичної густини, розтиснення в оригінальному документі та на копіях.

Порівняння растрової точки та проценту розтиснення в оригінальному документі та на копіях

Таблиця 4.1.

	Назва	% раст. точки	Копія 1	Копія 2	Копія 3
1	CANSON калька Tracing Paper	20	1.9	6.6	4.8
2	4CC з шовковими волокнами	46	5.2	3.6	2.6
3	4CC каландрований	50	8.5	1.5	1.3
4	Sirio Pearl oyster shell	74	8.2	5.9	1.4
5	Самоклейка Optima	69	7.9	3.5	1.2
6	Folia 300 г Fotokarton	62	11.4	2.2	7.6
7	Папір картковий тиснений	78	1.8	1.5	3.3
8	Папір двостороннього крейдування Art-Tech Gold	89	7.3	2.7	1.7
9	Fedrigoni constellation jade riccio	47	5.8	12.5	1.4
10	Constellation ivory	6	1.9	1.4	2.5

	Назва	Розтиснення, ΔG	Копія 1	Копія 2	Копія 3
1	CANSON калька Tracing Paper	80	7	12	8
2	4CC з шовковими волокнами	81	1	4	10
3	4CC каландрований	84	11	7	3
4	Sirio Pearl oyster shell	96	13	9	14
5	Самоклейка Optima	80	18	2	2
6	Folia 300 г Fotokarton	100	22	8	1
7	Папір картковий тиснений	99	16	10	3
8	Папір Art-Tech Gold	86	6	7	8
9	Fedrigoni constellation jade riccio	95	10	8	20
10	Constellation ivory.	87	15	14	11

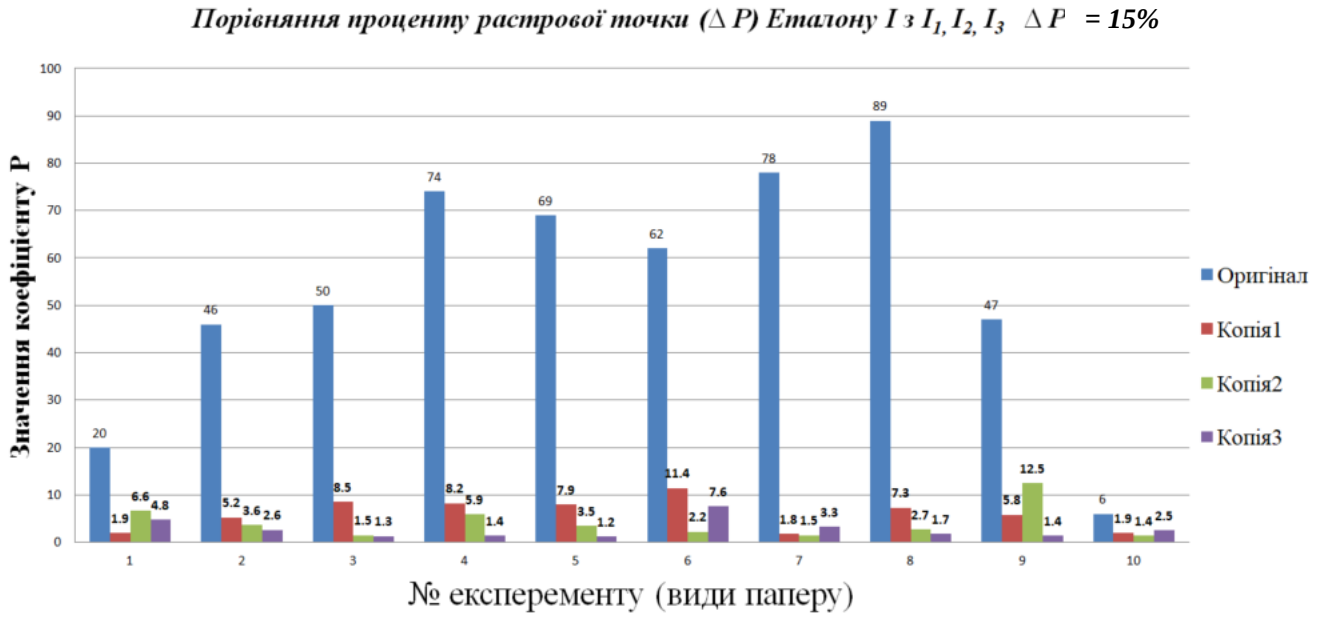


Рисунок 4.4. Порівняння експерементальних даних проценту раст. точки виміряних спектрофотометром ***x-rite spectroeye*** на оригінальному документі та копіях

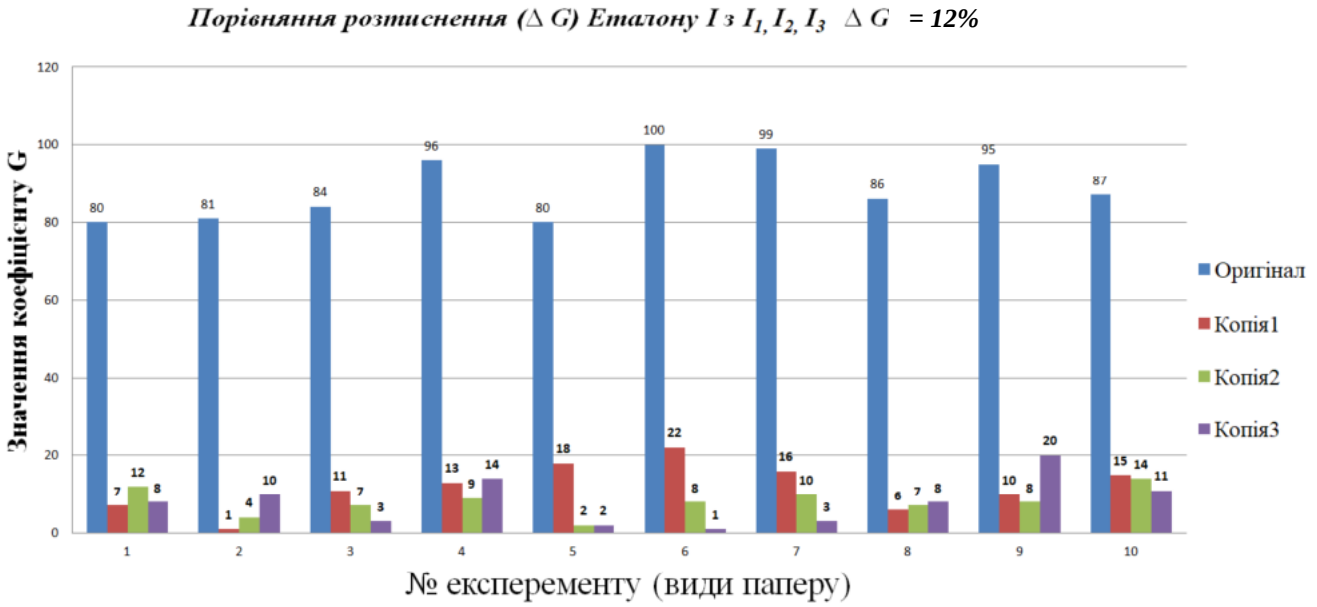


Рисунок 4.5. Порівняння експерементальних даних розтиснення виміряних спектрофотометром **x-rite spectroeye** на оригінальному документі та копіях

Порівняння трепінгу та оптичної густини в оригінальному документі та на копіях

Таблиця 4.2.

	Назва	Трепінг, ΔT	Копія 1	Копія 2	Копія 3
1	CANSON калька Tracing Paper	6.2	1.2	2.7	0.8
2	4CC з шовковими волокнами	7.4	0.6	1.7	0.2
3	4CC каландрований	9.5	2.9	0.7	0.3
4	Sirio Pearl oyster shell	9.4	2.8	0.6	1.4
5	Самоклейка Optima	4.5	0.9	0.8	0.2
6	Folia 300 г Fotokarton	7.8	1.2	0.2	0.7
7	Папір картковий тиснений	8.9	1.9	0.2	0.3
8	Папір Art-Tech Gold	7.7	1.9	1.6	1
9	Fedrigoni constellation jade riccio	8.5	2.7	3.2	0.4
10	Constellation ivory.	4.7	1.2	0.5	1.1

	Назва	Оптична густина, ΔR	Копія 1	Копія 2	Копія 3
1	CANSON калька Tracing Paper	28	6.2	3.2	2.7
2	4CC з шовковими волокнами	39	7.4	2.6	3.1
3	4CC каландрований	59	6.5	2.9	3.4
4	Sirio Pearl oyster shell	74	9.4	3.8	15.6
5	Самоклейка Optima	95	4.5	9.9	6.8
6	Folia 300 г Fotokarton	77	6.7	10.2	12.1
7	Папір картковий тиснений	68	7.8	2.8	12.2
8	Папір Art-Tech Gold	59	8.9	5.9	13.2
9	Fedrigoni constellation jade riccio	70	2.7	9.9	11.6
10	Constellation ivory.	89	8.5	38.7	13.2

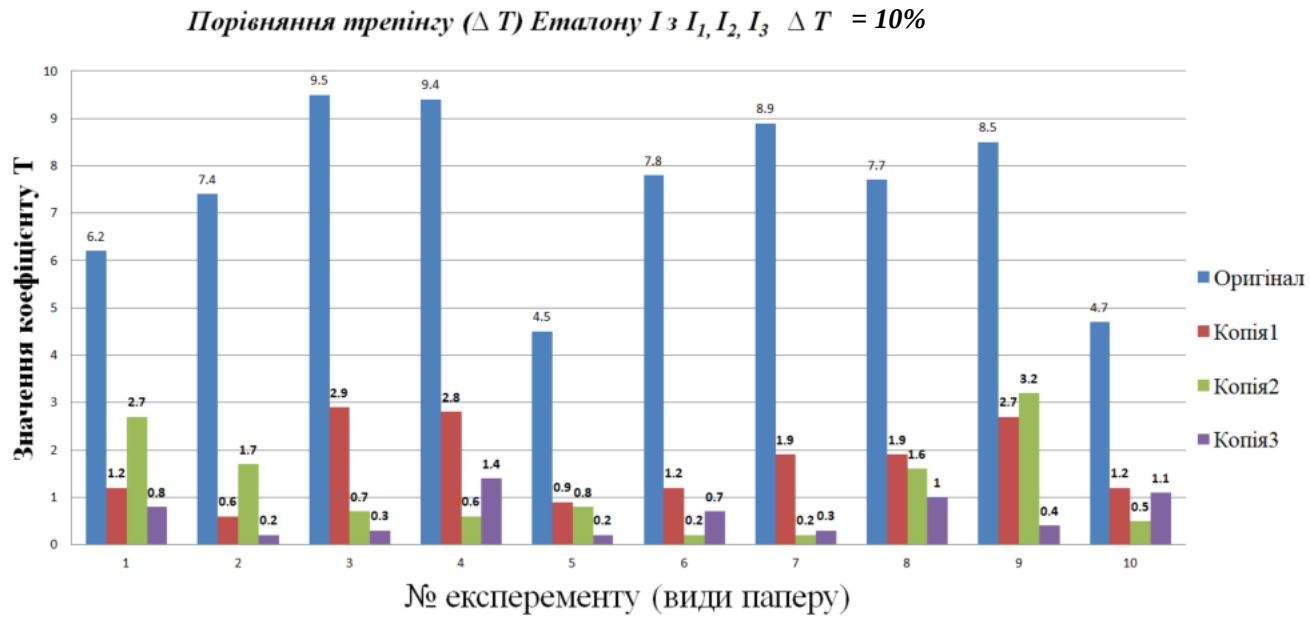


Рисунок 4.6. Порівняння експерементальних даних трепінгу виміряних спектрофотометром **x-rite spectroeye** на оригінальному документі та копіях

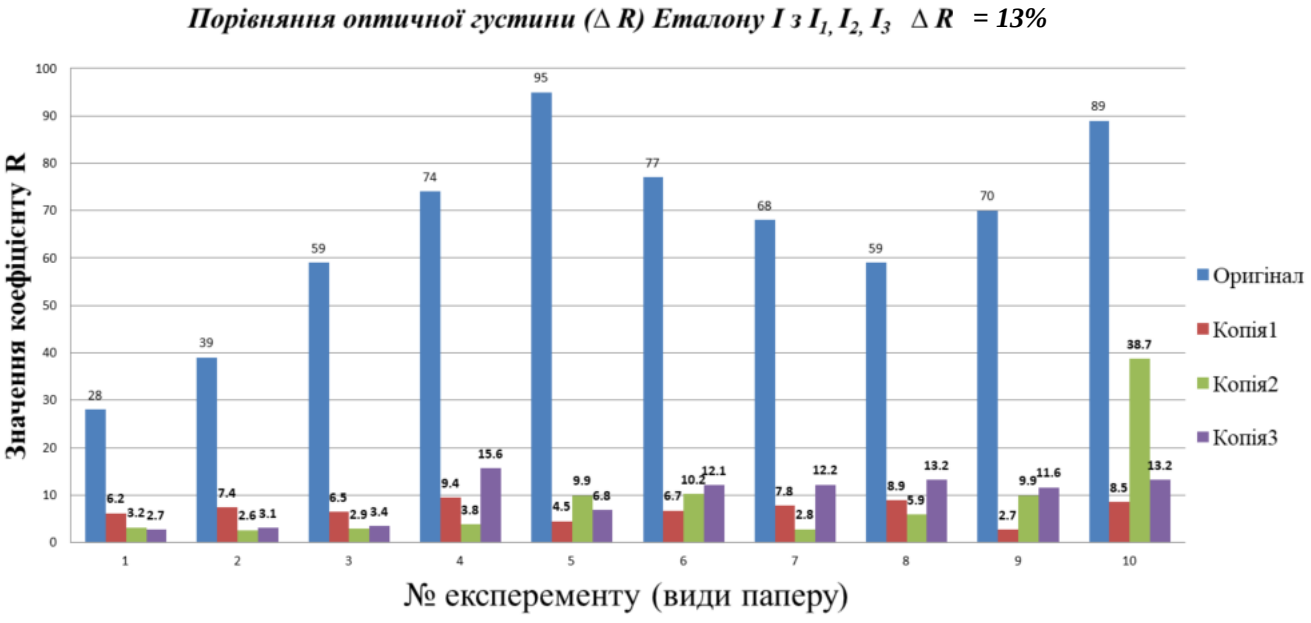


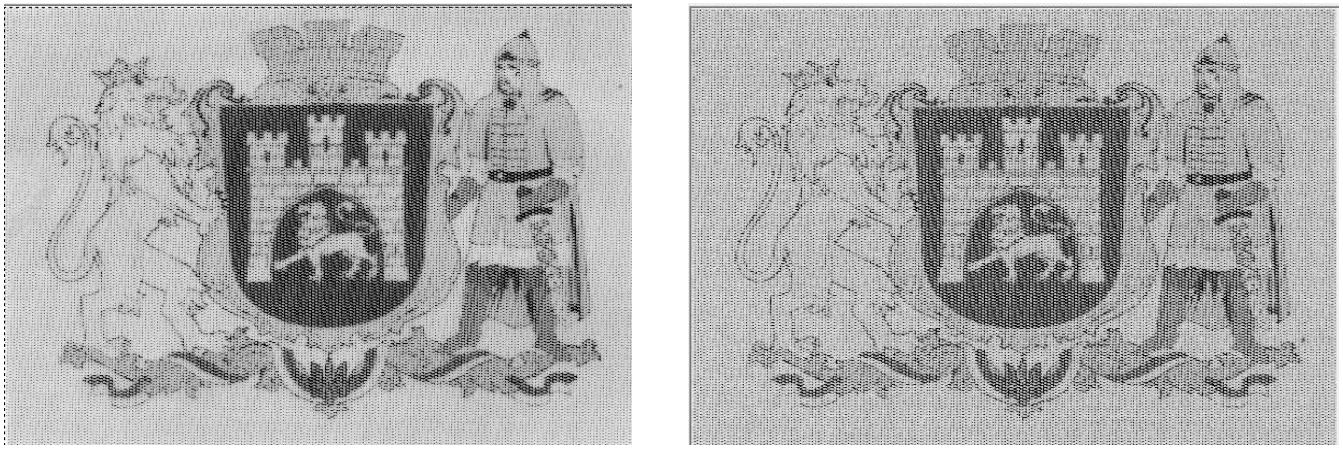
Рисунок 4.7. Порівняння експерементальних даних оптичної густини виміряних спектрофотометром ***x-rite spectroeye*** на оригінальному документі та копіях

Порівняльна характеристика ΔLab в оригінальному документі та на копії

Застосування друку з близькими по тональності або не просвічуваними барвниками робить неможливим відновлення оригінальних растрових сіток всіх застосованих кольорів на сканованому зображенні, а застосування барвників, не відтворюваних CMYK-пристроями, виключає можливість імітації за допомогою копіювальної техніки. Таким чином, даний спосіб забезпечує досить високий ступінь захисту, не вимагаючи застосування нестандартної техніки і дорогих матеріалів, що дозволяє широко використовувати його на практиці. При визначенні автентичності зразка слід звернути увагу на наступні моменти:

- ✓ наявність захисного зображення, його чіткість і відсутність муару;
- ✓ колірна відповідність барвників;
- ✓ відповідність способів растрування кожного кольору;
- ✓ правильну форму точок растра, відсутність ознак ретушування;

Для виключення можливості використання шаблону при фальсифікації поверх його растрової сітки наноситься текст або захисні знаки. Крім того, він не повинен містити зображення, може мати інший спосіб (і навіть кут) растрування. У більшості випадків оптимальним можна вважати 40% заповнення растром контрольної плівки. При цьому тональність барвника бажано підібрати так, щоб розбіжності були максимально помітні.



Оригінал – Еталон №4 (Sirio Pearl oyster shell) Копія – Еталон №4 (Sirio Pearl oyster shell)

Рисунок 4.8. Приклади експерементальних зразків

Експеремент проведено для порівняльної характеристики оригінального документу та фальсифікації в системі Lab. Досліди описано в таблиці 4.3.

Порівняння ΔLab в оригінальному документі та на копії

Таблиця 4.3.

	Назва	Оригінал			Фальсифікат		
		ΔL	Δa	Δb	ΔL	Δa	Δb
1	CANSON калька Tracing Paper,	88.81	42	24	99.89	12	12
2	4CC з шовковими волокнами	102	53	36	100	3.5	14.5
3	4CC каландрований	101.7	80	41	86.29	5.1	4.8
4	Sirio Pearl oyster shell	99.8	72	36	98.77	11.4	7.11
5	Самоклейка Optima	100	60	22	99.61	2.5	10.2
6	Folia 300 г Fotokarton	100	65	32	87.6	21.1	8.02
7	Папір картковий тиснений	108.6	42	37	95.13	12.1	5.31
8	Папір Art-Tech Gold	99.91	58	24	99.84	5.01	9.02
9	Fedrigoni constellation jade riccio	104	75	34	78.92	14.2	23.9
10	Constellation ivory.	97.64	59	37	73.8	13.4	22.63

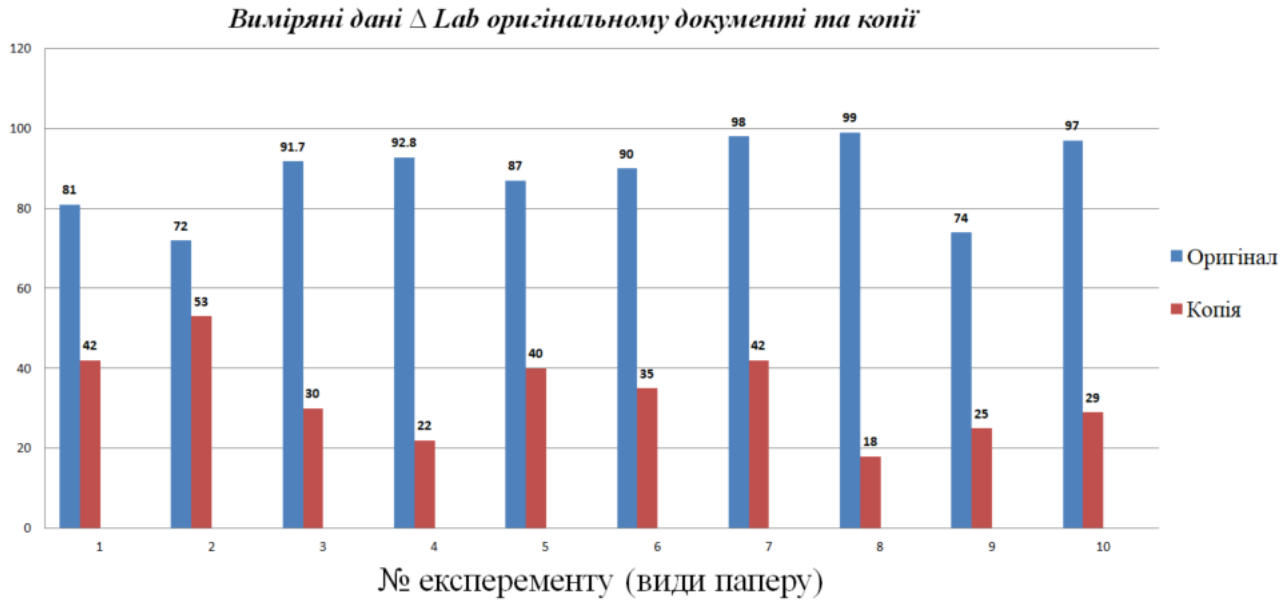


Рисунок 4.9. Порівняння експерементальних даних ΔLab виміряних спектрофотометром ***x-rite spectroeye*** на оригінальному документі та копіях

Порівняння тональності в оригінальному документі та на копії

Експеремент проведено для порівняльної характеристики оригінального документу та фальсифікації в тональності чорного 25%, 50%, 75%, 100%. Досліди описано в таблиці 4.4.

Таблиця 4.4.

	Назва	Оригінал				Фальсифікат			
		25%	50%	75%	100%	25%	50%	75%	100%
1	CANSON калька Tracing Paper	7.3	7.1	7.5	7.6	1.4	1.8	2.0	2.4
2	4CC з шовковими волокнами	5.2	5.8	6.1	6.2	1.0	1.1	1.2	1.3
3	4CC каландрований	6.9	7.1	7.5	7.9	3.1	3.3	3.5	3.8
4	Sirio Pearl oyster shell	7.8	8.2	8.4	8.8	1.1	1.4	1.6	1.7
5	Самоклейка Optima	7.2	7.6	7.8	8.2	1.1	1.9	2.0	2.1
6	Folia 300 г Fotokarton	4.1	4.5	4.9	5.1	3.2	3.8	3.9	4.2
7	Папір картковий тиснений	6.6	6.9	7.3	7.6	1.0	1.0	1.1	1.2
8	Папір Art-Tech Gold	7.9	8.1	8.5	8.9	2	2	2	2
9	Fedrigoni constellation jade riccio	8.1	8.5	8.9	9	3.1	3.3	3.5	4.1
10	Constellation ivory.	6.9	7.2	7.4	7.6	1.4	1.8	2.0	2.4

Рисунок 4.10. Порівняння експерементальних даних для оригіналу та копії

Експерименти та обчислення були проведені в рамках однієї моделі відтворення для аналізу зразків оригіналу та копії з прихованими елементами в документі. Зразки документів та латентних зображень для проведення цього експерименту були отримані шляхом, описаним у попередньому розділі.

На рисунку 4.9 представлено порівняння обох документів оригіналу та фальсифікату, а саме порівняння за відносним показником ΔLab та різницею метрик в оригіналі та меншою за стандартні метрики в ймовірній підробці. На рисунку 4.10 зображено середні значення тональності зібрані в різних процентних порогах.

Дані таблиць наочно ілюструють, що пристрої, які беруть участь в процесах відтворення кольору, працюють з апаратними даними аміряні в різних документах, що й дозволяє виявити фальсифікат. Це пояснює невідповідності кольоровідтворення між різними паперами та на оригіналі та копії.

У нашому випадку точність якості відбитків у документах має достатньо важливе значення, оскільки ми прагнемо підвищити ефективність використання латентних зображень.

Приховане зображення з поліпшеною якістю порівнюється з еталоном з контрольних зразків відповідним даного типу латентного зображення. При рівні відповідності прихованого зображення з еталоном вище порогового досліджуваний зразок визнається імовірно справжнім, інакше - починається послідовна перевірка:

1. Приховане зображення порівнюється з еталоном з контрольних зразків відповідним даного типу латентного зображення.

2. При рівні відповідності прихованого зображення з еталоном вище порогового досліджуваний зразок визнається ймовірно справжнім, і перевірка закінчується, інакше вибирається наступний прихований елемент і накладається на досліджуваний зразок. У разі, якщо досягнуто перевірки всіх прихованих елементів досліджуваний зразок визнається ймовірно підробленим.

Для проведення експериментів розроблений метод оцінювання

ефективності інформаційної технології відповідно до результату запропоновано критерій оцінювання параметрів, що впливають на ефективність. Прикладом використання гарантованого результату в області вимірювальної техніки є нормування похибок вимірювальних засобів за класами точності. Пропонований спосіб забезпечує високий ступінь унікальності результату і дозволяє визначати наявність прихованого візерунка і відсутність ознак, характерних для підробки (проведення експертизи займе мінімум часу).

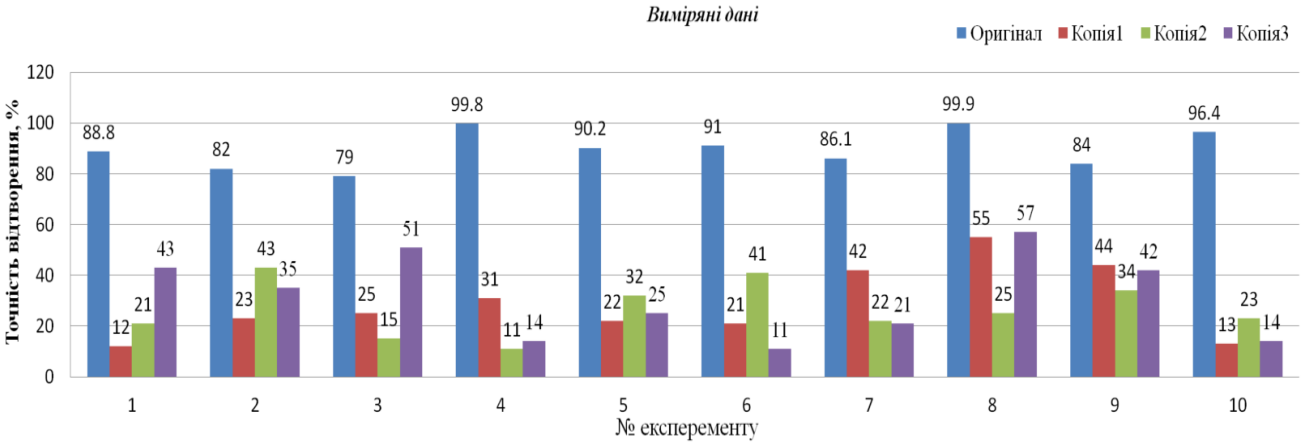


Рисунок 4.11 Порівняння розрбленого методу на оригіналі та копії

Згідно графіків, представлених вище, та таблиць результатів проведення експериментів можна зробити висновок, що методи формування латентних зображень з використанням тонкої графіки, фракталів та муароутворення дає кращі результати в виявленні фальсифікату та значно менші втрати документічв, ніж методи, які були розроблені раніше. Особливо помітною є різниця між цими методами на великих вибірках та на мільонних тиражах документів. Рисунок 4.11 підтверджує ефективність роботи методу ідентифікації латентних зображень, оскільки на основі аналізу отриманих результатів надано практичні рекомендації стосовно забезпечення достовірності друкованих документівта на основі аналітичної залежності оригіналу та копії знятої спектрофометричним приладом показників.

4.4. Розробка програмного модуля формування латентного зображення

Для проведення дисертаційного дослідження був розроблений програмний модуль на мові MATLAB формування латентного зображення, що дозволяє на основі двох зображень: вихідного і прихованого створити латентне зображення. Програмний модуль розроблений на основі алгоритму, представленого на рисунку 4.1, побудованого на основі моделі, описаній в розділі 2 дисертаційного дослідження.

Вікно програмного модуля створення латентного зображення (рисунок 4.2) включає в себе компоненти для вибору вихідного і впроваджуваного зображень (1), після вибору яких стає активною кнопка формування латентного зображення (2). Сформоване зображення з'являється у вікні попереднього перегляду (4). При задовільних результатах – латентне зображення можна «Зберегти» (3).

Програмний комплекс розроблений на основі структурно-функціональної моделі інформаційної технології аналізу та ідентифікації документів, яка описана в розділі 4.1. та складається з взаємопов'язаних програмних модулів:

1. Програмний модуль «Вибір типу методу формування латентного зображень».

2. Програмний модуль «Вибір функцій».

3. Програмний модуль «Побудова прихованого об'єкта в латентному зображенні».

4. Програмний модуль «Визначення достовірності документа по розпізнаному латентному зображенню».

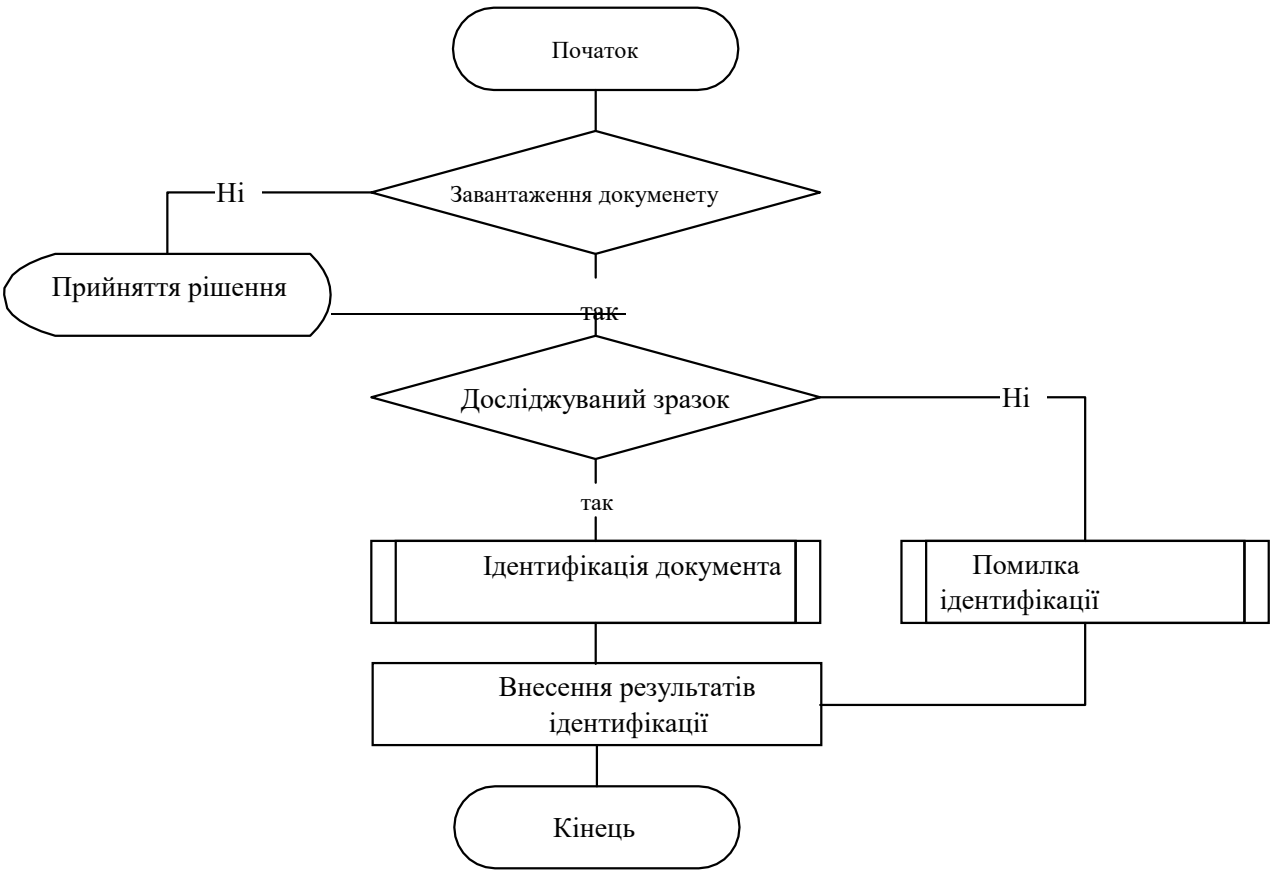


Рисунок 4.12 – Алгоритм приняття рішень

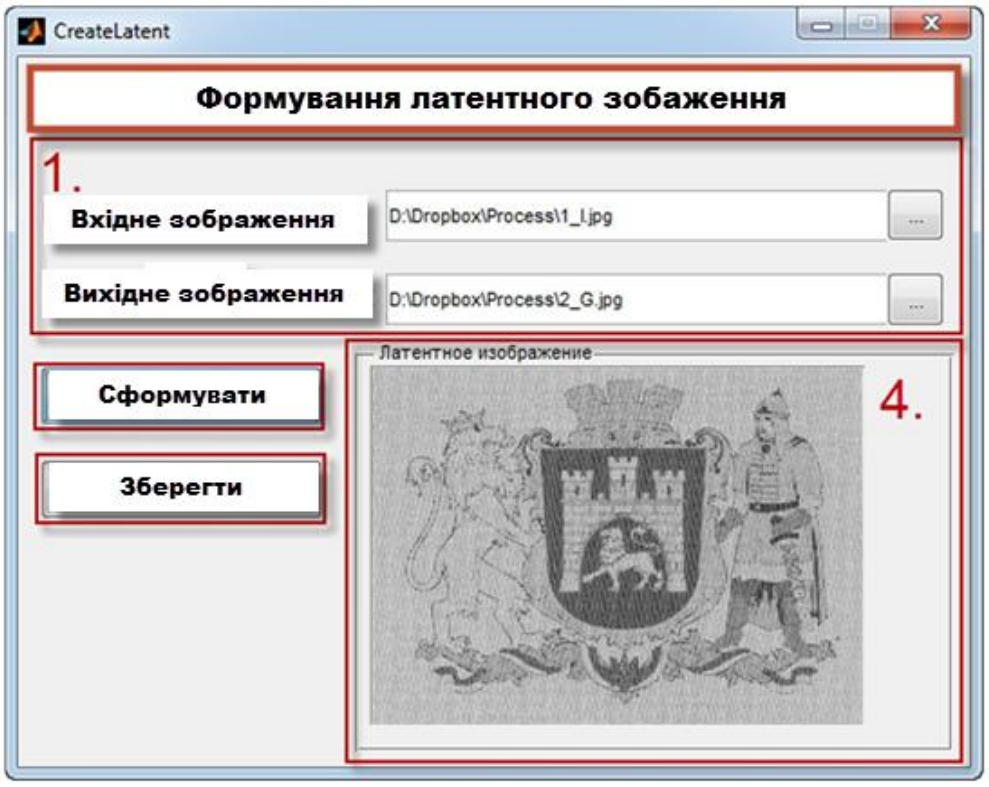


Рисунок 4.13. Вікно программного модуля формування латентного зображення

Розроблений програмний модуль дозволяє автоматично формувати латентне зображення на основі завантаженого основного і прихованого зображення. Розробка програмного комплексу контролю латентних зображень

Для вирішення задачі розпізнавання латентного зображення необхідно було вирішити наступні підзадачі:

1. Отримати придатне для розпізнавання латентне зображення. Зображення має зберегти свою структуру.

2. Визначити наявність прихованого зображення, і, відповідно, справжність документа.

3. Прийняти рішення про подальші дії на підставі результату визначення автентичності документа.

На рисунку 4.14 представлений узагальнений алгоритм вирішення задачі:

Рисунок 4.14 – Узагальнений алгоритм рішення задачі

Контрольовані зображення - це об'єкти, які виділяються в результаті аналізу на зображеннях, взятих в якості еталонних, і являють собою послідовність, яка використовується в подальшому для порівняння досліджуваних зображень з еталонними в модулі «Визначення достовірності документа».

4.5. Тестування розробленої інформаційної технології аналізу та ідентифікації документів

У цьому підрозділі для більш детального визначення параметрів ідентифікації латентних зображень було проведено імітаційне моделювання комп'ютерної програми з метою визначення того, як впливає застосування розробленого методу на визначення оригінальності документу.

Для перевірки роботи програми в режимі реального часу, з перевіркою проміжних результатів аналізувалися записи наступних типів: оригінальний документ – Еталон №4 роздрукований на папері Sirio Pearl oyster shell та фальсифікавана копія документу на якій не відображається приховане зображення з написом «оригінал».

Після запуску моніторингу починається захоплення зображення як описано в підрозділі 4.4 Програмний модуль «Визначення достовірності документа по розпізнаному латентному зображенню».

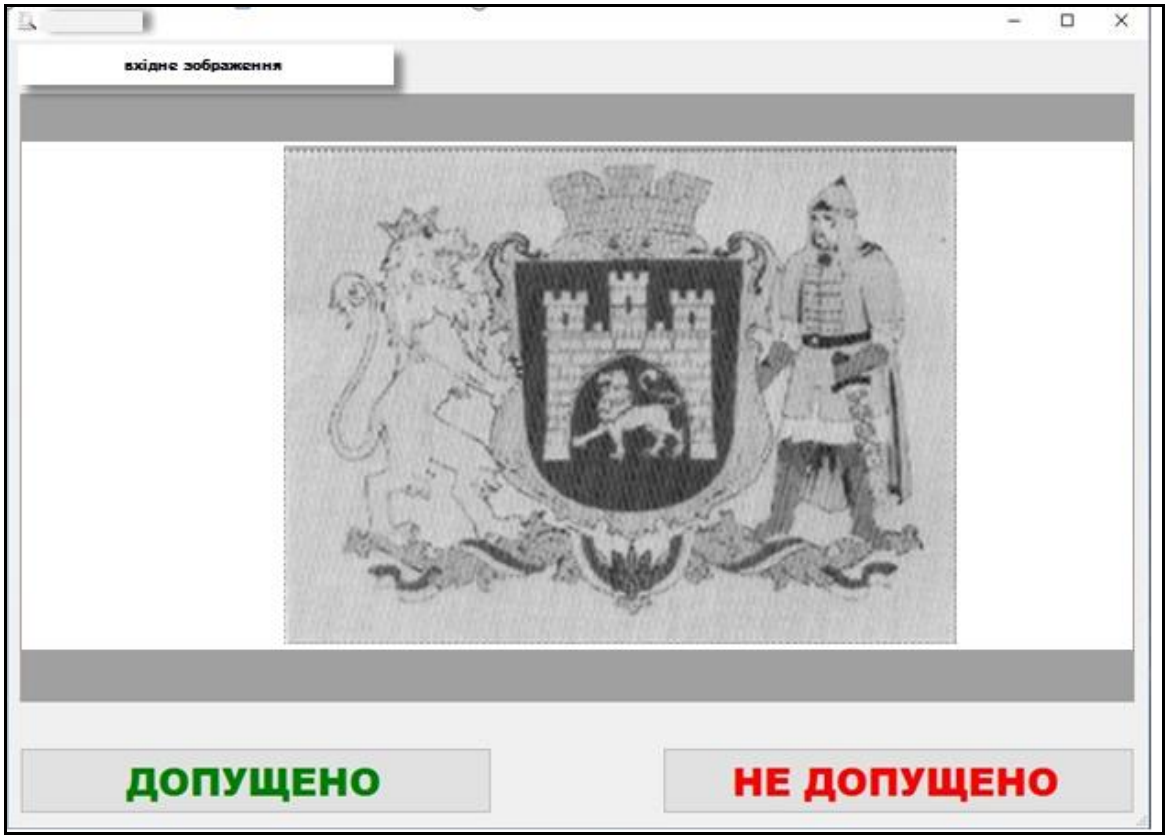


Рисунок 4.15. Завантажене латентне зображення з прихованим елементом

Дане ПЗ має велику базу даних готових прихованих елементів, які вже місять в собі алгоритми аналізу та етапів обробки вхідної інформації з врахуванням затрат часу та їх виконання реальними фізичними пристроями. По завершенню аналізу система визначає, що на досліджуваному зображенні виявлені приховані зображення (рисунок 4.14).

З'являється можливість переглянути оброблені різними способами з визначенням місця знаходження прихованих елементів зображення. Після чого прийняти остаточне рішення про правильність розпізнавання натисканням на кнопку «допущено» або «не допущено» (рисунок 4.16).

Вихідний код розробленого методу аналізу та ідентифікації документіав було додано до існуючої кодової бази моделей з можливістю викликати необхідні функції оброблення даних прогнозування та ідентифікації прихований зображень, а також було додано метод попіксельного порівнняння зображень на основі методу PSNR описаного в підрозділі 4.1.

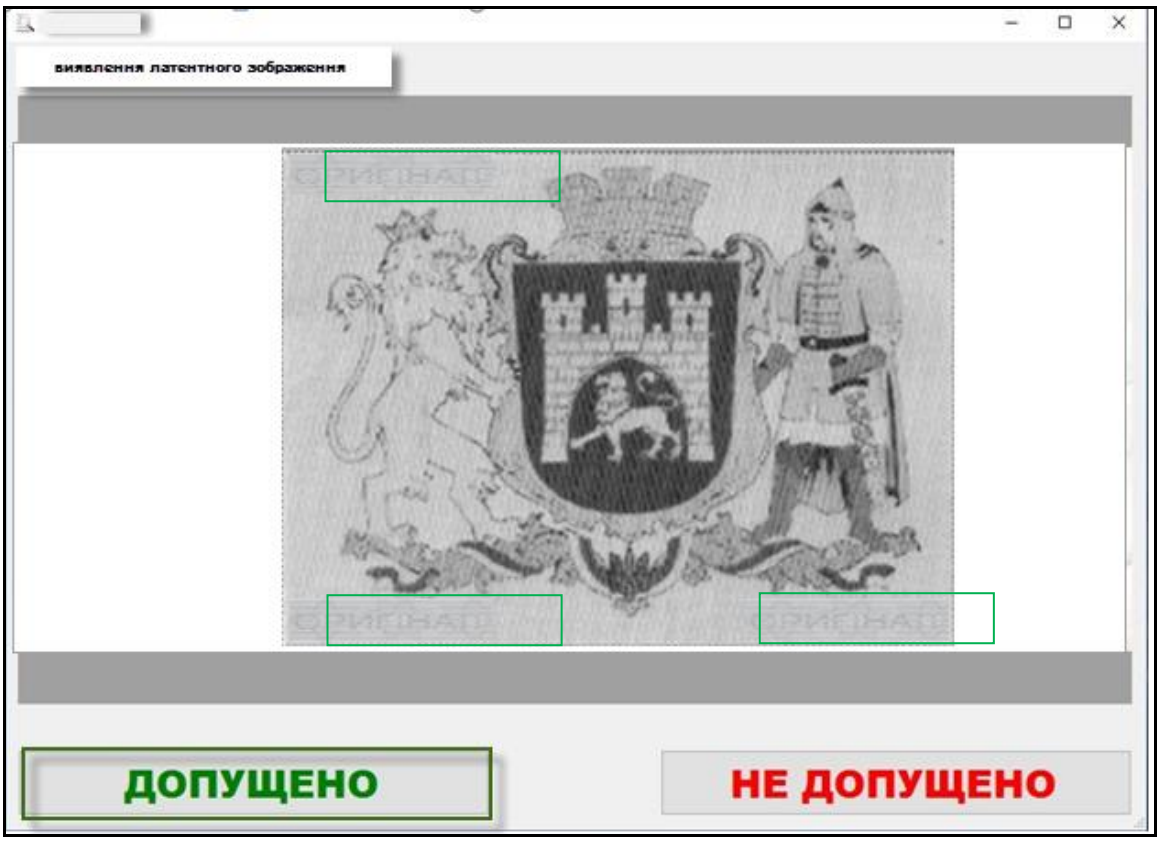


Рисунок 4.16 Визначення достовірності документа по розпізнаному латентному зображенню.

У випадку, коли загружено вхідне зображення рисунок 4.17, яке не відповідає оригіналу та після аналізу програми не виявлено прихованих елементів на ньому, а також визначено певне зміщення в попіксельному порівнянні, приймається рішення про те що документ є підробкою та підсвічується кнопка «не допущено», що зображено на рисунку 4.17.

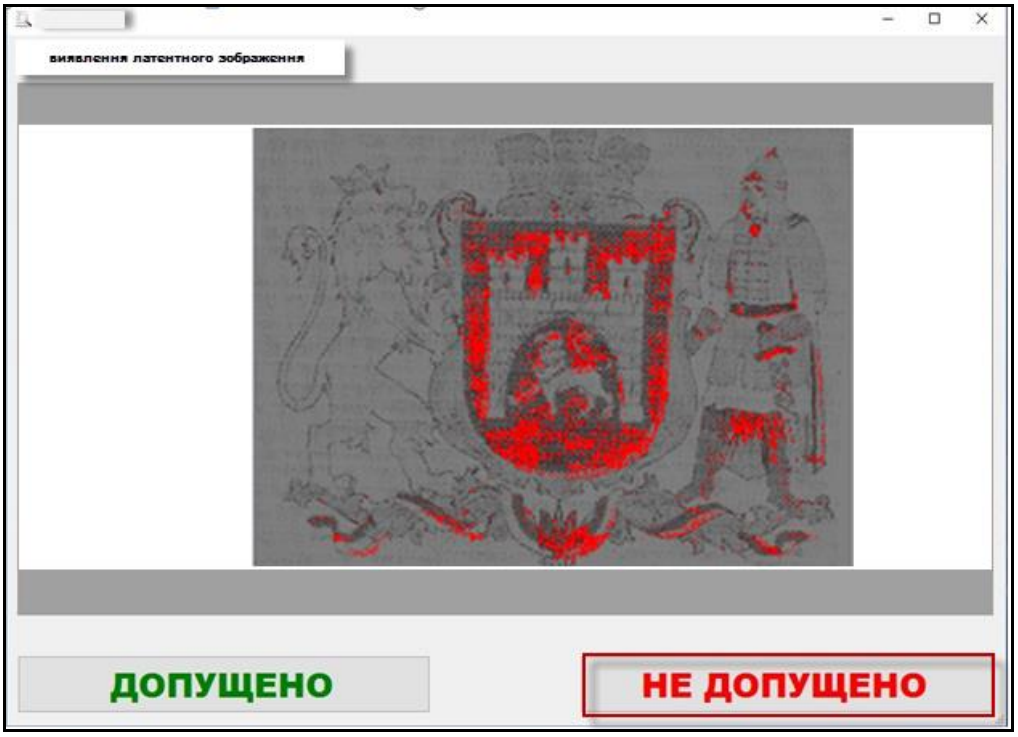


Рисунок 4.17 Визначення достовірності документа на основі методу PSNR

Ці результати показують вибірку з проведених експериментів та обраних вибірок даних і прихованих елементів.

Одним з висновків імітаційного моделювання є зменшення часу аналізу та ідентифікації документів на основі методу формування латентних зображень, і при цьому використовуються графічні елементи тонкої графіки, фракталів та ефекту муарутворення з метою підвищення продуктивності визначення достовірності.

Проведені експерименти показують покращення забезпечення достовірності документів на основі аналітичної залежності оригіналу та копії знятої спектрофометричним приладом показників: розтиснення растрової точки з похибою 15%, оптичною щільністю з похибою не більше 13%, рівномірністю розподілення фарби на відбитку 12%, трепінгу з похибою не

більше 10%. (див. рисунки 4.4 - 4.7).

Реалізоване комп’ютерне імітаційне моделювання показує підвищення продуктивності роботи інформаційної технології на базі удосконалення використаних методів формування латентних зображень роздрукованих на різних сортах паперу та здійсненні порівнняння оригіналу та копії, як візуально, так і приладо-контрольованими засобами.

Розроблений програмний комплекс системи розпізнавання латентних зображень дозволяє проводити оперативний контроль латентних зображень, що забезпечує високу візуальну якість виявленого прихованого зображення, за рахунок використання аналізу зображень та відображення прихованих елементів, які залежать від способу формування латентного зображення.

Розроблений програмний модуль формування та розпізнавання латентних зображень дозволяє формувати латентні зображення комбінованим способом з впровадженим тонкої графіки, фракталів та муару, що підвищує показники якості із значенням PSNR вище на 10-15% в порівнянні з відомими способами.

Висновки до розділу 4

1. Розроблено рекомендації для оптимізації ідентифікації документів. Відповідно до запропонованого раніше методу контролю достовірності документів було розглянуто та досліджено оригінали та копії на різних сортах паперу.
2. Підтверджено ефективність роботи методу використання латентних зображень створених на основі тонкої гафіки, фракталів та виявлення муару, оскільки даних підхід підвищує показники якості відносно PSNR вище на 10-15% та підвищує достовірність документів на основі показників: розтиснення растрової точки з похибою 15%, оптичною щільністю з похибою не більше 13%, рівномірністю розподілення фарби на відбитку 12%, трепінгу з похибою не більше 10%.
3. Реалізовано інформаційну технологію розроблення та ідентифікації латентних зображень для виявлення підробки в документах. Для цього у розробленому програмному продукті передбачена можливість зміни кольору в області документа, де була здійснена фальсифікація.
4. В таблицях 4.1, 4.2, 4.3 та 4.4 відображено значення середніх порівняльних характеристик для проведених експериментів при застосуванні методу визначення ідентифікації документу, що демонструє виведені порогових значень для визначення оригінальності документу. Значення отриманих результатів верифікують точність проведених експериментів.
5. З результатів моделювання можна зробити висновки, що впровадження інформаційної технології ідентифікації для забезпечення достовірності документів, запрограмованого на використання ЛЗ щодо зібраних та оброблених значень інформативних характеристик, створює умови для прогнозування параметрів та прийняття рішень щодо достовірності документів та на основі аналітичної залежності оригіналу та копії визначеної спектрофотометричним приладом можна оцінити оригінальність документів.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі на основі виконаних теоретичних та експериментальних досліджень розв’язано актуальне наукове завдання – підвищення захищеності друкованих документів, на основі розроблення інформаційної технології формування латентних елементів, яка включає методи формування цих елементів та встановлення їх достовірності. При цьому отримано такі результати:

1. Проведено аналіз методів, моделей та засобів формування графічних елементів для забезпечення надійності та достовірності документа, що засвідчив про існування потреби підвищення рівня достовірності друкованих документів. Визначено можливості вдосконалення та розроблення таких методів та засобів, а також показано, що ці методи не надають змоги підвищити точність ідентифікації підробки.
2. Обґрунтовано необхідність створення моделей та методів формування графічних елементів для забезпечення рівня захищеності документа та показано розв’язання цієї задачі на основі розробки інформаційної технології формування графічних елементів побудованих на основі методів тонкої графіки, латентних елементів, муару, фракталів.
3. Вперше розроблено метод формування латентних зображень, які складаються із шарів з градієнтними властивостями на основі лінії векторного формату, що підвищує точність побудови графічних елементів на 4.2%.
4. Вперше розроблено моделі побудови графічних пасток на основі муару, який створюється із тонких ліній з шириною від 0,25 мм та із частотами повторень, які кратні цілому числу, деформація яких спричиняє спотворення.
5. Вдосконалено метод на основі створення фрактальних елементів, що базується на побудові сіток, що підвищило ефективність виявлення

областей фальсифікації.

6. Розроблено інформаційну технологію встановлення достовірності документа способом побудови узагальненого критерію, який будується на основі даних, отриманих із використанням вимірювального устаткування. Досягнутий при цьому технічний результат полягає у підвищенні захисних властивостей друкованого документа на 10 - 15% від підробок. Захист друкованих документів на основі латентних зображень дав можливість зменшити час і вартість розроблення та ідентифікації документів.
7. Отримав подальший розвиток метод тонкої графіки, що ґрунтується на використанні математичного апарату, який забезпечує генерацію нових захисних елементів для позитивного виконання ліній 40 - 80 мкм та негативного 60 - 100 мкм. Новизна цього способу підтверджена Патентом України на корисну модель № 06221. «Спосіб захисту друкованих та електронних документів».
8. Інформаційна технологія розроблення та ідентифікації латентних елементів пройшла апробацію під час виконання робіт на основі досліджень наданої грантової підтримки Державного фонду фундаментальних досліджень “Технологія підвищення графічного рівня захищеності друкованих та електронних документів” та впроваджено на НГВУ “Бориславнафтогаз” ПАТ “Укрнафта”. Усі результати впровадження підтверджено відповідними актами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агрsuperновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Агрsuperновский, А.В. Балакин, В.Г. Грибунин и др. – М.: Вузовская книга, 2009. – 220 с.
2. Айфичер Э. Цифровая обработка сигналов: практический подход, 2- е издание / Эммануил Айфичер; [Пер. с англ.]. — М. : Издательский дом "Вильямс", 2004. — 992 с.
3. Бабак В.П. Теоретичні основи захисту інформації: підруч. / В.П. Бабак. – К.: Книжкове вид-во НАУ, 2008. – 752 с.
4. Валадов Д. О трафаретных защитных красках / Д. Валадов // Компьюарт. – 2011. – №6. – С. 24-27.
5. Глумов, Н.И. Алгоритм извлечения скрытой информации из отсканированных полиграфических изделий / Н.И. Глумов, В.А. Митекин, А.В. Сергеев, В.А. Федосеев // Вестник СГАУ. – 2008. – № 2 (15). – С. 216-220.
6. Глушаков, С.В. Математическое моделирование: Mathcad 2000, MATLAB 5: Учебный курс / С.В. Глушаков, И.А. Жакин, Т.С. Хачиров. – Харьков.: Фолио, 2001. – 524 с.
7. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р.Вудс // Техносфера. – 2012. – С. 1104
8. Гонсалес, Р. Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс. – М.: Техносфера, 2006. – 616 с.
9. Горбачев, В.Н. Методы цифровой стеганографии для защиты изобразительной информации [Электронный ресурс] / В.Н. Горбачев, Е.М. Кайнарова, А. И. Кулик и др. // Uprint Image Processing Group – Режим доступа: http://uipg.ru/assets/103-Metody-cifrstg-dlya-zashity-2010.pdf.
10. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційнотелекомунікаційних системах: Навч. посібник. Ч.1.

Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

11. Грицик В. В. Інформаційні технології захисту документів на основі унікальних графічних зображень у вигляді сіток / В. В. Грицик, В. В. Грицик (мол.), М. А. Назаркевич. // «Автоматика-2009»: Матеріали міжнародної конференції. — Чернівці, 2009.— С.346 – 347.
12. Грыцык В. В. Информационные технологии защиты документов средствами Ateb-функций. Часть 1. Построение базы данных Ateb-функций для защиты документов / В. В. Грыцык, И. М. Дронюк, М. А. Назаркевич. // Проблемы управления и информатики. — 2009. — № 2. — С. 139 – 152.
13. Грыцык В. В. Информационные технологии защиты документов средствами Ateb-функций. Часть 2. Об одном способе защиты электронных и напечатанных документов / В. В. Грыцык, И. М. Дронюк, М. А. Назаркевич. // Проблемы управления и информатики. — 2009. — № 3 — С. 144 – 153.
14. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2016. – 262 с.
15. Демида Б. А. Оптимізація розмірів файлів при програмуванні зображень для Web / Б. А. Демида, М. А. Назаркевич, Т. А. Марусенкова. // Поліграфія і видавнича справа: Наук.-тех. збірник. —2004. — № 41. — С. 79 – 84.
16. Дідух Л. А. Комп’ютерні методи обробки зображень для сучасних технологій захисту цінних паперів / Л. А. Дідух, М. В. Шовгенюк, Н. С. Писанчин. // Комп’ютерні технології друкарства. — 2006. — № 15. — С. 175 – 187.
17. Драган Я. П. Енергетична теорія лінійних моделей стохастичних сигналів / Я. П. Драган, Л. С. Сікора, Б. І. Яворський. — Львів : Центр стратегічних досліджень еко-біо-технічних систем, 1999. — 133 с.
18. Дронюк І. Комп’ютерна система побудови векторних зображень з поліграфічним захистом / І. Дронюк, М. Назаркевич. // Матеріали другої

міжнародної конференції «Комп'ютерні науки та інформаційні технології» CSIT. — Львів, 2007. — С.374 – 377.

19. Дронюк І. М. Математичне моделювання та автоматизація побудови захисних графічних зображень / І. М. Дронюк, М. А. Назаркевич, Ю. М. Пелех. // «Автоматика-2009»: Матеріали міжнародної конференції. — Чернівці, 2009.— С. 314 – 316.
20. Дронюк І. Метод захисту зображень антисканерними сітками / І. Дронюк, М. Назаркевич. // Актуальні проблеми економіки. Національна академія управління. — 2007. — № 10 (76). — С. 53 – 58.
21. Дронюк І. Методи створення періодичних та неперіодичних мозаїк у додрукарській обробці зображень / І. Дронюк, М. Назаркевич. // Технічні вісті. — 2007. — № 1 (25), 2 (26). — С. 58 – 60.
22. Дронюк І. Розробка програмного забезпечення для верстки макетів видань / І. Дронюк, М. Назаркевич, О. Коваленко. // Вісник Державного університету «Львівська політехніка». Інформаційні системи та мережі. — 2010. — № 673. — С. 274 – 282.
23. Дронюк І. М. Інформаційна технологія створення гравюр для захисту документів / І. М. Дронюк, М. А. Назаркевич, Ю. М. Пелех. // Матеріали міжнародної конференції «Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту» ISDMCI. — Євпаторія, 2010. — Т. 1. — С. 432.
24. Дронюк І. М. Розробка та створення моделей гравюри на основі осьової симетрії для поліграфічного захисту / І. М. Дронюк, М. А. Назаркевич, Ю. М. Пелех. // Системні технології. — 2010. — № 6 (71). — С. 80 – 88.
25. Дронюк І. М. Алгоритм побудови антисканерних сіток для захисту документів / І. М. Дронюк, М. А. Назаркевич. // XIV Всеукраїнська наукова конференція. Сучасні проблеми прикладної математики та інформатики. ЛНУ ім. І.Франка. — Львів, 2007. — С.55 – 56.
26. Дронюк І. М. До розв'язування одного класу звичайних нелінійних диференціальних рівнянь / І. М. Дронюк, М. А. Назаркевич. // Фізико-

технічне моделювання та інформаційні технології. — 2007. — № 6. — С. 136 – 140.

27. Дронюк І. М. Розробка програмного забезпечення для захисту документів фоновими сітками / І. М. Дронюк, М. А. Назаркевич, Ю. М. Пелех. // Вісник Державного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. — 2009. — № 650. — С. 245 – 250.
28. Дронюк І. М. Управління розв'язками системи нелінійних диференціальних рівнянь / І. М. Дронюк, М. А. Назаркевич. // «Автоматика-2006»: Матеріали міжнародної конференції. — Вінниця, 2006.— С. 14.
29. Дронюк, І. Метод захисту електронних та друкованих документів / Іванна Дронюк, Марія Назаркевич, Зореслава Шпак. // Матеріали третьої міжнародної конференції «Комп'ютерні науки та інформаційні технології» CSIT. — Львів, 2008. — С. 232 – 236.
30. Дронюк І. М. Розробка програмного продукту для захисту документів / І. М. Дронюк, М. А. Назаркевич. // «Автоматика-2008»: Матеріали п'ятнадцятої міжнародної конференції. — Одеса, 2008.— С. 14.
31. Дронюк І. М. Розроблення методу захисту цінних паперів на стадії додрукарської підготовки / І. Дронюк, М. Назаркевич, О. Миронюк // Вісник Національного університету "Львівська політехніка". – 2011. – № 694 : Комп'ютерні науки та інформаційні технології. – С. 352-357.
32. Дронюк І. М. Підвищення рівня безпеки документообігу на основі нових методів захиту та ідентифікації документів / І.М. Дронюк // Праці Одеського політехнічного університету. – 2013. – Вип.3(42). – с.157-160.
33. Дронюк І. М. Імовірнісна ідентифікакація захисних графічних елементів спотворених змазами / І.М. Дронюк, Д.Д. Пелешко, А.В. Клювак, М.З. Пелешко // Вісник Львівського державного університету безпеки життєдіяльності. – 2013. - №7ю – с.48-54.
34. Дубина Н. Полиграфические методы защиты. / Н. Дубина. // КомпьюАрт.

— 2002. — № 2.— С.63 – 71.

35. Дудикевич В.Б., Микитин Г.В., Гарасим Ю.Р. Ієрархічна модель захисту даних в інформаційних технологіях // Збірник тез доповідей II Міжнародної науково-практичної конференції «Проблеми і перспективи розвитку ІТ - індустрії». – Харків, 2010. – Вип. 7(88). – С. 212-213.
36. Дудикевич В., Сікора Л., Микитин Г., Рудник О. Методологічні засади захисту інформаційних технологій // Матеріали І-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". – 31 травня – 01 червня 2012 р. Львів. – С. 8-9.
37. Дурняк Б.В. Видавничо-поліграфічна галузь України: Стан, проблеми, тенденції: Статистично-графічний огляд : Моногр. / Б. В. Дурняк, А. М. Штангрет, О. В. Мельников; Укр. акад. друкарства. - Л., 2006. - 274 с. - Бібліогр.: с. 263-272.
38. Дурняк Б. В. Інформаційна технологія формування графічних засобів захисту документів: монографія / Б.В. Дурняк, В.З. Пашкевич, В.І. Сабат, О.В. Тимченко. – Львів: Укр. акад. друкарства, 2011. – 152 с.
39. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.
40. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К. : Держстандарт України, 1997. – 11 с.
41. ДСТУ 4010-2001. Бланки цінних паперів і документів суворого обліку та звітності. Загальні технічні вимоги. – К. : Держстандарт України, 2001. – 38 с.
42. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Бак, 2003. – 144 с.
43. Жарких, А.А. Система формирования и контроля латентных изображений [Текст] / А.А. Жарких, Г.В. Шагрова // Вестник Северо-Кавказского федерального университета: научный журнал / гл. ред. В.Н. Парахина. – Ставрополь: Изд-во СКФУ, 2015. – № 1 (46). – С.30-35.

44. Жмакин, М.О. Стеганография и перспективы ее применения в защите печатных документов / М.О. Жмакин // Безопасность информационных технологий. – 2010. – № 3. – С. 74-77.
45. Запоточний В.Й. Технології захисту цінних паперів [Навч. посіб.] / В.Й.Запоточний. Львів : Видавництво Національного університету "Львівська політехніка" , 2013. – с.152.
46. Завьялов С.В. Стеганографические методы защиты информации: учеб.пособие / С.В. Завьялов, Ю.В. Ветров. – Спб.: Изд-во Политехн. ун-та, 2012. − 190 с.
47. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Голос України: від 11.04.2006. — № 66.
48. Закон України «Про авторське право і суміжні права» // Відомості Верховної Ради України (ВВР), 1994, N 13, ст.64, зі змінами та доповненнями.
49. Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради (ВВР).- 2003.- №36. – ст.275, зі змінами та доповненнями.
50. Закон України «Про інформацію» //Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650, зі змінами та доповненнями.
51. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры : учебн. пособ. / А. Ю. Зубов. – М. : Гелиос АРВ, 2005. – 192 с.
52. Закон України «Про національну програму інформатизації» // Відомості Верховної Ради (ВВР).- 1998.- №27-28. – ст.181, зі змінами та доповненнями.
53. Інформаційні системи і технології: навч. посіб. для студ. вищ. навч. закл. / С. Г. Карпенко, В. В. Попов, Ю. А. Тарнавський, Г. А. Шпортюк. – К.: МАУП, 2004. – 192 с.
54. Иванова Т. Допечатная подготовка. Учебный курс / Т. Иванова. – СПб.: Питер, 2004. — 304 с.

55.Информационные технологии и защита информации в информационно-коммукационных системах : коллективная монография / С.П.Евсеев, М.Ю.Лосев, С.В.Минухин и др.; под ред. В.С.Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – с.486.

56.Информационние технологии и системы в управлении, образовании, науке: коллективная монография / С.П.Евсеев, М.Ю.Лосев, С.В.Минухин и др.; под ред. В.С.Пономаренко. – Х.: Вид-во ТОВ «Цифрова друкарня №1», 2013. – с.278.

57. Кипхан Г. Энциклопедия по печатным средствам информации. Технологии и способы производства / Г. Кипхан; [пер. с нем.] — М. : МГУП, 2003. — 1280 с.

58. Киричок П. Захист цінних паперів та документів сурового обліку / П. О. Киричок, Ю. М. Коростиль. — К. : НТУУ «КПІ», 2008. — 368 с.

59.Ковальчук А. Про один алгоритм шифрування-дешифрування зображень з використанням порозрядних операцій / А. Ковальчук, Д. Пелешко, А. Шкодин, О. Троян // Вісник Національного університету "Львівська політехніка". – 2011. – № 694 : Комп’ютерні науки та інформаційні технології. – С. 389-394.

60.Колмогоров А. Н. Элементы теории функций и функционального анализа / А. Н. Колмогоров, С. В. Фомин. - М. : Физматлит, 2004. - 572 с.

61. Конахович, Г.Ф. Компьютерная стеганография: Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – 288 с.

62. Коншин А. А. Защита полиграфической продукции от фальсификации / А. А. Коншин. — М. : Синус, 1999. — 160 с.

63. Корпинець Б. В. Скрывание информации в изображениях с использованием специфических особенностей формата файла / Б. В. Корпинець, Ю. Е. Яремчук. // Защита информации. — 2006. — № 2. — С. 24 – 29.

64. Корочкин, Л.С. Материалы и методы защиты специальных бумаг и документов от подделки / Л.С. Корочкин. – Минск: НТУП «Криптотех»,

2001. – 264 с.

65. Корочкин Л. Способы защиты и идентификации ценных бумаг / Л. Корочкин. — Минск : НТУП «Криптотех», 2003. — 114 с.
66. Корченко О.Г. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки // О.Г.Корченко, Д.А.Горніцька, В.В.Волянська // Захист інформації, 2012. - №1(54) – с.108 - 121.
67. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
68. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
69. Кульбич І.К. Оцінка якості відбитків при цифровому друці / І.К. Кульбич, О.І.Лотоцька // Технологія і техніка друкарства, 2013. – Вип. 4(42). - с.25-39.
70. Курбатова, Е.А. MATLAB 7: Самоучитель. / Е.А. Курбатова. – М.: Вильямс, 2006. – 256 с.
71. Лазаренко Е. Т. Захист друкованої продукції : навч. посіб./Е.Т.Лазаренко, В. З. Маїк, А. В. Шевчук, С. В. Жидецький. – Л.: УАД, 2007. – 104 с.
72. Лотошинська Н.Б. Теорія кольору / Н. Б. Лотошинська.–Львів: Видавництво Національного університету "Львівська політехніка", 2014. – с.200.
73. Маресин, В.М. Защищенная полиграфия: Справочник / В.М. Маресин: 2-е изд., стер. – М.: ФЛИНТА, 2014 – 640 с.
74. Масич А. Ю. Обнаружение подделок документов, выполненных с использованием реппрографической техники / А. Ю. Масич. // Ценные бумаги. — 2002. — № 7. — С. 56 – 63.
75. Медиковський М. Алгоритм управління ризиком використання поліграфічних документів / М. Медиковський, В. Пашкевич // Вісн. Нац. ун-ту "Львів. політехніка". - 2006. - № 565. - С. 254-262.
76. Медиковський М. Застосування семантичного підходу для аналізу

графічних об'єктів / М. Медиковський, М. Чаплагін // Вісн. Нац. ун-ту "Львів. політехніка". - 2006. - № 565. - С. 150-154.

77. Медиковський М.О. Інформаційні технології контролю та управління енергоактивними об’єктами / М.О. Медиковський. — Львів : ДНДІ інформаційної інфраструктури, 2000. — 247 с.
78. Мэтьюз, Д. Г. Численные методы. Использование MATLAB: пер. с англ. / Д. Г. Мэтьюз, К. Д. Финк. – М.: Изд. дом «Вильямс», 2001. – 713с.
79. Міжнародний документ «Модельний закон про інформатизацію, інформацію та захист інформації» від 8.11.2005 року – [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua/doc/?doc_id=160035
80. Микитин Г.В. Системний підхід до захисту інформаційних технологій // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України. – 2010. – Вип. № 57. – С.192-200.
81. Микитин Г.В. Системна, нормативна та комплексна моделі захисту інформаційних технологій // Вісник Національного університету “Львівська політехніка”: Автоматика, вимірювання та керування. – № 695. – 2011. – С.126-132.
82. Назаркевич М. А. Інструментальні засоби для розробки компонентів лінгвістичного забезпечення / М. Назаркевич, О. Коваленко, Є. Толстіков, К. Бурда. // Матеріали міжнародної конференції «Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту» ISDMCI. - Євпаторія, 2010. - Т. 1. - С. 376.
83. Назаркевич М. А. Розробка гарнітури шрифту півустав для комп’ютерного складання тексту / М. А. Назаркевич, Т. А. Марусенкова. //Вісник Державного університету «Львівська політехніка». Комп’ютерні науки та інформаційні технології. - 2005. - № 543. - С. 31 - 39.
84. Назаркевич М.А. Програма перетворення растрових контурних зображень на основі фрактальних сіток / М. Назаркевич, І. Клюйник // Вісник Національного університету «Львівська політехніка». Серія: Комп’ютерні науки та інформаційні технології. — Львів : Видавництво

Львівської політехніки, 2017. — № 864. — С. 42–48.

85. Назаркевич М. Аналіз сучасних методів та видів графічного захисту друкованих документів / М. Назаркевич, О. Троян // Вісник Національного університету "Львівська політехніка". – 2014. – № 800 : Комп’ютерні науки та інформаційні технології. – С. 61–65.
86. Назаркевич М. А. Розроблення програмного продукту для захисту інформації на основі плівок з прихованим латентним зображенням / М. А. Назаркевич, О. А. Троян // Вісник Національного університету "Львівська політехніка". – 2014. – № 806 : Комп'ютерні системи та мережі. – С. 187–194.
87. Назаркевич М. Розробка методу захисту документів латентними елементами на основі фракталів / М. Назаркевич, І. Дронюк, О. Троян, Т.Томащук // Захист інформації, Том 17. – 2015. – № 1. – С. 21–26.
88. Нечай О. Розроблення моделей загроз для друкованих документів, захищених графічними методами захисту / О. Нечай, М. Назаркевич, Ю. Христиніна // Вісник Національного університету "Львівська політехніка". – 2013. – № 751 : Комп’ютерні науки та інформаційні технології. – С. 170–177.
89. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. 34 с.
90. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с. 469
91. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
92. Овсяк В. К. Синтез і дослідження алгоритмів комп’ютерних систем.

[Навчальний посібник] / В. К. Овсяк, В. М. Бритковський, О. В. Овсяк, Ю. В. Овсяк. — Львів : УАД, 2004. — 276 с.

93. О голографическом торговом знаке [Электронный ресурс] // BH Group: сайт – Режим доступа: http://www.holo.ru/news/doc/9/1.html, свободный. (Дата обращения: 4.11.2014).
94. Описание программного продукта CERBER [Электронный ресурс] // SecuritySoft Co. Ltd. – Режим доступа: http://www.securesoft.ru/cerber.html, свободный. (Дата обращения: 25.11.2014).
95. Описание программного продукта BBS Designer [Электронный ресурс] // GuardSoft Ltd. – Режим доступа: http://www.guard-soft.com/designer.html, свободный. (Дата обращения: 25.11.2014).
96. Описание визуализатора DORS 25 [Электронный ресурс] // Компания «Система» : сайт – Режим доступа: http://www.systema.biz/590.html
97. Описание технологий защиты отпечатков [Электронный ресурс]: компьютерный журнал // КомпьютерПресс: сайт. – М., 2006. – Режим доступа: http://compress.ru/Article.aspx?id=16111, свободный. (Дата обращения: 25.11.2014).
98. Павлов И. В. Контроль подлинности документов, ценных бумаг и денежных знаков / И. В. Павлов. — М. : Техносфера, 2006. — 472 с.
99. Патент на корисну модель. №38479 Спосіб захисту текстової, табличної та графічної інформації / І. М. Дронюк, М. А. Назаркевич; заявник та власник патенту Національний університет «Львівська політехніка». Дата публ. 12.01. 2009 р. Бюл. № 1.
100. Патент України № 64836. Графічний елемент захисту банкнот, цінних паперів, документів та спосіб його виготовлення / М. В.Шовгенюк, В. Є.Білорус, М. П. Козловський, Т. Є. Крохмальський. Дата публ. 15.03. 2004 р. Бюл. № 3.
101. Пашкевич В. З. Опис графічних засобів захисту на основі їх графового представлення / В. З. Пашкевич // Моделювання та

інформаційні технології : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. – К., 2005. – Вип. 35. с.76–84.

102. Пашкевич В. З. Аналіз методів побудови графічних засобів захисту / В. З. Пашкевич // Зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. – К., 2005. – Вип. 30. – С. 101–108.

103. Пелешко Розпізнавання графічних захисних елементів на фонових зображеннях / Д. Пелешко, А. Ковальчук, І. Дронюк, М. Назаркевич // Вісник Національного університету "Львівська політехніка". – 2013. – № 751 : Комп’ютерні науки та інформаційні технології. – С. 227–230.

104. Пелешко Д.Д. Інваріантні моменти в прикладних задачах обробки та аналізу зображень / Д. Пелешко, А. Ковальчук, Н. Кустра, І. Ізонін // Вісник Національного університету “Львівська політехніка”. – 2011. – № 694: Комп’ютерні науки та інформаційні технології. – С. 265–270.

105. Пелешко Д.Д. Модель утворення локальних спотворень зображення / Д. Пелешко, А. Клювак, А. Ковальчук, І. Ізонін, М. Голубінська // Вісник Національного університету “Львівська політехніка”. – 2013. – № 771: Комп’ютерні науки та інформаційні технології. – С. 150–155.

106. Пелешко Д.Д. Суміщення наборів однотипних зображень [Текст] : монографія / Д.Д. Пелешко. – Львів : Видавництво Національного університету "Львівська політехніка", 2010. – с.138.

107. Петряєв С.Ю. Способи підробки паперових грошових знаків [Електрронний ресурс] / С.Ю. Петряєв // Вісник НТУУ «КПІ»: Соціологія. Політологія. Правознавство, 2009. - №4. – с23-28.

108. Пэдхем, Ч. Восприятие света и цвета / Ч. Пэдхем, Дж. Сондерс: пер. с англ. Р. Л. Бирновой и М. А. Островского. – М.: изд-во «Мир», 1978. – 255 с.

109. Пискунов Н. С. Дифференциальное и интегральное исчисление для втузов. / Н. С. Пискунов. — М. : Интеграл-Пресс, 2009. — 544 с.

110. Побудова оптико-цифрових інформаційно-вимірювальних систем для

обробки та кореляційного аналізу бінарних зображень: дис... д-ра техн. наук: 05.11.16 / Л. І. Муравський; НАН України, Фізико-механічний ін-т ім. Г. В. Карпенка. — Львів, 2001. — 348 с.

111. Потапов А. А. Новейшие методы обработки изображений / А. А. Потапов, А. А. Пахомов, С. А.. Никитин.— М.: Физматлит, 2008. -496 с.

112. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебн. пособ. / А. В. Потий. – Х. : ХНУРЕ, 2002. – 80 с.

113. Приборы и системы для определения подлинности банкнот, документов, ценных бумаг [Электронный ресурс] // научно-производственное предприятие «ВИЛДИС». – Режим доступа: http://www.vildis.ru/product/ultramag-s6/, свободный. (Дата обращения: 03.04.2016).

114. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851- IV // Урядовий кур’єр. — 2003. № 119. — С. 1 – 6.

115. Сікора Л. С. Перспективні інформаційні технології в системах автоматичного управління енергоактивними об'єктами виробничих структур / Л.С. Сікора, М.О. Медиковський, В.В. Грицик. — Львів : НАН України, Державний комітет зв'язку та інформатизації України, Державний НДІ інформаційної інфраструктури, 2002. — 416 с.

116. Созведие Евриона и система CDS: первые рубежи защиты купюр // Банкноты стран мира. – 2008. – № 2. – С. 30-33.

117. Специальное программное обеспечение для работы с изображениями [Электронный ресурс] // Компания«Регула». – Режимдоступа: ttps://regulaforensics.com/ru/products/software/, свободный. (Дата обращения: 03.04.2016).

118. Способ формирования латентного изображения: патент на изобретение RUS 2337403: G 06 T 5 00,G 06 K 9 00 / Маккарти Л.Д., Свиджерс Г.Ф.; Правообладатель: Коммонвелс сайнтифик энд

индастриал рисеч организейшен; дата регистрации 04.06.2004.

119. Способы защиты документов [Электронный ресурс] // ООО «ВИЛДИС». Режим доступа: http://www.bnti.ru/showart.asp?aid=940&lvl=01.03.05.&p=1.

120. Сучасні інформаційні системи і технології: конспект лекцій / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова, В. В. Карасюка. – Х.: Нац. юрид. ун-т ім. Ярослава Мудрого, 2014. – 347 с.

121. Рашкевич Ю.М. Нейроподібні методи, алґоритми та структури обробки сигналів і зображень у реальному часі. / Ю.М. Рашкевич, Р.О. Ткаченко, І.Г. Цмоць, Д.Д. Пелешко: Монографія – Львів: 2014. – 256с.

122. Різник В.В. Методи та технології захисту документів і цінних паперів від підробки / В.Різник, О.Ляхович // Вісник Національного університету “Львівська політехніка”. Комп’ютерні науки та інформаційні технології.– 2010. – № 686: – С. 271–275.

123. Технологии защиты — [Електронный ресурс].– Режим доступу: http://www.securesoft.ru/in fo_technologies.html.

124. Терещенко Л.О. Інформаційні системи і технології в обліку: навч. посіб./ Л.О. Терещенко, І.І. Матієнко-Зубенко. – К.: КНЕУ, 2004. – 187 с.

125. Топчиев, И. Н. Математическое моделирование и программный комплекс для контроля магнитных полей и латентных изображений: дис. канд. техн. наук: 05.13.18 / Топчиев Иван Николаевич. – Ставрополь, 2010. – 168 с.

126. Трубачев А. П. Оценка безопасности информационных технологий / А. П. Трубачев ; под общ. ред. В. А. Галатенко. М. :СИП РИА, 2001.356 с

127. Федотова Е.Л. Информационные технологии и системы: учеб. пособие / Е.Л. Федотова. – М.: ИД “ФОРУМ”: ИНФРА-М, 2014. – 352 с.

128. Хорошко В. А. Методи і засоби захисту інформації / В. А. Хорошко, А. А. Чекатков. – К. : Юніор, 2003. – 504 с.

129. Цмоць І. Г. Інформаційні технології та спеціалізовані засоби обробки сигналів і зображень у реальному часі / І. Г. Цмоць — Львів, Вид-во

УАД, 2005. — 227 с.

130. Цмоць І.Г. Апаратна реалізація покращення якості цифрових зображень / Цмоць І.Г., Пелешко Д.Д., Ізонін І.В. // Optoelectronic Information Technologies “Photonics ODS- 2015”: proc. of intern. scien. conf., 21-23 April 2015 y., Vinnytsia. – Vinnytsia: [VNTU], 2015. – P. 28.

131. Цмоць І.Г. Інформаційні технології та спеціалізовані засоби обробки сигналів і зображень у реальному часі.: Монографія. – Львів.: Видавництво УАД, 2005. – 227 с.

132. Шавард, Н. А. Экспресс-анализ подлинности специальных, акцизных, и идентификационных марок /Н. А. Шавард. – М.: «Вилдис»,1999. – 32 с.

133. Шведова, Н.Н. Вопросы методологии криминалистического исследования документов / Н.Н. Шведова // Судебная экспертиза. – 2015. – Т. 1. – № 1 (41). – С. 16-23.

134. Шевелёв А. Латентные изображения на основе стохастических растровых структур / А. Шевелёв, Ю. Андреев. // Известия вузов. Проблемы полиграфии и издательского дела. 2009. — № 1. — С. 29– 39.

135. Шевелев, А.А. Создание латентных изображений с использованием стохастических растровых структур / А.А. Шевелев // Технологія і техніка друкарства. – 2009. – №1-2 (23-24). – С. 226-233

136. Шевчук А. В. Теоретичні основи побудови інформаційних технологій захисту поліграфічної продукції спеціального призначення: Автореф.дис. д-ра техн. наук: 05.13.06 / А. В. Шевчук. // Державний комітет зв’язку та інформатизації України. – Львів, 2004. — 34 с.

137. Шовгенюк М. В. Метод кодування графічних зображень та впровадження нової технології захисту цінних паперів / М. В. Шовгенюк, Л. А. Дідух. //Наука та інновації. – 2009. Т.5, № 1. С.52 – 61.

138. Шовгенюк М. В. Дослідження властивостей бінарних фазових елементів для голографічних систем розпізнавання образів [Текст] / М. В. Шовгенюк [и др.] ; Нац. акад. наук України, Ін-т фізики конденс. систем. - Л. : [б.в.], 1999. - 43 с.: (Препр. / НАН України;

ICMP-99-28U).

139. Шовгенюк М. В. Методи кодування графічних зображень та впровадження нової технології= захисту цінних паперів [Текст] / М.В.Шовгенюк, Л.А.Дідух// Наука та іновації. – 2009.Том 5, №1, с.52-61.

140. Юсупова М. Ф. Компьютерные информационные технологии в обучении начертательной геометрии : монография / М. Ф. Юсупова. – К. : Вид-во НПУ имени М. П. Драгоманова, 2006. – 280 с.

141. Якуцевич С. Розробка концепції комп'ютерних систем контролю та оцінки якості друкованої продукції / С.Якуцевич, С,О,Войтенко // ,Технологія і техніка друкарства. 2009. – Вип.4. – с.53-68,

142. Яцимірський М.М. Швидкі алгоритми ортогональних тригонометричних перетворень / М.М. Яцимірський – Львів, Академічний експрес,1997. — 219 с..

143. Amidror Isaac The Theory of the Moire Phenomenon [електронний ресурс]. / Isaac Amidror. Academic Publisher, Springer, 2000 - Режим доступу: https://www.springer.com/la/book/9781848821804.

144. Amidror Isaac Glass patterns in the superposition of random line gratings / Isaac Amidror // Journal of Optics A: Pure and Applied Optics. – 2003. – p 205 – 2015.

145. Aleshin, A.A. Software for scanned polygraphic products steganalysis / A.A. Aleshin, D.M. Bogomolov и др. // Pattern Recognition and Image Analysis: New Information Technologies (PRIA-9-2008): 9th International Conference (Nizhni Novgorod, October 15-19, 2008): conference proceedings. – Nizhni Novgorod, 2008. – Vol.1. – P. 3-6.

146. Alldrin N. Super–Resolution / Neil Alldrin // UCSD Research Exam Paper.– 2006. – P. 1–12.

147. Avcibas, I. Statistical evaluating of image quality measures / I. Avcibas, B. Sankur, K. Sayood // Journal of Electronic Imaging. – 2002. – Vol.11. – №2. – P. 206- 223.

148. Bartholdi L., Grigorchuk R., Nekrashevych V. From fractal groups to fractal sets / L. Bartholdi, R. Grigorchuk, V. Nekrashevych // Trends in Mathematics, Birkhauser, 2003, pp.25-118.

149. Brigham E. The fast fourier transform and its application / E. O. Brigham - HJ: Prentice Hall, 1988. — 468 с.

150. Guard-soft Cerberus – [Електронний ресурс]. – Режим доступу : http://www.guard-soft.com/cerb_filters.html.

151. Conjugate cluster screens for embedding digital watermarks into printed halftone documents, United States Patent № 7,352,879, H04K 1/00 (20060101), Wang; Shen-ge, заявитель Xerox Corporation (Norwalk, CT),: опубл. 1.04.2008.

152. Documents by Gernot Hoffmann – [Електронний ресурс]. – Режим доступу : http://www.fho-emden.de/~hoffmann.

153. Droniuk I. Documents protecting and decorating using cubic splines interpolation / Ivanna Droniuk, Maria Nazarkevich, Iryna Verbenko. // Proceedings of the Vth International Scientific and Technical Conference CSIT'2010, October 14-16, Lviv Polytechnic National University. — Львів, 2010. — С. 106 – 108.

154. Droniuk I. M. Development of linguistic content text editorfor prepress / I. M. Droniuk, M. A. Nazarkevich, K. I. Burda, E. V. Tolstikov. // Proceedings of the Vth International Scientific and Technical Conference CSIT, 2010, October 14-16, Lviv Polytechnic National University. . — Львів, 2010. — С.83 – 85.

155. Droniuk I.M. Development of printed packaging protection technology by means of background nets / I.M. Droniuk, M.A. Nazarkevich. // Матеріали міжнародної науково-технічної конференції CADSM, 2009. 24-28 лютого. — Львів-Поляна. — С.401 – 404.

156. Droniuk I. M. Modeling nonlinear oscillatory system under disturbance by means of Ateb-functions for the Internet / I. M. Droniuk,

M. A. Nazarkevich. // Proceedings of 6th working international conference «Het-Nets2010». —Gliwice, 2009. — C.325 – 335.

157. ISO 32000-1:2008 - Document management — Portable document format — Part 1: PDF 1.7. [Електронний ресурс]. Режим доступу : http: // www. iso.org/iso/catalogue_detail.htm.

158. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

159. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

160. jura.at [Електронний ресурс]. Режим доступу : http: //www.jura.at /en /index.htm.

161. Lim J. Two-Dimensional Signal and Image Processing / Jae S. Lim - NJ: Prentice Hall, 1996. — 984 p.

162. Montufar Chaveznava R. Face Tracking using a Polling Strategy // Proc. of World, 1992. — 385 p.

163. Nazarkevich M. Research of numeral transformations of Ateb-functions in the mathematical design / M. Nazarkevich. // IV Sympozjum modelowanie i symulacja komputerowa w technice. Wyzsza szkola informatyki. — Lodz, 2005. C. 161 – 163.

164. Moiré formations, Isaac Amidror, The theory of the moiré phenomenon. Periodic layers, 2nd edition, (London; Springer, 2009), p. 36.

165. Ostromoukhov V. Digital Facial Engraving / V. Ostromoukhov. // Computer Graphics Proceedings, Annual Conference Series, 1999 p. 417-424.

166. Petrou M. Image Processing: the fundamentals. / M. Petrou. — M.: Panagiota Bosdogianni, 1999. — 842 p.

167. PostScript language reference manual / Adobe Systems Incorporated

[Електронний ресурс]. Режим доступу : www. adobe.com/ products /postscript/ pdfs/PLRM.pdf.

168. PostScript language tutorial and cookbook / Adobe Systems Incorporated [Електронний ресурс]. Режим доступу: www.freebookcentre.net/PostScript-Language-Tutorial-and-Cookbook. html.

169. Practical PostScript. A Guide to Digital Typesetting / David Byram-Wigfield. [Електронний ресурс]. Режим доступу : http://www.computer-books. Us /postscript_0001.php

170. Fridrich, J. Steganography in digital media: principles, algorithms, and applications / J. Fridrich. – Cambridge: University Press, 2010. – 437 p.

171. Sergeyev, V. Gabor Filter Based Attack on Printed Documents Protection Methods via Digital Watermarks / V. Sergeyev, V. Fedoseev, V. Mitekin // Intelligent Information Hiding and Multimedia Signal Processing: Eighth International Conference (18-July 2012, Piraeus-Athens, Greece): proceedings. – Piraeus-Athens: IEEE, 2012. – P. 265-268.

172. Goryaev, M.A. Two models of the latent image formation / M.A. Goryaev // IS&T's: 52nd Annual Conference (Savannah, GA, April 25-28, 1999): proceedings. – Savannah, 1999. – P. 11-13.

173. Fridrich, J. A new steganographic method for palette-based image / J. Fridrich // Proceedings of ISBT: PISP conference (Savannah, GA, April 1989): proceedings. – Savannah, 1989. – P. 285-289.

174. Identification system comprising a partially reflective retardation device: patent US 4659112: IC B42D 15/10, G06K 19/14, B42D 015/00 / Daniel T. Reiner, Lawrence Bolt, Philip W. Morlan Jr., Ali Tavasolian; Assignee: Optical Devices, Inc; filed 3.12.1984; published 21.04.1987, Appl. No.06/677,427

175. Polymer materials with latent images visible in polarized light and

methods for their production: patent US 6124970: IC G02B 5/30, G06K 19/14, G02B 027/28, B42D 015/00 / Andrei Karassev, Anatoli Vannikov, Vladimir Kazarinov, Ludmila Karasseva; Assignee: Latents Image Technology Ltd. (Jerusalem, IL); filed 20.10.1997; published 26.09.2000, Appl. No. 08/953,992

176. Tytyk R. Neural Network Technology for Image Downscaling [Electronic edition] / R. Tytyk, R. Tkachenko, I. Izonin, K. Hrytsyk // Litteris et Artibus: proc. of 5 intern. youth sience forum, 26–28 Nov. 2015 y., Lviv, Ukraine. — Lviv : Lviv Polytechnic Publishing House, 2015. — P. 72–74.

ДОДАТОК 1.

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Назаркевич М.А. Розробка методу захисту документів латентними елементами на основі фракталів / М.А. Назаркевич, І.І. Дронюк, О.А. Троян, Т.Ю. Томащук // Захист інформаці ї. – 2015. – № 1. – С. 21–26.
2. Troyan Oksana Identification latent elements in the printed and electronic documents // Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. – 2016. – Вип. № 843. – С. 213 – 220.
3. Troyan Oksana Method of forming latent image to protect documents based on the effect moire // Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. – 2015. – № 826. – С. 394 - 403.
4. Назаркевич М.А. Метод захисту документів на основі ефекту муару / М.А. Назаркевич, О.А. Троян // Науковий вісник НЛТУ України. – 2015. – Вип. 25.8. – С. 337 – 346 (метод формування графічних пасток на основі муару).
5. Dronjuk Ivanna "The Modified Amplitude-Modulated Screening Technology for the High Printing Quality" / Ivanna Dronjuk, Maria Nazarkevych, Oksana Troyan // International Symposium on Computer and Information Sciences, ISCIS 2016: Computer and Information Sciences, Krakow-Poland, Springer, 26 - 27October 2016. С. 270 - 276.
6. Назаркевич М.А. Розроблення програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням // М. А.Назаркевич, О.А.Троян // Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі. – Львів. – 2014. – Вип. № 806. – С. 187-194.
7. Назаркевич М.А. Аналіз сучасних методів та видів графічного захисту

друкованих документів // Назаркевич М.А., Троян О.А. // Вісник Національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології. – Львів. – 2014. – Вип. № 800. – С. 61-65.

8. Nazarkevych M.A. Method of electronic and printed documents of protection on the basis of moire effect / M. A. Назаркевич, О.А.Троян, І.М. Дронюк // Актуальні проблеми економіки, Київ – 2016. – Вип №5 (179) С. 382-394.
9. Назаркевич М.А. Математична модель захисту документів з формуванням муару на основі кратних періодичних решіток // М. А. Назаркевич, О.А. Троян // Комп'ютерні технології друкарства: Зб. наук. праць. – Львів: УАД, – 2015. – Вип. № 34 – С. 156 – 163.
10. Назаркевич М.А. Разработка скрытого изображения для защиты документов с использованием эффекта муара. / Мария Назаркевич, Иванна Дронюк, Оксана Троян // Wspolczesne problemy bezpieczenstwa i marketingu. Marketing : [monogr. nauk.] / Wyzsza szkola zarzadzania marketingowego i jez. obcych w Katowicach ; pod red. nauk. A. Limanskiego, Katowice – 2015. – С. 215-226.

Наукові праці, які додатково відображають наукові результати дисертації:

11. Пат. України на корисну модель 06221 України, МПК(2006) G 06 K 15/22. Спосіб захисту друкованих та електронних документів / І.М.Дронюк, М.А.Назаркевич, О.А.Троян, Л.В.Легкий; заявник і патентовласник Національний університет «Львівська політехніка».–№ a201406221; заявл. 05.06.2014; опубл. 26.08.2014, Бюл. № 16.– 4с.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Troyan O.A Analysis of threats falsification of printed documents / Troyan O.A, Korobchynskyi M., Didyk O. // Proceedings of the 2016 IEEE 1st International Conference on Data Stream Mining and Processing, DSMP – 2016. С. 248 - 253.
13. Nazarkevych M. A. Data protection based on encryption using Ateb-functions Nazarkevych M., Oliarnyk R., Troyan O., Nazarkevych H // Proceedings of the 11-th International Scientific and Technical Conference «Computer

Science and Information Technologies» (CSIT 2016), Lviv. – 2016. –P.30-32.

14. Назаркевич М.А. Захист цінних паперів на основі нових методів захисту інформації / М. А. Назаркевич, О.А. Троян // Мат.V-ої міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем» – Львів. – 2016. – С. 150-151.
15. Troyan O. A. Development system of protection electronic document to ensure the integrity and confidentiality of information / Troyan O. A. // Materials of the XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics. – Поляна. – 2015. – С. 376 – 378.
16. Medykovskyy M Methods of protection document formed from latent element located by fractals / Medykovskyy M., Lipinski P., Troyan O., Nazarkevych M., // Proceedings of the 10-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2015) Lviv. – 2015. – P. 70–73.
17. Троян О.А. Розроблення вільного програмного забезпечення для захисту документів на основі латентних муарових елементів / О.А. Троян // Матеріали п’ятої міжнародної конференції FOSS Lviv. – Львів. – 2015. – С. 91-92.
18. Дронюк І.М. Метод створення мультимедійних документів, захищених ементами на основі ефекту «муар» / І.М.Дронюк, М. А. Назаркевич, О.А. Троян // Мат.XIV-ої міжнародного наукового семінару «Сучасні проблеми інформатики в управлінні, економіці, освіті». – Київ-Світязь. – 2015. – С. 207-209.
19. Дронюк І.М. Метод захисту латентними елементами на основі ефекту муару / І.М.Дронюк, М. А. Назаркевич, О.А. Троян // Мат.IV-ої міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів. – 2015. – С. 179-180.
20. Троян О.А. Спосіб захисту друкованих документів на основі латентних елементів за допомогою ефекту муару / О.А. Троян // Всеукраїнська конференція «Сучасні комп’ютерні інформаційні технології» АСІТ-2015. – Тернопіль. – 2015. – С.180-182.

21. Троян О.А. Спосіб захисту документів на основі латентних елементів побудованих за допомогою фрак талів / О.А. Троян // Міжнародна науково-практична конференція «Комп'ютерні технології та інформаційна безпека». – Кіровоград. – 2015. – С. 31-32.
22. Назаркевич М. А. Розроблення вільного програмного забезпечення для захисту друкованих документів мікрографікою / М. А. Назаркевич, О.А. Троян // Матеріали четвертої міжнародної конференції FOSS Lviv – Львів. – 2014. – С.132-134.
23. Troyan O. Analysis and development of latent elements as a metod to protected documents / Troyan O.A., Tomashchyk T.Yu. // Proceedings of the 9-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2014) Lviv. – 2014. – P. 91- 92.
24. Троян О.А. Метод формування гільйошних елементів для задач захисту графічних зображень / О.А. Троян // Всеукраїнська конференція «Сучасні комп'ютерні інформаційні технології» ACIT-2014. – Тернопіль. – 2014. – С. 222-223.
25. Троян О.А. Аналіз латентних елементів на основі теорії Ateb-функцій / О.А.Троян // Міжнародна науково-практична конференція молодих вчених та студентів «Інформаційні технології, економіка та право: стан та перспективи розвитку». – Чернівці. – 2014. – С. 34-35.
26. Назаркевич М.А. Розроблення програмного забезпечення для захисту друкованих документів / М. А. Назаркевич, О.А. Троян // Матеріали IV науково-технічної конференції ITSEC. – Київ. – 2014. – С. 33-34.
27. Троян О.А. Аналіз біометричних видів захисту інформації / О. А.Троян , М. А.Назаркевич, З. Я.Шпак , І.І.Клюйник // матеріали Міжнародної науково-практична конференція «Сучасні наукові підходи до стабільного економічного розвитку та економічної безпеки». – Чернігів. – 2014. – С. 45-47.
28. Troyan O. A. Development protection software document based on the engraving / O.A.Troyan , Terlecka N. T., Oliyarnik R. // Global scientific unity 2014. – Prague, Czech Republic. – 2014. – С. 146-152.

29. Назаркевич М.А. Технологія графічного способу захисту документів на основі гравюр // М. А. Назаркевич, О.А. Троян // ІІІ-ої Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології». – Одеса. – 2014 – С.175-178.
30. Назаркевич М.А. Аналіз сучасних методів та програмних ужитків з графічним захистом друкованих документів / М. А. Назаркевич, О.А. Троян // Технічні вісті: 2013/1 (37), 2 (38). – С. 42-44.
31. Nasarkevych M.A. Analysis of software protection and development of methods of latency in printed documents/ Nasarkevych M.A., Troyan O. A. // Proceedings of the 8-th International Scientific and Technical Conference «Computer Science and Information Technologies» (CSIT 2013) Lviv. – 2013. – P. 120-121.

ДОДАТОК 2
Акти впроваджень результів дисертаційних досліджень

"Затверджую"
Проректор з науково-педагогічної роботи
Національного університету
"Львівська політехніка"
_____ О.Р. Давидчак
"___" _____ 2019 р.

АКТ

про впровадження в навчальний процес результатів
кандидатської дисертаційної роботи
Троян Оксани Анатоліївни

Цей акт складено про те, що результати кандидатської роботи Троян Оксани Анатоліївни на тему "Інформаційна технологія розроблення та ідентифікації латентних зображень" представленої на здобуття наукового ступеня кандидата технічних наук, використовуються у навчальному процесі кафедри "Автоматизовані системи управління" Національного університету "Львівська політехніка". Матеріали дисертаційного дослідження використовуються під час написання студентами курсових робіт, кваліфікаційних бакалаврських та магістерських робіт, а також під час викладання дисциплін: "Системний аналіз видавничих процесів", "Інформаційні технології захисту даних".

Зокрема в навчальному процесі використовуються запропоновані О.А.Троян:

– моделі побудови графічних елементів на основі формування фракталів, які завдяки рекурсивній процедурі покривають всю площу зображення із заданими параметрами дроблення, що забезпечує побудову графічних елементів з високою точністю (дисципліна "Інформаційні технології захисту даних", тема 3 "Застосування фрак талів для захисту" для студентів освітньо-кваліфікаційного рівня "бакалавр", що навчаються за спеціальністю 122 "Комп'ютерні науки");

–вдосконалений метод створення елементів тонкої графіки для формування графічних елементів, що створюють умови для вибору позитивних та негативних ліній та забезпечує візуалізацію прихованих елементів при копіюванні та допомагають виявити спотворення в документах (дисципліна "Системний аналіз видавничих процесів", тема 12 "Маркетинг виготовлення цінних паперів (Метод мозкового штурму)" для студентів освітньо-кваліфікаційного рівня "бакалавр", що навчаються за спеціальністю 122 "Комп'ютерні науки");

– метод формування латентних зображень, де графічним елементом є лінії векторного формату, які формують зображення шарами з наперед заданими

градієнтними властивостями та забезпечують підвищення інформативних характеристик побудови графічних елементів (дисципліна "Інформаційні технології захисту даних", тема 2 "IT технології для захисту друкованих документів" для студентів освітньо-кваліфікаційного рівня "бакалавр", що навчаються за спеціальністю 122 "Комп'ютерні науки").

Ефект від використання результатів кандидатської дисертаційної роботи Троян О.А. полягає у вивченні майбутніми фахівцями сучасних методів та засобів ідентифікації документів, що грунтується на використанні моделей формування графічних елементів для контролю та виявлення спотворень в документах.

Доцент кафедри АСУ
к.т.н., доцент — Я.В. Ковівчак

Доцент кафедри АСУ
к.ф-м.н., доцент — І.М. Дронюк

Зав. кафедри АСУ
д.т.н., проф. — І.Г. Цмоць

"ЗАТВЕРДЖУЮ"
Проректор з наукової роботи
Національного університету
"Львівська політехніка"
_____ проф. Чухрай Н.І.
"07" 06 2019 р.

АКТ

про використання результатів дисертації

"Інформаційна технологія розроблення та ідентифікації латентних зображень"

асистента кафедри автоматизованих систем управління

Троян Оксани Анатоліївни

представленої на здобуття наукового ступеня кандидата технічних наук

за спеціальністю 05.13.06 – Інформаційні технології

при виконанні науково-дослідних робіт Національного університету "Львівська політехніка".

Ми, що нижче підписалися, начальник НДЧ к.т.н., доц. Жук Л.В. та члени комісії: завідувач відділу науково-організаційного супроводу наукових досліджень к.т.н. Лазько Г.В.; завідувач планово-фінансового відділу Чулой Т.М. та завідувач кафедри інформаційних технологій видавничої справи Ткаченко Роман Олексійович цим актом підтверджуємо, що результати дисертаційної роботи асистента кафедри автоматизованих систем управління Троян Оксани Анатоліївни використано під час виконання на основі досліджень наданої грантової підтримки Державного фонду фундаментальних досліджень "Технологія підвищення графічного рівня захищеності друкованих та електронних документів" (номер державної реєстрації 0115U004704).

В рамках науково-дослідної роботи Троян О.А розробила метод формування фрактальних елементів, який базується на створенні захисної сітки, яку утворюють на основі фракталу у векторному форматі за допомогою рекурсивної процедури до генерування одиничного елементу із заданими параметрами дроблення. Фрактали будуються рекурсивною процедурою, де кожен одиничний графічний елемент постає в ролі генератора і задає величину захисного елемента. Розроблений метод демонструє процес генерування фрактального растра з прихованою інформацією для захисту друкованих документів.

Голова комісії:

Начальник науково-дослідної частини,
к.т.н., доцент Л.В. Жук

Члени комісії:

зав. відділу науково-організаційного
супроводу наукових досліджень, к.т.н. Г.В. Лазько

заст. начальника планово-фінансового
відділу Т.М. Чулой

зав. каф. інформаційних технологій видавничої справи
д.т.н., професор Р.О.Ткаченко

"ЗАТВЕРДЖУЮ"
Проректор з наукової роботи
Національного університету
"Львівська політехніка"
_____ проф. Чухрай Н.І.
"04" 05 2019 р.

АКТ

про використання результатів дисертації
"Інформаційна технологія розроблення та ідентифікації латентних зображень"
асистента кафедри автоматизованих систем управління
Троян Оксани Анатоліївни
представленої на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – Інформаційні технології
при виконанні науково-дослідних робіт Національного університету "Львівська політехніка".

Ми, що нижче підписалися, начальник НДЧ к.т.н., доц. Жук Л.В. та члени комісії: завідувач відділу науково-організаційного супроводу наукових досліджень к.т.н. Лазько Г.В.; завідувач планово-фінансового відділу Чулой Т.М. та завідувач кафедри інформаційних технологій видавничої справи Ткаченко Роман Олексійович цим актом підтверджуємо, що результати дисертаційної роботи асистента кафедри автоматизованих систем управління Троян Оксани Анатоліївни використано під час виконання науково-дослідної роботи Національного університету «Львівська політехніка»: "Відслідковування рухомих об'єктів у відеопотоках реального часу"(державний реєстраційний №0115U000432).

В рамках науково-дослідної роботи Троян О.А розробила метод ідентифікації латентних зображень за критеріальними ознаками, які побудовані на порогових характеристиках експеременталь них даних дає змогу ідентифікувати оригінальність документа. Впровадження методу ідентифікації для забезпечення достовірності документів на основі зібраних та оброблених значень параметрів створює умови для прогнозування та прийняття рішень на основі аналітичної залежності оригіналу та копії щодо оригінальності документів. Розроблена система ідентифікації латентних зображень в документах характеризується високою точністю виявлення фальсифікації.

Голова комісії:

Начальник науково-дослідної частини,
к.т.н., доцент Л.В. Жук

Члени комісії:

зав. відділу науково-організаційного
супроводу наукових досліджень, к.т.н. Г.В. Лазько

заст. начальника планово-фінансового
відділу Т.М. Чулой

зав. каф. інформаційних технологій видавничої справи
д.т.н., професор Р.О.Ткаченко

"ЗАТВЕРДЖУЮ"
Проректор з наукової роботи
Національного університету
"Львівська політехніка"
_____ проф. Чухрай Н.І.
"05" 05 2019 р.

АКТ

про використання результатів дисертації

"Інформаційна технологія розроблення та ідентифікації латентних зображень"

асистента кафедри автоматизованих систем управління

Троян Оксани Анатоліївни

представленої на здобуття наукового ступеня кандидата технічних наук

за спеціальністю 05.13.06 – Інформаційні технології

при виконанні науково-дослідних робіт Національного університету "Львівська політехніка".

Ми, що нижче підписалися, начальник НДЧ к.т.н., доц. Жук Л.В. та члени комісії: завідувач відділу науково-організаційного супроводу наукових досліджень к.т.н. Лазько Г.В.; завідувач планово-фінансового відділу Чулой Т.М. та завідувач кафедри автоматизованих систем управління Цмоць Іван Григорович цим актом підтверджуємо, що результати дисертаційної роботи асистента кафедри автоматизованих систем управління Троян Оксани Анатоліївни використано під час виконання науково-дослідної роботи Національного університету «Львівська політехніка»: "Розвиток теорії синтезу нейронних мереж на НВІС-структурах для обробки сигналів в робототехнічних системах", державний реєстраційний №0112U001204).

В рамках науково-дослідної роботи Троян О.А. розробила моделі побудови графічних пасток на основі формування геометричних перетворень ліній, які при копіюванні здійснюють часткове чи повне спотворення об'єктів, завдяки чому спрощується виявлення фальсифікації при видимому муарі. Головною метою створення графічних пасток є реалізація принципово нових методів, що є необхідною передумовою для підвищення надійності документів у процесах додрукарської підготовки. Технологія формування елементів, які завдяки їх побудови із врахуванням умов друку унеможливлюють несанкціоновану модифікацію документа запобігає порушенню цілісності та попереджає фальсифікацію, за рахунок чого зменшує ймовірність підробки.

Голова комісії:

Начальник науково-дослідної частини,
к.т.н., доцент Л.В. Жук

Члени комісії:

зав. відділу науково-організаційного
супроводу наукових досліджень, к.т.н. Г.В. Лазько

заст. начальника планово-фінансового відділу Т.М. Чулой

зав. каф. автоматизованих систем управління
д.т.н., професор І.Г. Цмоць

"Затверджую"
Начальник НГВУ»Бориславнафтогаз»
ПАТ "Укрнафта"
_____ Михайлишин І.Б.
«28 » грудня 2016 року

АКТ

Про використаннярезультатів
дисертаційної роботи Троян Оксани Анатоліївни
«Інформаційна технологія розроблення
та ідентифікації латентних зображень»
поданої до захисту на здобуття
наукового ступеня кандидата технічних наук

Комісія у складі головного інженера НГБУ «Бориславнафтогаз» В.В.Костецького, начальника відділу впровадження та експлуатації інформаційних систем В.С. Кузбит, інженера з комп'ютерних систем відділу впровадження та експлуатації інформаційних систем Гороховатського С.В. склали даний акт про те, що у НГВУ "БОРИСЛАВНАФТОГАЗ" ПАТ "УКРНАФТА" використовуються результати дисертаційних досліджень роботи Троян Оксани Анатоліївни «Інформаційна технологія розроблення та ідентифікації латентних зображень » для підвищення достовірності друкованих документів та збереження надійності оригінальних даних в документах за допомогою ідентифікації персоніфікуючих атрибутів.

Необхідність збереження оригінального (первинного) вмісту друкованих та електронних документів, особливо у випадках оперативної перевірки та аналізу достовірності даних в системі збереження та обробки даних друкованої продукції було використано формування графічних атрибутів для контролю, класифікації та виявлення спотворень в документах, в основу якийх по кладено такі результати дисертаційної роботи:

1)Модель утворення графічних пасток, які формуються при створенні тонких паралельних ліній з шириною 0,25мм та частотами повторень, які кратні цілому числу і виявляються при муарі для друкованих документів

2)Метод формування латентних елементів на основі побудови графічних елементів, який завдяки використанню технології накладанні шарів з деякими градієнтними характеристиками підвищує ефективність виявлення часткової чи повної зміни документа.

3)Отримано інструкції для використання розробленої технології та визначення оригінальності документів

Використання зазначених результатів дисертаційної роботи Троян О.А. дає можливість підвищення рівня своєчасного виявлення несанціонованих спотворень друкованих чи електронних документів , а також унеможливлює копіювати, відтворювати, змінювати та частково модифікувати документи за рахунок складності відтворення латентних елементів.

Використання результатів дисертаційної роботи на основі аналітичної залежності оригіналу та копії підтвердили свою ефективність та зменшили кількість документів, які могли зазнати фальсифікації.

Комісія у складі :

Голова комісії

головний інженер
НГВУ «Бориславнафтогаз» _____В.В.Костецький,

Члени комісії:

начальник ВВ та ЕІС _____В.С. Кузбит,

інженер з комп'ютерних систем
ВВ та ЕІС _____Гороховатський С.В.

ДОДАТОК 3
Частина програмного коду розробленого ПЗ

```
const
LatentLibrary = loadLibrary('Latent_CommonLib', loadLibrary);
var currentPlatform = Latent.config.platformName.toLowerCase();
const
MOIRE = resources[Latent.config.deviceModel];
LatentLibrary.setLocTol(Latent.config.location, 0.01);
Step('Perform Image sequence.', function() {
    pump.SetDate('2019-01-25 02:00:45');
    pump.TherapyStates.therapyControlState = 0x55; // remove redline
    pump.TherapyStates.autoModeState = 0x02;
    LatentLibrary.initial_sequence(Latent, pump, true);
    Latent.waitUntilears(Latent.uiID.HomePanel., 30);
});
Observe("Observe that screen is displayed", {
    actual : IsElementPresentOnScreen(Latent.uiID.HomePanel.),
    expected : true
});
Step("Lock device.", function() {
    lockDevice();
});
Observe("Observe that device locked", {
    actual : IsElementNotPresentOnScreen(Latent.uiID.HomePanel., Latent.uiID.HomePanel.,
Latent.uiID.HomePanel.),
    expected : true
});
Step("Generate 1.Image(Not licable)(fault 001).", function() {
    actualTime = pump.GetTimeString();
    pump.TrigerFault("NM_CLEARED_E");
});
if (currentPlatform === "fractal") {
    Step("Turn on LCD.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
    });
    Latent.waitUntilears(Latent.uiID, 5);
    elemName = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationName, 5);
    Observe("Observe  that  image on locked screen is displayed", {
        actual : elemName.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Name)
    });
    elemIcon = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationImage, 5);
    Observe("Observe  that  Image on locked screen is displayed", {
        actual : elemIcon.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Image)
    });
}
else {
    Latent.waitUntilears("name|NotificationShortLookView", 80);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
if (currentPlatform === "fractal") {
    element = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader);
```

```
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : element.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
Step("Expand System Dismissible Notification.", function() {
    expandDismissibleNotification();
});
if (currentPlatform === "fractal") {
    elem = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationDetail, 4);
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : elem.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
else {
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
Verify("Verify that System Dismissible Notification is displayed expanded with timestamp", {
    actual : IsElementPresentOnScreen(Latent.uiID.PopUpNotifications.NotificationTime),
    expected : true,
});
Step("Tap on the System Dismissible Notification.", function() {
    tapOnSystemDismissibleNotification();
});
var timeLabel = getProperty(Latent.uiID.PopUpNotifications.NotificationTime, 'text');
timeLabel = timeLabel.substring(3, timeLabel.length);
actualTime = actualTime.substring(1, actualTime.length);
Verify("Verify that timestamp on the Notification is equal to time when the fault was
generated on the pump.", {
    actual : actualTime,
    expected : timeLabel
});
Verify("Verify that the Latent   navigate to Home Screen if user taps on System Dismissible
Notification", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
if (currentPlatform === "fractal") {
    Step("Open the Notification Center Identification.", function() {
        Latent.qm_openNotificationCenter();    });}
else {
    Step("Navigate to Identification screen.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.wait(1);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(2);
        Latent.wait(0.5);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(3);
    });
}
if (currentPlatform === "fractal") {
```

```
    elem3 = Latent.waitUntilears(Latent.uiID.NotificationCenter.Notif, 5);
    Verify("Verify that last Latent image displayed correctly on Notification Center
Identification", {
        actual : elem3.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Notif)
    });
    elem4 = Latent.waitUntilears(Latent.uiID.NotificationCenter.NotifActive, 5);
    Verify("Verify that Active  value displayed on Notification Center Identification", {
        actual : elem4.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_NotifActive)
    });
}
else {
    Verify("Verify that last Latent image displayed correctly on Notification Center
Identification", {
        actual : getProperty(Latent.uiID.NotificationCenter.Notif, "text"),
        expected : "100"
    });
    Verify("Verify that Latent  displays Active  value.", {
        actual : getProperty(Latent.uiID.NotificationCenter.NotifActive, "text"),
        expected : "0.5 U"
    });
}
Step("Tap on the Notification Center Identification.", function() {
    tapOnNotificationCenterIdentification();
});
Verify("Verify that the Latent   navigate to Home Screen if user taps on Notification Center
Identification. ", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
Step("Dismiss OS Notification.", function() {
    DismissOSNotification();
});
Verify("Verify that Latent   allows the user to dismiss a shown Notification from the
display.", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeScreen)
});
if (currentPlatform === "fractal") {
    Step("Turn on LCD.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
    });
    elemName = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationName, 5);
    Observe("Observe  that   name on locked screen is displayed", {
        actual : elemName.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Name)
    });
    elemIcon = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationImage, 5);
    Observe("Observe  that  Image on locked screen is displayed", {
        actual : elemIcon.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Image)
    });
}
else {
    Latent.waitUntilears("name|NotificationShortLookView", 65);
    Latent.wait(1);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
```

```
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
if (currentPlatform === "fractal") {
    element = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : element.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
Step("Expand System Dismissible Notification.", function() {
    expandDismissibleNotification();
});
if (currentPlatform === "fractal") {
    elem = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationDetail, 5);
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : elem.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
else {
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
Verify("Verify that System Dismissible Notification is displayed expanded with timestamp", {
    actual : IsElementPresentOnScreen(Latent.uiID.PopUpNotifications.NotificationTime),
    expected : true,
});
Step("Tap on the System Dismissible Notification.", function() {
    tapOnSystemDismissibleNotification();
});
var timeLabel = getProperty(Latent.uiID.PopUpNotifications.NotificationTime, 'text');
timeLabel = timeLabel.substring(3, timeLabel.length);
actualTime = actualTime.substring(1, actualTime.length);
Verify("Verify that the Latent navigate to Home Screen if user taps on System Dismissible
Notification", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
if (currentPlatform === "fractal") {
    Step("Open the Notification Center Identification.", function() {
        Latent.qm_openNotificationCenter();
        Latent.wait(3);
    });
}
else {
    Step("Navigate to today Identification screen.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.wait(1);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(2);
        Latent.wait(0.5);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
```

```
        Latent.wait(3);
    });
}
if (currentPlatform === "fractal") {
    elem3 = Latent.waitUntilears(Latent.uiID.NotificationCenter.Notif, 5);
    Verify("Verify that last Latent imagedisplayed correctly on Notification Center
Identification", {
        actual : elem3.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Notif)
    });
    elem4 = Latent.waitUntilears(Latent.uiID.NotificationCenter.NotifActive, 5);
    Verify("Verify that Active  value displayed on Notification Center Identification", {
        actual : elem4.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_NotifActive)
    });
}
else {
    Verify("Verify that last Latent imagedisplayed correctly on Notification Center
Identification", {
        actual : getProperty(Latent.uiID.NotificationCenter.Notif, "text"),
        expected : "100"
    });
    Verify("Verify that Latent  displays Active  value.", {
        actual : getProperty(Latent.uiID.NotificationCenter.NotifActive, "text"),
        expected : "0.5 U"
    });
}
Step("Tap on the Notification Center Identification.", function() {
    tapOnNotificationCenterIdentification();
});
Verify("Verify that the Latent   navigate to Home Screen if user taps on Notification Center
Identification. ", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
Step("Dismiss OS Notification.", function() {
    DismissOSNotification();
});
Verify("Verify that Latent   allows the user to dismiss a shown Notification from the
display.", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeScreenAlerCleared)
});
if (currentPlatform === "fractal") {
    Step("Turn on LCD.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader, 5);
    });
    elemName = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationName, 5);
    Observe("Observe  that   name on locked screen is displayed", {
        actual : elemName.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Name)
    });
    elemIcon = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationImage, 5);
    Observe("Observe  that  Image on locked screen is displayed", {
        actual : elemIcon.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Image)
    });
}
```

```
else {
    Latent.waitUntilears("name|NotificationShortLookView", 65);
    Latent.wait(1);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
if (currentPlatform === "fractal") {
    element = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : element.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
Step("Expand System Dismissible Notification.", function() {
    expandDismissibleNotification();
});
if (currentPlatform === "fractal") {
    elem = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationDetail, 4);
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : elem.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
else {
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
Verify("Verify that System Dismissible Notification is displayed expanded with timestamp", {
    actual : IsElementPresentOnScreen(Latent.uiID.PopUpNotifications.NotificationTime),
    expected : true,
});
Step("Tap on the System Dismissible Notification.", function() {
    tapOnSystemDismissibleNotification();
});
if (currentPlatform === "fractal") {
    Step("Open the Notification Center Identification.", function() {
        Latent.qm_openNotificationCenter();
        Latent.wait(3);
    });
}
else {
    Step("Navigate to today Identification screen.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.wait(1);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(2);
        Latent.wait(0.5);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(3);
    });
}
```

```
if (currentPlatform === "fractal") {
    elem3 = Latent.waitUntilears(Latent.uiID.NotificationCenter.Notif, 5);
    Verify("Verify that last Latent image displayed correctly on Notification Center
Identification", {
        actual : elem3.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Notif)
    });
    elem4 = Latent.waitUntilears(Latent.uiID.NotificationCenter.NotifActive, 5);
    Verify("Verify that Active  value displayed on Notification Center Identification", {
        actual : elem4.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_NotifActive)
    });
}
else {
    Verify("Verify that last Latent image displayed correctly on Notification Center
Identification", {
        actual : getProperty(Latent.uiID.NotificationCenter.Notif, "text"),
        expected : "100"
    });
    Verify("Verify that Latent  displays Active  value.", {
        actual : getProperty(Latent.uiID.NotificationCenter.NotifActive, "text"),
        expected : "0.5"
    });
}
Step("Tap on the Notification Center Identification.", function() {
    tapOnNotificationCenterIdentification();
});
Verify("Verify that the Latent   navigate to Home Screen if user taps on Notification Center
Identification. ", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
Step("Dismiss OS Notification.", function() {
    DismissOSNotification();
});
Verify("Verify that Latent   allows the user to dismiss a shown Notification from the
display.", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeScreenAlerCleared)
});
if (currentPlatform === "fractal") {
    Step("Turn on LCD.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader, 5);
    });
    elemName = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationName, 5);
    Observe("Observe  that   name on locked screen is displayed", {
        actual : elemName.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Name)
    });
    elemIcon = Latent.waitUntilears(Latent.uiID.NotificationCenter.identificationImage, 5);
    Observe("Observe  that  Image on locked screen is displayed", {
        actual : elemIcon.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Image)
    });
}
else {
    Latent.waitUntilears("name|NotificationShortLookView", 65);
    Latent.wait(1);
```

```
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
if (currentPlatform === "fractal") {
    element = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationHeader);
    Verify("Verify that the Notification Banner ears with correct System Notification
information.", {
        actual : element.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Notification_Banner)
    });
}
Step("Expand System Dismissible Notification.", function() {
    expandDismissibleNotification();
});
if (currentPlatform === "fractal") {
    elem = Latent.waitUntilears(Latent.uiID.PopUpNotifications.NotificationDetail, 4);
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : elem.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
else {
    Verify("Verify that System Dismissible Notification is displayed expanded with the
ropriate System Notification information", {
        actual : Latent.takeScreenshot(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_description)
    });
}
Verify("Verify that System Dismissible Notification is displayed expanded with timestamp", {
    actual : IsElementPresentOnScreen(Latent.uiID.PopUpNotifications.NotificationTime),
    expected : true,
});
Verify("Verify that the Latent   navigate to Home Screen if user taps on System Dismissible
Notification", {
    actual : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
if (currentPlatform === "fractal") {
    Step("Open the Notification Center Identification.", function() {
        Latent.qm_openNotificationCenter();    });}
else {
    Step("Navigate to today Identification screen.", function() {
        Latent.executeScript("Latent:presskey", [{
            "keySequence" : "HOME"
        }]);
        Latent.wait(1);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(2);
        Latent.wait(0.5);
        Latent.ipe("10%", "50%", "90%", "50%", 200);
        Latent.wait(3);
    });
}
if (currentPlatform === "fractal") {
    elem3 = Latent.waitUntilears(Latent.uiID.NotificationCenter.Notif, 5);
    Verify("Verify that last Latent imagedisplayed correctly on Notification Center
Identification", {
```

```
        actual : elem3.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_Notif)
    });
    elem4 = Latent.waitUntilears(Latent.uiID.NotificationCenter.NotifActive, 5);
    Verify("Verify that Active  value displayed on Notification Center Identification", {
        actual : elem4.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fault_NotifActive)
    });
}
else {
    Verify("Verify that last Latent imagedisplayed correctly on Notification Center
Identification", {
        actual : getProperty(Latent.uiID.NotificationCenter.Notif, "text"),
        expected : "100"
    });
    Verify("Verify that Latent  displays Active  value.", {
        actual : getProperty(Latent.uiID.NotificationCenter.NotifActive, "text"),
        expected : "0.5 PIXEL"
    });
}
Step("Tap on the Notification Center Identification.", fpixelnction() {
    tapOnNotificationCenterIdentification();
});
Verify("Verify that the Latent   navigate to Home Screen if pixelser taps on Notification
Center Identification. ", {
    actpixelal : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeNotification)
});
Step("Dismiss OS Notification.", fpixelnction() {
    DismissOSNotification();
});
Verify("Verify that Latent   allows the pixelser to dismiss a shown Notification from the
display.", {
    actpixelal : Latent.takeScreenshot(),
    expected : LatentLibrary.getExptdReithLocTol(MOIRE.HomeScreenAlerCleared)
});
if (cpixelrrentPlatform === "fractal") {
    Step("Tpixelrn on LCD.", fpixelnction() {
        Latent.execpixelteScript("Latent:presskey", [{
            "keySeqpixelence" : "HOME"
        }]);
        Latent.waitPIXELntilears(Latent.pixeliID.PopPIXELpNotifications.NotificationHeader,
5);
    });
    elemName =
Latent.waitPIXELntilears(Latent.pixeliID.NotificationCenter.identificationName, 5);
    Observe("Observe  that   name on locked screen is displayed", {
        actpixelal : elemName.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fapixellt_Name)
    });
    elemIcon =
Latent.waitPIXELntilears(Latent.pixeliID.NotificationCenter.identificationImage, 5);
    Observe("Observe  that  Image on locked screen is displayed", {
        actpixelal : elemIcon.cropImg(),
        expected : LatentLibrary.getExptdReithLocTol(MOIRE.Fapixellt_Image)
    });
```