УДК 004.056.5:655.25

М. А. Назаркевич, О. А. Троян
Національний університет “Львівська політехніка”,
кафедра інформаційних технологій видавничої справи

РОЗРОБЛЕННЯ ПРОГРАМНОГО ПРОДУКТУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПЛІВОК ІЗ ПРИХОВАНИМ ЛАТЕНТНИМ ЗОБРАЖЕННЯМ

Розроблено новий метод захисту даних, в основу якого покладено безпеку друку. В загальному випадку цей метод може бути застосований для безпеки фінансових документів, таких як банкноти та цінні папери. Метод захисту створює приховані повідомлення чи зображення, котрі стають видимими на підроблених документах. Розглянуто шлях підвищення ефективності виявлення цифрових зображень та локалізації несанкціонованого впливу “copy paste”.

Ключові слова: безпека друку, латентні зображення, документи.

PROGRAMME PRODUCT DEVELOPMENT FOR INFORMATION PROTECTION ON THE GROUND OF FILMS WITH HIDDEN LATENT IMAGES

The authors developed a new data protection method, which is based on security printing. This method can be employed for protecting financial documents such as banknotes and securities in general. The protection method creates hidden messages or images, which become visible on counterfeited documents. The way of increasing the efficiency of digital image detection and localization of unauthorized interference “copy paste”.

Key words: security printing, latent images, documents.

Вступ

Для захисту документів розробляють та застосовують комплекси заходів безпеки. Особливу роль у питаннях захисту відіграють друковані та електронні документи. Щоб забезпечити надійний захист, необхідно впроваджувати нові технології, основані на сучасних програмних та апаратних засобах. Розроблена концепція побудови захисту інформації з урахуванням критеріїв надійності, ефективності та економічності узагальнила методи та засоби захисту, що дало можливість розвинути захист інформації та підвищити його ступінь.

Постановка проблеми

У цій роботі розроблено програмні засоби для захисту друкованих документів. Одним з напрямків досліджень є створення друкованого документа з прихованим латентним зображенням. Запропоновано програмне забезпечення та технологію формування латентних елементів на друкованому документі, що міститиме додаткову плівку-детектор, яка визначатиме достовірність документа. Ця технологія та програмне забезпечення відповідають світовим стандартам якості поліграфічної продукції згідно ISO 9001:2000.

Аналіз методів та засобів захисту зображень

Високий ступінь захисту поліграфічної продукції визначається трьома складовими: складністю технологічних процесів, обмеженням доступу до матеріалів та обладнання, новизною і закритістю застосовуваних методів.

Розроблення і застосування технологій друку, наприклад, металографічного, глибокого способу друку, використання спеціальних фарб і лакування, нанесення голограм не завжди доцільні з економічного погляду. Застосування матеріалів зі спеціальними хімічними, фізичними властивостями спричиняє використання спеціального обладнання для визначення автентичності продукції.

Найпростішими, зручними і економічно доцільними є засоби захисту, що реалізуються на додрукарському етапі. Їх застосування не вимагає спеціального устаткування і матеріалів. При цьому залишається можливість їх використання для створення комбінованих засобів захисту.

Для захисту від підробки використовують такі технології для друкованої продукції. Їх можна поділити на п’ять великих груп [1]:

1. Захист на стадії дизайну за допомогою спеціальних видів верстки та опрацювання зображень: гільйошні елементи; спеціальні лінійні растри; гравюри; спеціальні “дефекти”; мікротекст; об’ємні ефекти; приховані елементи; зображення, що поєднуються; контрольні і штрихові коди і ноу-хау.

2. Технологічні способи друку: орловський спосіб друку; ірисовий спосіб друку; металографічний спосіб друку; офсетний спосіб друку з глибоких форм; трафаретний спосіб друку; глибокий спосіб друку; шестифарбовий друк; офсет без зволоження.

3. Захист на основі особливостей паперу або іншої основи, на яких здійснюється друк: водяні знаки; захисні кольорові волокна; металізовані смужки; планшетки; матеріали, чутливі до розчинників; флюоресцентні частинки і т.д.

4. Захист на основі спеціальних фарб чи інших носіїв друкованої інформації.

5. Застосування окремих післядрукарських операцій.

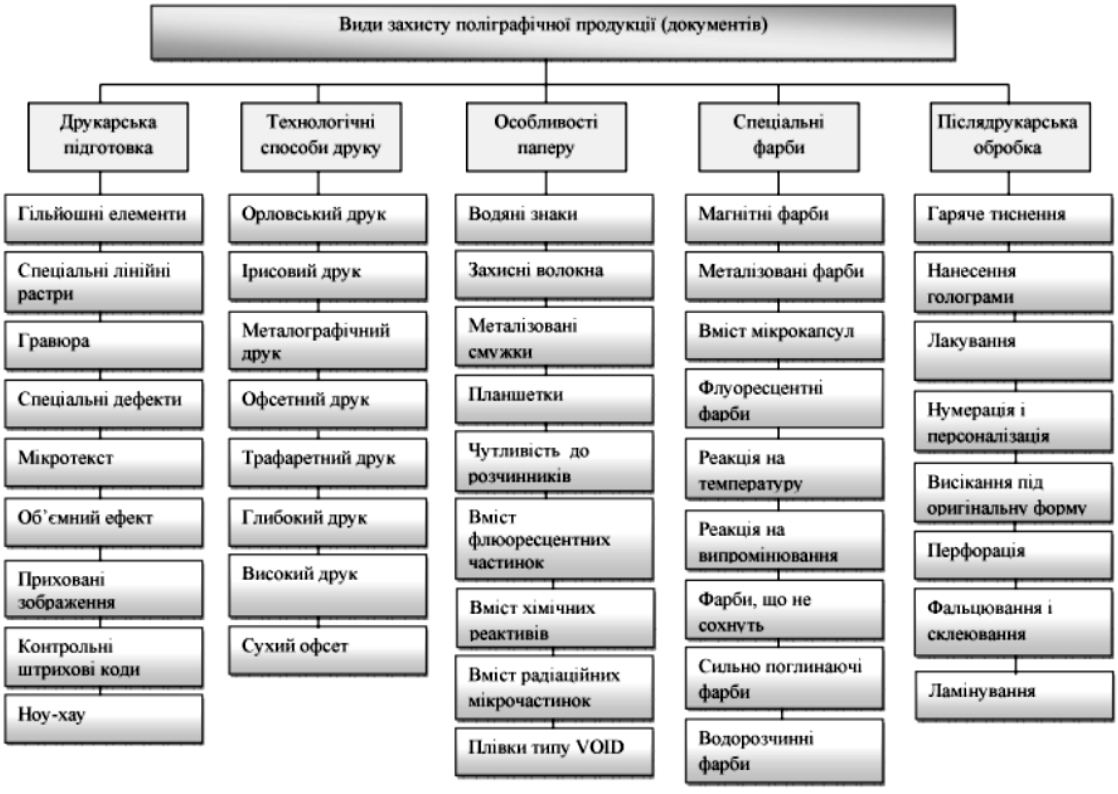


Рис. 1. Методи й засоби захисту інформації

Важливу роль у захисті від фальсифікації і підробки відіграють спеціальні заходи і методи, спрямовані на захист інформації документів, цінних паперів і банкнот від дублювання.

Для захисту документів застосовуються суміщені зображення, в яких одна частина малюнка наноситься на лицьовий бік, а інша частина друкується на зворотному. На просвіт всі елементи суміщеного зображення повинні збігтися і утворити цілісний малюнок. Подібні зображення

формуються так, що непофарбовані деталі малюнка стають кольоровими завдяки забарвленим частинам малюнка протилежного боку плівки. Суміщені зображення виготовляють на спеціальних машинах і створити їх вручну або в умовах загальної поліграфії практично неможливо.

Для створення надійного захисту сьогодні необхідно розробляти програмні та апаратні засоби для приховування інформації у документі. Для поліграфічного відбитка атрибутами прихованого зображення є друк стохастичним растром; чи наявність упорядкованої структури при растуванні; чи наявність оригінального растрування з великою кількістю растрових точок, які при збільшенні стають нечіткими і розмитими, чи, звичайно, ноу-хау в області фарб і паперів.

Аналіз технологій захисту інформації

Останнім часом спеціалізовані фірми розробляють свої ноу-хау для захисту документів.

Фірма Security Soft [8] є провідною у розробленні програмних засобів для створення документів, цінних паперів і банкнот для захисту їх від фальсифікації і підробки. Займається розробленням методів, алгоритмів і програм для розробників і виробників захищеної поліграфічної продукції.

Brand security system [7] – компанія, яка розробляє методи захисту документів, використовуючи під час друку мітки й захисні марки. Використовують для захисту пакування.

Захист здійснюють такими способами: 1. Захист міткою за допомогою вбудованого прихованого зображення, яке проявляється за допомогою прозорого пластикового декодера. 2. Захист з прихованим зображенням, яке вбудовано в папір, та виявляється за допомогою пластикового декодера. 3. Захист за допомогою прихованого зображення, яке вбудовується в полотно; стає видимим при накладенні плівки.

Компанія Guardsoft розробила технології захисту Ghost on Duty [4], яка містить декоративні гільйошні елементи, гравіювання, мікротекст і складні векторні сітки. Всі ці елементи максимально захищають інформацію в документі. Суть захисного ефекту всіх елементів полягає в тому, що: елементи візерунка мають бути достатньо тонкими, у такому випадку при скануванні створюються помилки та неточності; елементи візерунка мають мати нерегулярну структуру, у такому випадку їх важко відтворити, дублювати чи ретушувати; елементи різних кольорів слід застосовувати так, щоб після сканування їх було неможливо поділити на різні шари.

Документи, які захищені технологіями компанії Guardsoft, є надійними, що є першим фактором захисту. Якщо відбувається фальсифікація, тобто копіювання документа, то стають помітними зміни в растровій структурі зображення. Так можна виявити підробку документа. Наявність надрукованого зразка легко відрізнити від оригінального зображення, що відображає певну кількість геометричних спотворень, що також відображається в муарі при застосуванні спеціальної плівки. Плівка допоможе визначити достовірність документа. Другим важливим фактором є чіткість зображення. При звичайному копіюванні якість зображення значно погіршується, дрібні деталі зникають і зображення стає розмитим.

Фірмою запропоновано вид захисту, який базується на використанні особливого виду фарб. Якщо документ містить два кольори: темно-синій і помаранчевий, захист будується на основі додавання до темно-синього кольору 30 % срібної фарби і до помаранчевого кольору 30 % бронзової фарби. Особливістю вказаних домішок в фарбах є те, що фарби відтворюють блиск, а при скануванні блиск не відображається. Таким чином при фальсифікації, використовуючи той самий вид паперу, але не маючи рецептури фарб, підробку буде помітно через різницю кольорів тексту. Скануючи документ і здійснюючи кольороподіл, отримаємо стандартні кольори CMYK, які не відтворюватимуть повністю оригінал.

Компанія Guardsoft розробила технологію захисту для багатоколірних зображень. Розробка полягає у зміні растра на всіх кольорах. В геометричних спотвореннях структури растра застосовують сітку щільних тонких паралельних ліній, що дає можливість використати плівку-декодер, яка дозволить перевірити оригінальність документа. Застосувавши таку плівку для будь-якого іншого зображення, отримаємо монотонний муар по всій поверхні. На оригінальному зображенні в контурних лініях приховане зображення стає видимим.

Основні функції технології компанії Guardsoft: відтворення однотонних та багатоколірних зображень; використання класичних і декоративних форм растра;плавний перехід між різними формами растра; зміна растра на основі додаткового зображення; зміна растра на основі математичних формул; геометрична деформація структури растра; введення одного або двох прихованих додаткових зображень; генерація плівок, що показують приховані зображення.

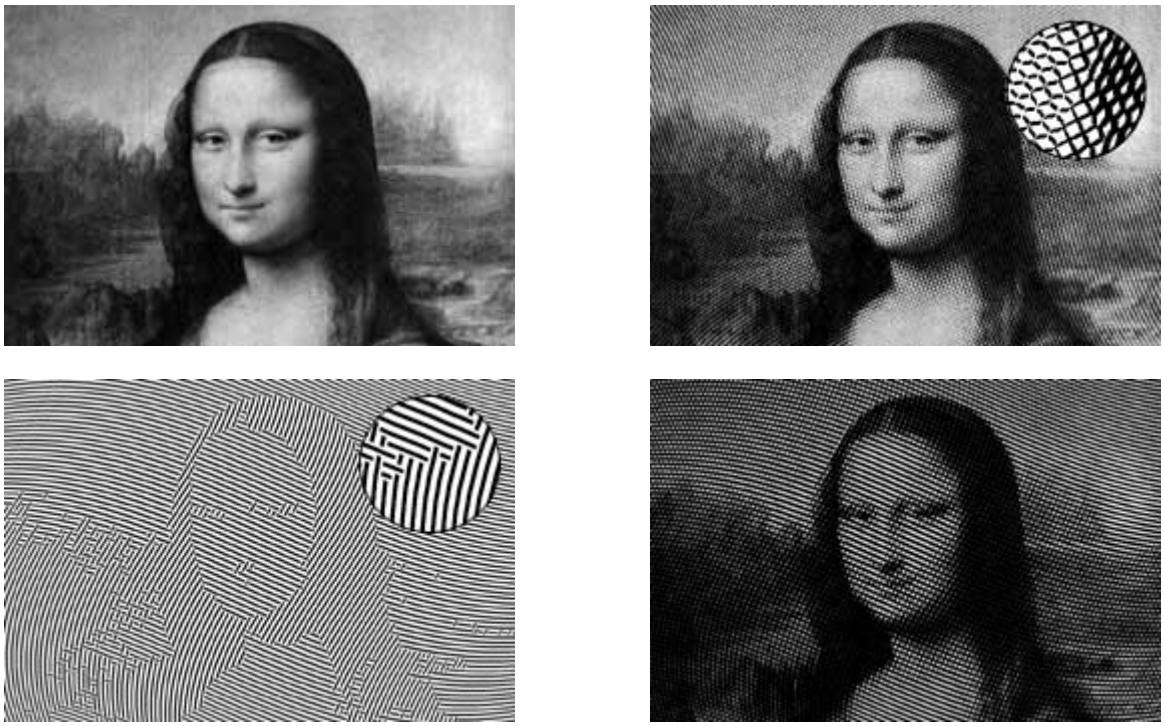


*Рис 3. Захист за допомогою плівки, розроблений Guardsoft технологією Ghost on Duty**[4]***

Формування цілей статті

У цьому дослідженні розроблено метод захисту інформації на основі плівок із прихованим латентним зображенням. Існуючі технології ghost on Duty, line deflection images and latent images є ефективними і можуть бути застосовані для виготовлення документів з високим ступенем захисту. Розроблення програмного продукту для підвищення ступеня захисту передбачає наявність додаткових плівок, які розроблені з врахуванням перетворень колірних просторів та остаточній генерації CMYK + плівка. На основі математичного апарату security генеруються 4 основні плівки та плівка-детектор. Плівка-детектор містить захисний ключ та є компонентом, що доповнює готове зображення.

Виклад основного матеріалу

Будь-яке зображення можна представити в одному з двох видів: растровому або векторному. У векторному форматі зображення будується на базі деяких примітивів, наприклад, прямих ліній, сплайнів і т.д. У випадку растру (bitmap) зображення зберігається як двовимірний масив, причому кожен елемент цього масиву (піксель) зберігає (у деякому вигляді) колір відповідної крапки. Растрові зображення, своєю чергою, діляться на зображення з палітрою і без неї. У випадку зображення з палітрою колір зберігається як індекс у деякій палітрі (яку теж необхідно зберігати). Якщо виділяється n бітів на піксель, то палітра повинна зберігати 2^n кольорів.

Колірність зображення зберігатися в різних форматах. Одним з найпростіших є формат у градаціях сірого (grayscale), при якому значення пікселя зберігає інформацію про яскравість відповідного пікселя. При цьому якщо виділяється n бітів на піксель, то можна зберегти 2^n градацій сірого.

Вхідними файлами для створення фонових сіток можуть бути будь-які векторні зображення. У випадку растрових рисунків кращим є контрастне зображення, в якому прослідковується великий перепад світлоти і тіней. Структура прихованого зображення з високим ступенем захисту складається з двох прихованих зображень, які накладаються. Кожне з накладених прихованих зображень видно з різних кутів зору. Визначають елементи рельєфу для кожного прихованого зображення, що передаються частинами відповідним лінійним структурам для полегшення утворення зображення і тла, які співпрацюють для створення прихованого зображення. Елементи рельєфу надаються тільки в місцях, де лінійні структури рельєфу першого і другого прихованого зображення перетинаються. У результаті створюється приховане зображення, яке має перевагу стосовно плоского вигляду та допомагає приховати присутність будь-якого з прихованих зображень, що накладаються.

Колірний простір у моделі RGB (Red, Green, Blue) задається як куб у декартовій системі координат. Кожен колір задається вершиною цього куба і визначається як сума основних кольорів. Основні кольори (червоний, зелений і синій) є адитивними основними кольорами. Так, малиновий колір як сума червоного і синього задається вершиною (1, 1, 0). Головна діагональ куба з однаковими кількостями кожного основного кольору представляє ахроматичні (сірі кольори): чорному кольору відповідає крапка (0, 0, 0), а білому – (1, 1, 1).

У кольоровому друці частіше використовуються моделі CMY (Cyan, Magenta, Yellow) і CMYK (Cyan, Magenta, Yellow, Black). Ці моделі на відміну від RGB є субтрактивні – для того, щоб одержати необхідний колір, базові коліри віднімаються від білого кольору. Розглянемо, як це відбувається. Коли на папір наноситься блакитний (cyan) колір, то червоне світло, падаючи на папір, повністю поглинається. Отже, голуба фарба віднімає червоне світло з падаючого білого (як суми червоного, синього і зеленого світла). Аналогічно малинова (magenta) фарба поглинає зелене, а жовта фарба – синє світло. Поверхня, покрита голубою і жовтою фарбою, поглинає червону і синю, залишаючи тільки жовту компоненту. Голуба, жовта і малинова фарби поглинають всі три світла, залишаючи в результаті чорну. Ці співвідношення можна представити у вигляді формул

$$C = 1 - R, M = 1 - G, Y = 1 - B \tag{1}$$

Існує багато причин, внаслідок яких доцільно використовувати чорний колір як основний, а не отримувати його в результаті змішування голубого, жовтого і малинового. Тому виходить модель CMYK. Для переходу до неї від моделі CMY застосовують формулу

$$\begin{aligned} K &= \min(1 - R, \quad 1 - G, \quad 1 - B), \\ C &= \frac{(1 - R - K)}{1 - K} \\ M &= \frac{(1 - G - K)}{1 - K} \\ Y &= \frac{(1 - B - K)}{1 - K} \end{aligned} \tag{2}$$

де C, M, Y, K – нормовані до діапазону $[0 \ldots 1]$ густини голубої, пурпурної, жовтої та чорних фарб, а R, G, B – числові координати червоного, зеленого та синього кольорів, нормовані до діапазону $[0 \ldots 1]$ [1].

Вхідними зображеннями можуть бути чорно-білі та кольорові. Кольорові рисунки програмне забезпечення сприймає, як правило, у кольоровій моделі RGB. Для створення фонової сітки, яка має бути виконана за правилами додрукарської підготовки для тиражування, необхідно перетворити її на іншу кольорову модель, яка використовується саме у поліграфії – CMYK. Для цього використовуємо формули перетворення цих моделей та їх взаємозв’язок.

З формального погляду процес перетворення колірної інформації можна описати системною моделлю репродукційного процесу, яка містить множину характеристик, функцій і відображень, а також мету репродукційного процесу і може бути представлена у вигляді таких співвідношень:

$$S =< X, O, v, C, M > \tag{3}$$

$$\begin{cases} X = F(O, v, U, C, M), \\ O = \{R_i, G_i, B_i\}_{i=1,\dots,n} \\ M = \{X_x, Y_y, Z_z\}, \\ C = (\tilde{C}, \overline{C}), \quad \overline{C} = \left(\overline{x}(\lambda), \overline{y}(\lambda), \overline{z}(\lambda)\right), \quad \tilde{C} = \{C_j\}_{j=1,\dots,N}, \text{де } C_j = \{S_i(\lambda)\}_{i=1,\dots,34} \end{cases}$$

де X – координати елементів зображення, які характеризують відбиток; O – набір координат пікселів зображення, характеристики оригіналу; $v = \{\Phi_i^j\}$ профілі пристроїв, які задані набором відображень Φ_i^j, що здійснюють пряме перетворення між апаратно-залежним і апаратно-незалежним колірними просторами *i*-го пристрою для *j*-ї мети передачі кольору; ε – похибка узгодження колірних охоплень; U – градаційні перетворення, кольорокорегування; C – умови перегляду поліграфічного продукту (спектральні характеристики та колірні координати точки білого випромінювача); M – характеристики фарби та паперу.

Під час підготовки поліграфічної продукції до друку слід враховувати, що споживач сприймає графічну інформацію в умовах діючих джерел освітлення, кількість яких, припустімо, дорівнює *N*. На формування основних стимулів у зоровій системі людини при візуальному оцінюванні кінцевого поліграфічного продукту споживачем впливають такі фактори, як умови перегляду, а також характеристики фарби та паперу. До умов перегляду належать: параметри освітлення [] $\tilde{C} = \{C_i\}_{i=1,\dots,N}$, зумовлені спектральним складом *i*-го джерела випромінювання

$$C_i = \{S_i(\lambda)\}, \tag{4}$$

де S_i – спектр фактичного джерела випромінювання у видимому діапазоні довжин хвиль λ =380..720 нм, та особливості сприйняття кольору зоровою системою людини – функції додавання $\overline{x}(\lambda), \overline{y}(\lambda), \overline{z}(\lambda)$, що визначають відгуки фоторецепторів стандартного спостерігача. До характеристик фарби та паперу належать колірні координати точки білого носія $M_1 = \{X_x, Y_y, Z_z\}$, що залежать від характеристик поліграфічних фарб і відбивної здатності задруковуваного матеріалу.

Технологія виготовлення прихованих (латентних) зображень грунтується на тому факті, що впорядкованій полімерній структурі властива оптична анізотропія. Впорядковані полімерні структури, що формують зображення або текст, нанесені на поверхню, створюють ефект латентного зображення. Крім цього, в захисний елемент входять ще кілька шарів: основний шар, шар з латентним зображенням, відображаючий шар. Шар з прихованим зображенням може містити будь-яку текстову, графічну (фото, логотип, ілюстрація) або змінну інформацію, наприклад, нумерацію.

Програмний продукт для захисту інформації на основі плівок з прихованим латентним зображенням оснований на тому, що в систему подають зображення в форматі RGB. Є наявний банк еталонів, ключів у колірній системі RGB. На першому етапі здійснюється перетворення колірних координат та забезпечення єдиного колірного простору в системі. На наступному етапі відбувається перетворення CMYK+ плівка-детектор, враховуючи вибраний ключ з банку ключів. Здійснюємо растрування документа розробленими програмними засобами з врахуванням показників лініатури растру, роздільчої здатності та кількості фарб. Відбувається перевірка якості растрованого відбитку і якщо отриманий результат не задовольняє вимоги, растрування відбувається повторно, вводимо нові показники параметрів растрування та повторюємо процедуру. В результаті отримуємо чотири плівки і плівку-детектор (рис. 5).

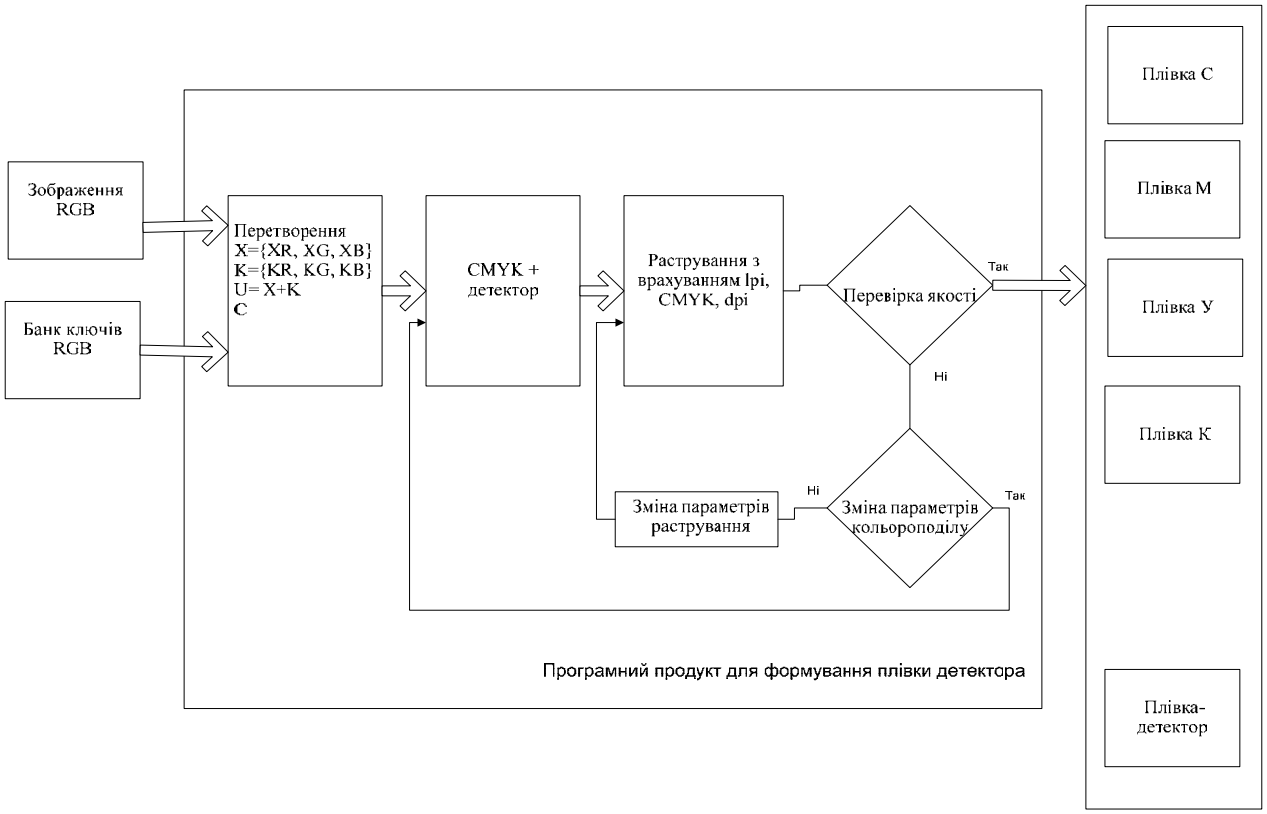
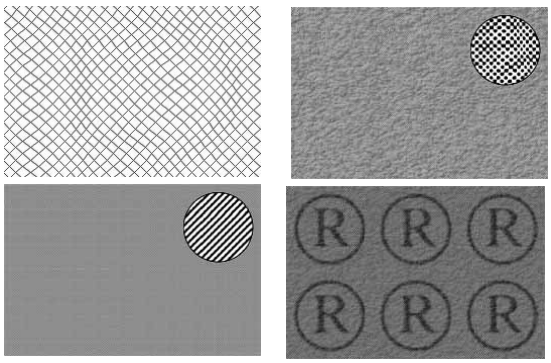


Рис. 5. Схема програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням

Розроблення методу захисту документів:
1. Растрування початкового зображення
2. Створення захисної сітки із заповненням 40 %
3. Встановлення кута сітки на 0 градусів
4. Генерація деформації сітки щодо зображення
5. Генерація видалених даних на плівку
6. Друк зображення та роздрук плівки
7. Накладання зображення та плівки із прихованими елементами



Висновок

Розроблено програмний продукт для захисту інформації на основі плівок з прихованими латентними зображеннями. Суть цієї технології полягає у розробленні елементів поліграфічного захисту, а саме – захисних плівок на основі прихованих елементів. Для розроблення програмного продукту для підвищення ступеня захисту використано додаткові плівки, які розроблені з врахуванням перетворень колірних просторів та остаточної генерації CMYK + плівка. На основі математичного апарату security генеруються 4 основні плівки та плівка-детектор. Плівка-детектор містить захисний ключ та є компонентом, що доповнює готове зображення. Створено зразки фонових зображень відповідно до розробленого методу. Розроблений метод у поєднанні з іншими технологіями технологічного, поліграфічного та фізико-хімічного захисту запропоновано використати для захисту інформації.

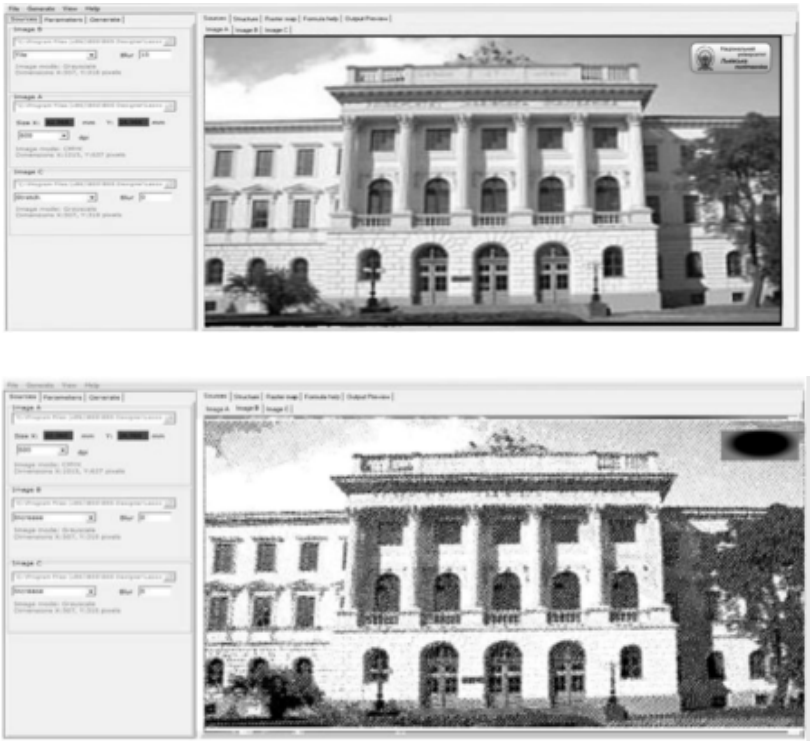


Рис. 6. Захист інформації на основі плівок з прихованим латентним зображенням

Проведений огляд та аналіз методів та засобів захисту друкованих документів за допомогою плівок засвідчив існування проблеми підвищення рівня захищеності інформації та показав розв'язання цієї проблеми на основі введення спеціалізованого математичного апарату security генерується 4 основні плівки та плівка-детектор.

1. Коншин А.А. Защита полиграфической продукции от фальсификации [текст] / А. А. Коншин. – М.: ООО "Синус", 1999. – 157 с. 2. Назаркевич М. Аналіз сучасних методів та програмних ужитків з графічним захистом друкованих документів / Марія Назаркевич, Оксана Троян // Технічні вісті. – 2013. – № 1 (37). – С. 42 – 44. 3. Назаркевич М.А. Розроблення програмного забезпечення для захисту друкованих документів / М. Назаркевич, О. Троян // Матеріали міжнародної наук.-прак. конф. ITSEC. 4. GuardSoft - Security Printing and Design Software. – Режим доступу до журналу: http://www.guard-soft.com/cerb_filters.html- Назва з екрану. 5. http://latent.ru/constructor/index/index.php. 6. http://www.ofs.ch/en/products/protecting-brands/. 7. http://www.brand-security.de/swf/index.php. 8. http://www.banknotes.ru/info.html.