УДК 531.36+534

І. Дронюк, М. Назаркевич, О. Миронюк
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

РОЗРОБЛЕННЯ МЕТОДУ ЗАХИСТУ ЦІННИХ ПАПЕРІВ НА СТАДІЇ ДОДРУКАРСЬКОЇ ПІДГОТОВКИ

Розроблено новий спосіб захисту інформації, який базується на теорії Ateb-функцій і застосовується для захисту цінних паперів. Запропонований метод створює приховані зображення, які стають видимими при спробі підробки.

Ключові слова: спосіб захисту, теорія Ateb-функцій, цінні папери, додрукарська підготовка

The authors developed a new data protection method, which is based on the theory of Ateb functions. 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.

Key words: method of protection, theory Ateb-functions, securities, prepress

1. Вступ

З розвитком поліграфічних технологій підробки стають все складнішими і високотехнологічними. Паралельно з розвитком засобів захисту друкованої продукції удосконалюються методи фальсифікації. Постійно потрібно розробляти нові види захисту цінних паперів.

Приблизно до кінця XX ст. індустрія фальсифікації технологічно базувалася на найдорожчому й найдосконалішому методі – аналоговому. Тобто підробка створювалася технологічними методами, ідентичними або максимально близькими до методів виготовлення оригіналу. Корінний перелом у розвитку техніки фальсифікації збігся з поширенням у 80-х роках систем оперативної поліграфії, розмножувальної професійної техніки, комп'ютерних технологій і настільних видавничих систем [1].

Доступність нових технічних засобів зробила технологію фальсифікації простішою і рентабельнішою. З розвитком нових носіїв інформації і засобів платежу (кредитні, дисконтні, таксофонні та інші магнітні картки) для фальсифікаторів відкрився новий перспективний сектор. Прикладів різних фальсифікацій навіть за останні роки більш ніж достатньо.

Сучасні інформаційні технології продовжують розвиватися. Тому можливості обладнання, за допомогою якого найчастіше створюють фальсифіковану продукцію, а саме ксерокси, принтери та сканери, також покращуються. З кожним роком ксерокс використовує все більшу кількість кольорів, покращується якість друку принтерів, а сканери розпізнають елементи з усе більшою роздільною здатністю. Тому постійно виникає потреба у створенні нових інформаційних технологій захисту.

2. Захист від копіювання за допомогою технології мікрографіки

З часів виникнення технологій друку тонка графіка стала однією з найпоширеніших видів захисту. Група захистів тонкої графіки ґрунтується на створенні тонких графічних елементів, сіток, розеток, віньєток, прихованих елементів і мікрографіки.

Найпопулярнішим є графічний спосіб захисту від копіювання, адже навіть для найдосконалішої цифрової технології відтворення мікрографіки залишається недоступним. Труднощі відтворення пов'язані зі складною геометричною структурою і мінімально можливою товщиною ліній елементів тонкої графіки [2].

Одним з найвідоміших видів тонкої графіки є гільйош. Цей вид захисту базується на нанесенні орнаменту у вигляді густої сітки хвилястих фігурних ліній, що переплітаються. Гільйош може бути як симетричним, так і асиметричним за дизайном. За чинними нормативами гільйошні елементи повинні займати не менше ніж 70 % площі цінних паперів, причому її велика частина повинна містити багатоколірні гільйошні композиції. Гільйошну композицію неможливо відтворити на копіювальному апараті, оскільки мала товщина (40-70 мкм) ліній і постійна зміна кривизни кожної лінії створює перешкоди для відтворення [7].

Іншим способом захисту є нерапортні сітки [6], що створюють оригінальний малюнок, який важко скопіювати. Для відтворення такого зображення неможливо взяти його частину і розмножити за допомогою копіювання, так само як і неможливо відтворити його вручну, не маючи вихідних даних. Ця технологія дає змогу створювати не тільки прості малюнки з ліній та синусоїд, але й перетворювати повноцінні зображення, наприклад, фірмову символіку компанії.

Ще одним видом графічного способу захисту поліграфічної продукції є мікрографіка. Вона базується на ефекті прихованого зображення на основі високої роздільної здатності ліній. Візуально мікрографіка сприймається як неперервна лінія, хоча складається зі знаків та символів, які можна побачити лише при значному збільшенні. Є два підвиди цього способу захисту: NaNOcopy та LogoDot [4, 5]. Суть першого підвиду захисту полягає у застосуванні символів та знаків для побудови лінії, а другого – у використанні деякого вибраного зображення.

Одним із перших способів захисту документів від копіювання на етапі розроблення дизайну стала технологія «прихованого повідомлення». Ця технологія полягає у нанесенні спеціальних слів «ПОШКОДЖЕНО» або «КОПІЯ» на фон зображення. Якщо споживач бачить на виготовленому документі приховані слова, то можна стверджувати, що продукт сфальсифікований. Такого ефекту досягають двома способами. Перший – за рахунок незначної різниці кольорів між фоном та прихованими словами, якої не можна досягти, використовуючи сучасні принтери чи ксерокси. За другим способом використовують нестандартної форми крапку, яку сканер не може розпізнати, тому залишає пусті місця, у яких відтворюються слова.

Із способів захисту поліграфічної продукції користується попитом технологія з використанням латентного зображення.

3. Технологія створення латентних зображень

Латентні зображення – велика група зображень, що мають одну спільну властивість – зміну видимості елементів зображення у разі зміни умов спостереження. Латентні зображення можна створювати 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.

Латентні зображення, сформовані з використанням різних орієнтованих штрихів, не потребують використання будь-яких пристроїв для ідентифікації. Однак, якщо розмір елементів сформованого зображення великий, їх легко можна скопіювати з високою точністю. Ця обставина значно знижує захисні властивості зображень цього типу.

Існують спеціальні методи растрування: імітація гравюри, використання особливої форми растрової точки, растрування криволінійними лініями змінної товщини тощо. Вони забезпечують достатньо високий ступінь захисту. Але якщо стандартні способи растрування орієнтовані на максимально точне відтворення оригіналу, то завданням спеціальних способів є захист від

копіювання, що завдає шкоди художній якості репродукції. Ця обставина в багатьох випадках звужує сферу застосування спеціальних методів растрування.

Упровадження прихованого вмісту в латентні зображення на стадії растрування характеризується відсутністю багатьох недоліків, описаних вище. Крім цьому, завдяки малому розміру елементів сформованого зображення і прихованості факту присутності захисту забезпечується високий ступінь захисту.

Спільним для більшості методів формування прихованих зображень є кодований характер вбудованої інформації. Це вимагає спеціально розробленого програмного забезпечення для створення зображень і виявлення прихованої частини. Іншим недоліком є високі вимоги до точності друку і складності під час зчитування зображення.

У патенті [9] 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, щоб полегшити утворення зображення і тла, які взаємодіють 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 наявність будь-якого з прихованих зображень, що накладаються.

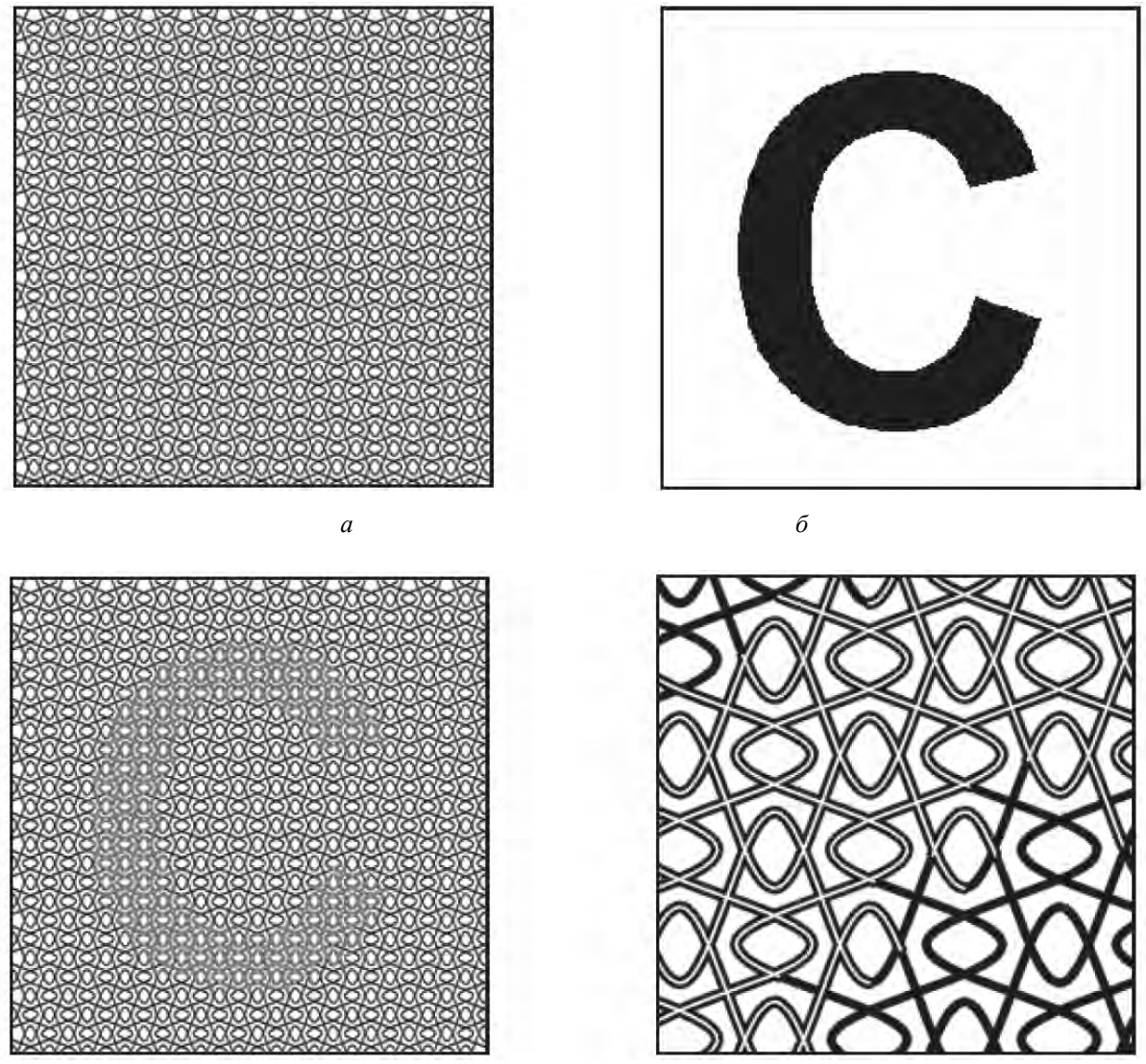
Вибираючи різні значення лініатури для прихованого повідомлення-попередження і фону зображення, щоб запобігти дублюванню, беруть різні тональні значення кольорів відтворення на документі (тобто відсоток розміру елемента і товщина фарби), так що приховані попередження виникають на відтвореннях оригінального документа.

Через невідповідність між рядковими і тональними значеннями кольору прихованого попередження та фонового зображення просто комбінація цих двох методів не може бути ефективною, оскільки приховане повідомлення-попередження може бути звичайним, видимим для випадкового переглядача оригіналу. Щоб звести до мінімуму виникнення видимих попереджень з цими комбінованими методами, відповідні тональні значення кольору вибирають так, щоб вони візуально були схожі між собою. Масковане зображення можна надрукувати більшого розміру або в поєднанні з прихованим попередженням і фоном, щоб допомогти замаскувати приховані зображення від випадкового спостерігача оригінального документа [3].

Інший спосіб захисту розроблено в 1980-х роках і названо Screen angle modulation (SAM), тобто екранна кутова модуляція. За допомогою цього методу екранні точки замінюються мінімальними лініями. Ці лінії неправильно відтворюються під час сканування і друкується зображення, яке створює повідомлення-попередження на копії. Збільшення відмінності між прихованим попередженням і фоновими елементами за допомогою маскування значно поліпшує антикопіювальні можливості. Цю методику запатентувала торгова марка ThermoSafe ™.

4. Метод антикопії

Фірма GuardSoft розробила спеціалізоване програмне забезпечення Cerberus [8]. Вона основана на створенні подвійної лінії, що має антикопіювальний ефект, який досягається розщепленням лінії гільйошу на дві або більше. У результаті деякі частини гільйошного зображення складатимуться з подвійних ліній. Ширина кожної лінії буде меншою порівняно з початковою. На рис. 1, *а* показано мотив гільйошу, на рис. 1, *б* – літеру “С”. На рис. 1, *в* наведено результат роботи програми Cerberus з прихованим зображенням літери “С”. На збільшеному зображенні (рис. 1, *г*) можна побачити, що літера “С” відтворена подвійними лініями.



а *б*

в *г*

Рис. 1. Розробка фірми GuardSoft програма Cerberus, що реалізує метод антикопії

5. Розроблення методу захисту на основі ateb-функцій

Цей метод захисту базується на побудові ліній різної товщини, що відповідають графікам періодичних Ateb-функцій. Ми розробили метод числового та графічного представлення Ateb-функцій. Як було доведено, вигляд Ateb-функції залежить від двох раціональних параметрів. Якщо змінюються параметри Ateb-функція, набуває іншого вигляду її графічне представлення, яке вибираємо за одиничний графічний елемент. На основі одиничних графічних елементів будуються гільйошні мотиви. На наступному етапі у гільйошний мотив вбудовується приховане повідомлення за допомогою зміни товщини лінії.

Розроблено програмне забезпечення з використанням мови PostScript, яке забезпечує високий рівень якості захищеного документа. Стандартно система координат розпочинається з лівого верхнього кута сторінки. У системі відліку мови PostScript початком координат вважають лівий нижній кут сторінки. Вважаємо, що вісь *x* проходить горизонтально, а вісь *y* – вертикально. Кожна точка документа має чітко визначені координати (*x*, *y*).

Розробка реалізує метод зміни товщини лінії для побудови прихованого повідомлення. Наведений документ складається з великої кількості повторюваних ліній, побудованих функцією Ateb-синуса, що утворює гільйошний мотив. Більшу частину площі документа займають неперервні лінії заданої товщини, для виведення яких розроблена процедура. В місцях розміщення літер слова «КОПІЯ» одинарну лінію замінюємо подвійною меншої товщини, для чого також створена спеціальна процедура.

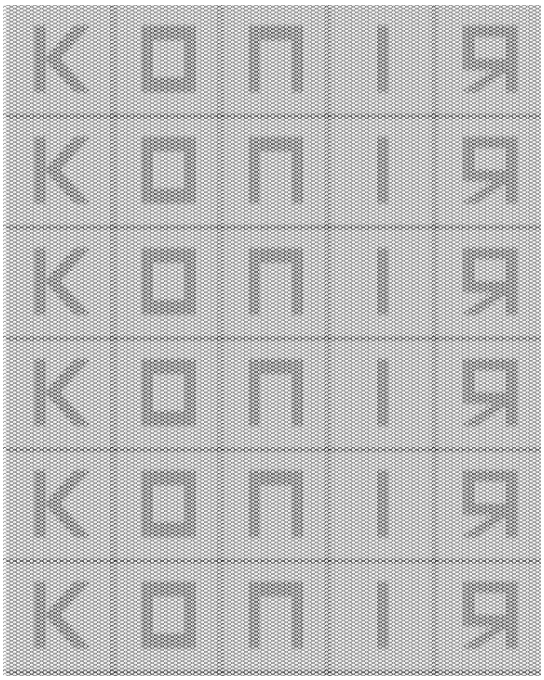


Рис. 2. Вигляд захищеного документа

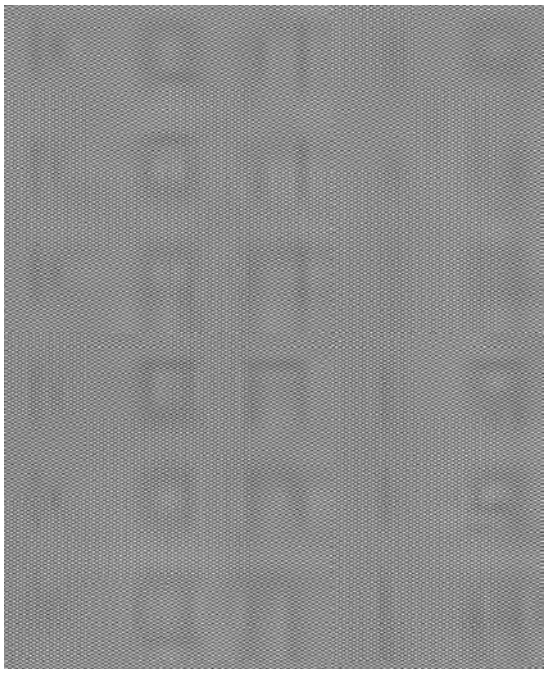


Рис. 3. Сканований вигляд документа

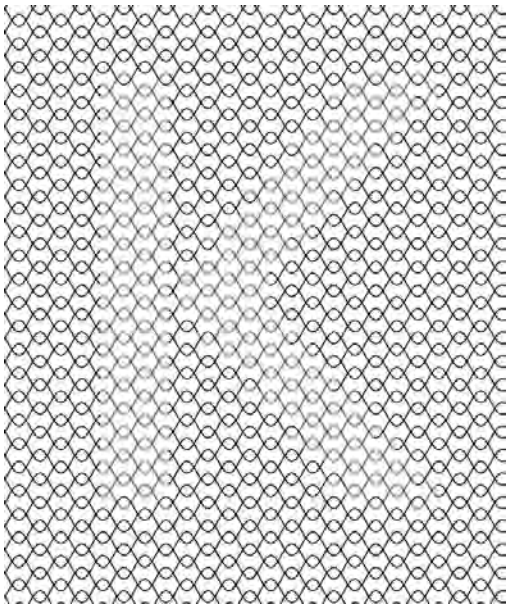


Рис. 4. Збільшений масштаб літери "К" із захищеного документа

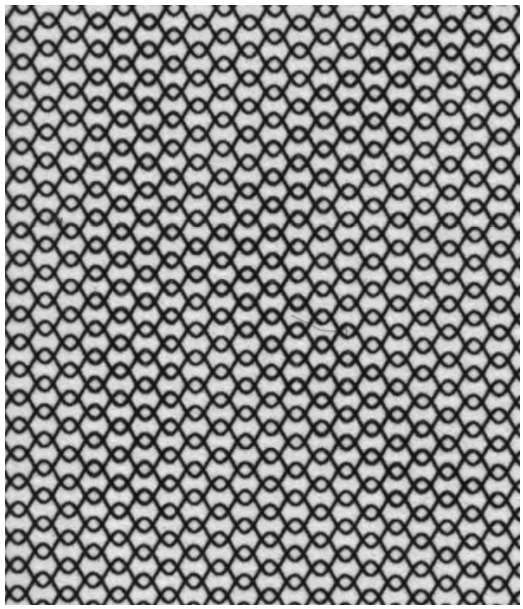


Рис. 5. Збільшений масштаб літери "К" із сканованого документа

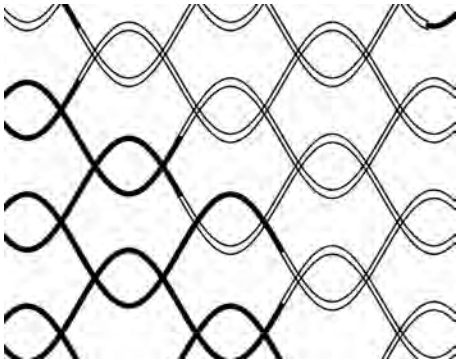


Рис. 6. Фрагмент гільйошного мотиву при переході літера-фон

Опишемо принцип роботи обох процедур. Перевіримо поточні координати документа (x, y) на потрапляння у простір прихованого слова. Якщо координати потрапляють у площу прихованого слова, то викликаємо процедуру побудови подвійної лінії, у протилежному випадку будуємо одинарну лінію. У процедури передається один параметр – поточна координата *x*. Під час побудови одинарної лінії в тілі функції обчислюємо значення координати *y* для заданого *x* , і потім будуємо лінію з попередньої точки в задану. Функція побудови подвійної лінії дещо складніша. Спочатку поточні координати заносимо в локальні змінні і знаходимо координати попередньої точки, після чого відшукуємо зміщені на деяку константу по осі ординат координати попередньої і нової точки, між якими проводимо лінію. Таких ліній є дві – одна зміщена вгору, а інша – вниз. При цьому для збільшення чіткості слова «КОПІЯ» на оригінальному документі товщину ліній зменшуємо вдвічі.

Оскільки кожна з літер має свої параметри відображення (ширина, положення тощо), то для виведення кожної літери створено окрему процедуру, якій передаються два параметри – координати *x* та *y* положення лівого нижнього кута літери на документі. При цьому в тілі процедури зберігаємо поточні налаштування графічного режиму (до якого також входить точка початку відліку координат), точку початку відліку змінюємо на задані координати, і побудова ведеться вже відносно них. В кінці процедури відновлюємо збережений стан графічного режиму, що дає змогу в основному тілі програми точно позиціонувати букви відносно однієї точки. Головне тіло програми реалізується циклом, завдяки якому слово «КОПІЯ» позиціонується по осі ординат.

На рис. 2 показано вигляд захищеного документа, а на рис. 3 – його скановану копію. Навіть візуально помітна втрата якості та чіткості зображення. На рис. 4 наведено збільшене зображення літери “К”, а на рис. 5 – його скановану копію. Під час візуального перегляду на копії літери не видно, оскільки на усьому полі проглядається сітка. На рис. 6 показано збільшений фрагмент утворення літери на основі поділу товщини лінії.

Висновки

Проаналізовано методи захисту документів на етапі додрукарської підготовки. Показано, що одним із найбільш перспективних та ефективних є метод мікрографіки. Розглянуто різні способи реалізації мікрографіки. Наведено приклад закордонної розробки мікрографіки, основаної на зміні товщини лінії. Запропоновано метод захисту документа, що базується на побудові розщеплення ліній, які відповідають графікам періодичних Ateb-функцій. Розроблено відповідне програмне забезпечення з використанням мови Post Script, що забезпечує високу якість тиражованого захищеного документа. Роботу програми проілюстровано прикладами. Порівняння сканованого та оригінального документа підтверджує ефективність такого способу, що показано на рисунках. Цей спосіб захисту можна використати для захисту цінних паперів на стадії додрукарської підготовки.

1. Киричок П.О. Захист цінних паперів та документів суворого обліку: [моногр.] / П.О. Киричок, Ю.М. Коростіль, А.В. Шевчук. – К.: НТУУ «КПІ», 2008. – 368 с. 2. Коншин А.А. Защита полиграфической продукции от фальсификации [текст] / А. А. Коншин. – М.: ООО «Синус», 1999. – 157 с. 3. Gary G. Field – Color and It’s Reproduction. Graphic Arts Technical Foundation / Gary G. Field Graphic Arts Technical Foundation. January № 3, 1988. – P. 1430–1450. 4. Philips G.K. Combining nanocharacter printing, digital watermarking and UV-Coded taggents for optimal machine-readable security // SPIE proc., Conference on Optical Security and Counterfeit Deterrence Techniques V, 4677, 2002. – P. 150–158. 5. George K. Phillips. Document Security System Having Thermo Activated Pantograph and Validation Mark. Patents 5,873,604 and 6,665,406. 6. When failure is not an option. – Режим доступу до журналу: http:// www.adlertech.com/securitypaper.htm. – Назва з екрана. 7. – Security-paper. Режим доступу до журналу: http://www.security-paper.ru/11-elementov-zaschity. – Назва з екрана. 8. GuardSoft - Security Printing and Design Software. – Режим доступу до журналу: http://www.guard-soft.com/cerb_filters.html- Назва з екрана. 9. Patent Publication (Source: USPTO). Latent image structure – US 6296281. published on 02-Oct-2001.