Аналіз сучасних методів та програмних ужитків з графічним захистом друкованих документів

Д.т.н., доц. М. Назаркевич, асп. О. Троян

Lviv Polytechnic National University, 22/806 Bandera St., Lviv-13, 79013, Ukraine

Abstract. Analysis modern graphic ways toprotect printed documents. It is shown that the image remains promising ways to protect the formation of latent images. Latent images can reliably protect printed documents by photocopying. A method for forming latent images.

Key words: protect printed documents, latent images, security printing.

Вступ

Протидія методам підробки та фальсифікації паперових, а останнім часом і пластикових, документів є традиційним і актуальним завданням захисту носіїв інформації. Одним з ключових елементів для багатьох документів є графічні способи захисту.

1. Аналіз видів графічних способів захисту

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 [1].

Графічні захисти можна розділити на такі види: гільйошні композиції, тангірні сітки, приховані елементи: *Void Pantograp, Copy Ban, Latent image*, мікрографіка, призматичний друк [2].

Одним з найрозвиненіших є **гільйошні захисти**. До гільйошних композицій належать системи кривих тонких ліній, що перетинаються й утворюють фонові малюнки, які через малу товщину ліній не можуть бути коректно зісканованні. Для того, щоб додатково ускладнити відтворення гільйошних композицій, використовують спеціальні технології друкування.

Тангірні сітки – рельєфні рисунки із систематично розміщених точок і ліній для отримання штрихових кліше із рівним тоном.

«Void Pantograph» - захист орієнтований на прояв в копії поліграфічного продукту прихованої в фоновій сітці. Текст прихованого напису може бути довільним. На оригіналі прихований запис візуально невидимий, а яскравий напис на фоні копії виробу наочно показує, що перед користувачем не оригінал. Технологічно даний захист заснований растуванням точок при офсетному методі друку. Растрове зображення тангірної сітки, задане різновеликими растровими точками на першому етапі друкованого процесу, робить прихований напис видимим. На другому етапі розтягування растрової точки прихованого зображення зливається з растровим фоном і стає візуально невидимим. Цей ефект невидимості заснований на оптичній природі людського зору. Приховане зображення, що злилося з растровим фоном в результаті розтягування, проявляється на ксерокопії. Зображення захисної сітки має регулярний систематичний характер. Розмір шрифта прихованого напису може змінюватись.

Технологія **«*Copy Ban*»** це створення захисту з нерегулярною структурою. Найдосконаліші копіювальні апарати не в змозі відтворити захист *Copy Ban*. Захисний напис багаторазово повторюється в межах поля захисної сітки. Нерегулярна структура захисної сітки забезпечує прояв прихованих написів хоча б в одному місці копії. Підроблення документу, який захищено за технологією «*Copy Ban*» на сьогоднішній день залишається нереалізованим. Розмір шрифта прихованого надпису є необмеженим і захищений для всіх видів формату. Слід також враховувати, що на відміну від тангірних сіток, *Copy Ban* за рахунок нерегулярної структури більшою мірою впливає на візуальне сприйняття графічної й текстової інформації, що наноситься поверх захисної сітки. Як приклад, цей захист використовують як публічний або клієнтський захист. Цифрова фальсифікація описаного захисту проявляється при візуальному контролі на фоні продукції. Подібна підробка візуально відображається на копіювальному апараті.

Технологія **«*Latent image*»** дозволяє вбудувати приховані елементи [3]. Спосіб включає вбудовування прихованого зображення в основі при растуванні і виявлення прихованого зображення з використанням цифрової фільтрації.

Вбудовування прихованого зображення відбувається за допомогою того, що частина основного зображення растується з використанням різних стохастичних растрових структур. При фальсифікації елементів тонкої графіки з прихованими зображеннями вони зникають або, навпаки, стають видимими. Такі ефекти ґрунтуються на виведенні зображень з високою роздільною здатністю ліній тонкої графіки.

Мікрографіка. Візуально мікрографіка сприймається як неперервна лінія. Тільки за 10–20-кратного збільшення видно, що неперервна лінія складається зі знаків і символів. Як правило, мікрографіку створюють на основі літер чи символів. Тому найпоширенішим видом мікрографіки є мікрошрифт. Це зручно для ідентифікації автентичності. Користувачеві досить перевірити наявність напису мікрошрифтом у певному місці. Рекомендовані висоти мікрошрифту, що утворюють мікротекст для позитивного зображення – 200–300 мікрон, для негативного зображення – 300–400 мікрон. Під час ксерокопіювання і сканування мікротекст утворює неперервну лінію.

Призматичний, або ірисовий друк – ще один спосіб захисту, де створюється багатофарбовий фон, який ускладнює кольорове ксерокопіювання або сканування. Такий плавний перехід не відтворюється копіюванням або скануванням.

Формування прихованих (латентних) зображень для захисту документів, які досить добре видно у разі

спостереження зображення під кутом краще здійснюється при офсетному способі друку. Друкуючи офсетним способом друку на спеціальних видах паперу, також можна створювати приховані зображення, якщо застосовувати спеціальні растри [3]. Найпростіший спосіб створення прихованого зображення – це штрихування певної ділянки. Якщо розглядати це зображення за допомогою циліндричного растра у певному напрямку, його видимість краща. Під час ксерокопіювання на доволі однорідному полі документа спостерігається зображення об'єкта, яке раніше не було видимим.

2. Аналіз програмного забезпечення для захисту документів.

Відомі такі компанії, розробники програмного забезпечення для захисту документів: *JSP Jura*, зі своїми ужитками *GS Layout GS Vector Starlight*, фірма *Orell Fussli Security Documents AG* з ужитком *Banknotizer*, *GuardSoft* із розробками *Cerberus, StrokesMaker*, *Barco Graphics* із ужитком *Gilloche Generator*, SecuritySoft C^{o} із додатками Гравер та Цербер.

Австрійська компанія JSP Jura розробляє спеціальне програмне забезпечення для забезпечення високого рівня захисту банкнот, і використовує найновіші досягнення в комп'ютерних технологіях [5].

Рис.1. Розробка фірми JSP Jura. Голуб виконаний літерами "Jura"

Ця система програмного забезпечення включає в себе програмне забезпечення для створення захисних графічних елементів для забезпечення найвищого рівня захисту. Програмні додатки створюють високоточні гільошні та інші векторні графічні елементи захисту, генерують приховані зображення, реалізовують системи захисту анти-ксерокопії.

Ужиток Banknotizer - програмне забезпечення для розробки складного дизайну глибокого та офсетного способів друку.

Фірма SecuritySoft C^{o} розробила програмне забезпечення для створення гільйоширних елементів, мікротексту, гравюр. Їхні розробки – це програмні продукти Гравер і Цербер [6].

Програмний продукт Гравер призначений для виготовлення цифрових гравюр з півтонових чорно-білих і кольорових зображень. Програма використовує оригінальні алгоритми для аналізу початкового зображення, розбиття його на зони та штрихування кожної зони для отримання кінцевого результату у вигляді чорно-білого зображення в стилі гравюри.

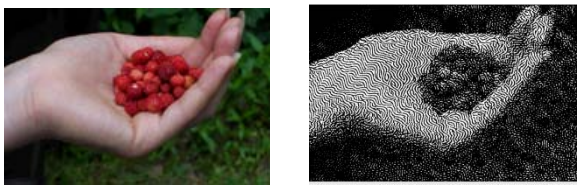

Рис. 2. Цифрова гравюра програми «Гравер» (справа), утворена за принципом «рівень»

За допомогою програми «Гравер» можна одержати імітацію гравюри, тобто зображення, у якого півтони передаються за рахунок штрихування різної інтенсивності і напряму [6]. Штрихування в межах однієї зони має однаковий напрям. Для згладжування переходів на межах сусідніх зон застосовується розмиття зон. Напрям штрихування може бути вибраний згідно за одним з наступних принципів: «рівень», «градієнт» або «колір».

Програма «Цербер» призначена для створення захисних і декоративних гільйоширних елементів: розеток, лінійних елементів бордюрів; елементів фону захисних та декоративних сіток; поверхні — нерегулярні гільйошні сітки, які створюються на основі початкового зображення, яке накладається на тривимірну поверхню; спеціальні ефекти, які базуються на півтонових зображеннях [6].

Рис. 3. Гільйошна композиція з латентністю - розробка фірми «Цербер»

3. Метод формування латентних зображень

При виведенні текстової та графічної інформації традиційно використовується растрування. При виведенні кольору застосовується система CMYK. Вивід здійснюється із певним значенням лініатури. Цей параметр належить лише до регулярних амплітудно-модульованим растрів. Він визначає щільність накладення ліній растру на одиницю довжини (зазвичай - дюйм). Чим більше значення частоти накладання ліній на одиницю довжини зображення, тим стає менш помітна дисретність зображення.

Людина, котра має середньостатистичну гостроту зору, не помічає растру в зображеннях з лініатурою понад 133 lpi.

Зображення у кольорі досягається шляхом суміщення кольороподілених поліграфічних форм чи фарб, у залежності від обраної технології друку. Причому форма для кожної фарби повинна виготовлятися під певним кутом повороту растру, або при друці, коли накладається один шар фарби на інший, щоб не виникав муар, який додає труднощі у сприйнятті зоб-

раження. У технології репродукційних процесів було визначено та стандартизовано певні кути повороту та частоти растрової структури, які обумовлені в стандарті DIN 16547.

Для голубої фарби встановлено стандартне значення повороту 15^0, для пурпурної - 75^0, для жовтої - 0^0 , для чорної - 45^0. Теорія кольороподілу стверджує [7], що не можна використовувати одні й ті значення кута нахилу растру для різних фарб одночасно, оскільки це може викликати сильні спотворення зображення , які проявляються в зміні кольору і появі інтерференційної періодичної структури внаслідок накладення двох періодичних растрових структур, які називаються муаром.

Муаровий візерунок виникає при цифровому фотографуванні і скануванні сіткових та періодичних зображень, якщо їхній період близький до відстані між світлочутливими елементами обладнання. Цей ефект рекомендовано використовувати таким чином: на документ наноситься хвилеподібний малюнок, який при скануванні може покритися дуже помітним візерунком, який вирізнить підробку від оригіналу.

Інтерференцію на документі можна отримати, формуючи векторні об'єкти при накладанні двох періодичних структур за принципом суперпозиції, див. рис. 2.

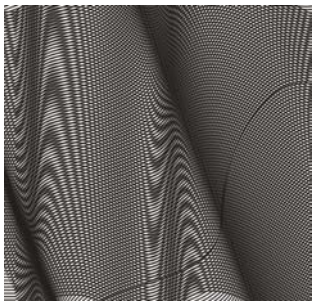

Рис. 2. Приклад інтерференції при накладанні двох періодичних структур на документ (товщина лінії 60 мкм)

Запропоновано створювати ефект латентності для формування захисту на основі інтерференціїї періодичних структур, що створені векторною графікою. У першому шарі створюємо напис, наприклад слово "Дублікат", який буде читатися при роздруку на виведенні ксерографією.

Запропоновано створення верхніх шарів хвилями з частотами, яка відповідає найтоншому штриху при друці офсетом. Їй відповідають значення порядку 10-60 мкм з найменш можливим значенням інтенсивності кольору. А зверху накладаємо інший шар періодичної структури, яку будуємо за принципом суперпозиції.

На рис. 3 показано векторне зображення з ефектом латентності. Це ж зображення було виведене засобами ксерографії то оцифроване (рис.4). Навіть візуально спостерігається втрата якості та розмиття ліній сіток. На рис. 4 схований напис не читається.

Висновки

Проведено аналізи графічних способів захисту, які дозволяють ефективно боротись з підробками та фальсифікацією паперових та пластикових документів. Проаналізовано можливості сучасних технологій захисту і встановлено, що надійний захист можна забезпечити, розробляючи нові інформаційні технології, що базуються на нерегулярному растуванні, нестандартних кутах повороту растрової структури, тощо.

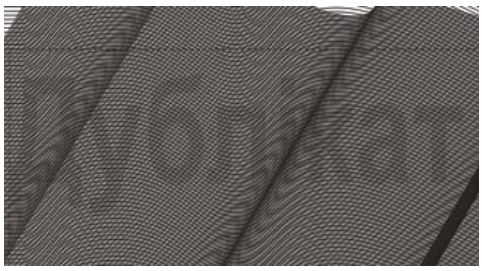

Рис. 3. Приклад векторного зображення з латентністю

Рис. 4. Скановане зображення на основі створеного векторного

Проведено аналіз сучасного програмного забезпечення, яке забезпечує захист друкованих документів. Приведено приклади розробок.

Запропоновано метод створення латентності документа, який базується на ефекті інтерференції векторних об'єктів при накладанні періодичних структур. Документ, створений за розробленою технологією матиме високу якість та міститиме захисні елементи.

[1]. Шевчук А. В. Модель засобів захисту друкованих докуенів / А. В. Шевчук.// Захист інформації. – 2013. – Том 15, № 1 (2013). — С. 63—66.

[2]. Разработка способа защиты полиграфической продукции. – Електронні дані. – [Електронний ресурс]. Режим доступу: http://www.dissercat.com/content/razrabotka-sposoba-zashchity-poligraicheskoi – produktsii-s-ispolzovani-em-skrytogo-rastrovogo #ixzz 2hxNrox2r

[3]. Latent image generator and method of embedding watermarks into an input image, United States Patent no 7,006,256 B2, H04N 1/46, Hui Cheng, заявитель: Xerox Corporation, Stamford, CT (us),: опубл. 28.02.2006.

[4]. Шевелёв А. А., Андреев Ю. С. Латентные изображения на основе стохастических растровых структур. // Известия вузов. Проблемы полиграфии и издательского дела. 2009, № 1, с. 29-39.1. Другие публикации.

[5]. Jura JSP GMBH [Електронний ресурс] / Jura JSP GMBH. – Електронні дані. – Vienna, 2010. – Режим ДОСтупу : http://www.jura.at/en /index.htm.

[6]. Securesoft [Електронний ресурс] / securesoft Електронні дані. Режим доступу : – www.securesoft.ru/soft.html.

[7]. Кузнецов Ю.В. Технология обработки изобразительной информации [Текст] / Ю. В. Кузнецов – СПб. : Петербургский институт печати, 2002. – 312 с.