УДК 004.056.5: 655.25

І. М. Дронюк
Національний університет “Львівська політехніка”

МОДЕЛЮВАННЯ ЗАГРОЗ ТА ГРАФІЧНИЙ ЗАХИСТ ДЛЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Запропоновано класифікацію загроз для матеріальних носіїв інформації. Запропоновано методи графічного захисту як засіб протидії атакам на матеріальні носії інформації. Розроблено метод захисту на основі модифікованого методу автотипного растрування.

Ключові слова: загрози для матеріальних носіїв інформації, графічний захист, автотипне растрування.

The paper presents a classification of threats for physical media. Methods of graphical protection as a means of counteraction against attacks on physical media were proposed. A protection technique based on the modified method of autotypical screening was developed.

Key words: threats for the physical media, graphic protection, autotypical screening.

Вступ

Однією з важливих ланок створення безпеки інформаційних систем у державі є захист інформації на паперових та інших матеріальних носіях інформації. До цього класу належать документи, що посвідчують особу (наприклад, паспорт) або спеціальні вміння (права водія), належність до категорії, що має певні пільги (пенсійне посвідчення), документи, що забезпечують грошовий обіг (банкноти, доручення), поштові знаки. Аналізуючи цей далеко не повний перелік, можна зробити висновок, що фальсифікація документів приносить державі щороку багатомільйонні збитки, і створення відповідного рівня безпеки інформаційних ресурсів на матеріальних носіях є справою державної ваги [1]. Тому актуальною є задача аналізу та класифікації атак на друковані документи з метою забезпечення цілісності інформації, попередження фальсифікацій та створення ефективних та економічно вигідних систем захисту [2].

Класифікація загроз на друковані документи

Можна виділити такі критерії для класифікації атак на друковані документи: ступінь загрози; рівень складності; спрямованість результату; інструментальні засоби реалізації атак; тип атаки; рівень організованості; рівень автоматизованості; суб’єкт атаки; середовище обігу.

За ступенем загрози атаки можна поділити на державні, професійні та побутові. За рівнем складності поділяємо атаки на імітаційні, технологічні та так звані суперпідробки, що використовують технології, аналогічні оригінальним. Атаки можуть бути спрямовані на порушення свободи і прав людини, на розкриття державної таємниці, можливі фальсифікації з метою уникнення покарання або привласнення чужого майна, отримання наживи або незаконних пільг. За інструментальними засобами виконання атаки поділяємо на репрографічні, поліграфічні та комбіновані. За способом виконання вирізняємо такі типи атак як механічні, хімічні, пряма зміна, маскування та аплікації. За рівнем організованості можна вирізнити одноосібні, групові, мережеві та глобальні міжнародні атаки. Відносно критерію автоматизації атаки поділяємо на ручні, автоматичні та автоматизовані. За суб’єктами атакування загрози можуть бути спрямовані на графічні елементи, на захист паперів, на післядрукарські захисти, на персоніфікувальні елементи та на технологічні захисти. Для захисту документів надзвичайно важливо враховувати середовище обігу, яке може бути контрольованим, неконтрольованим та професійним.

Описану вище розроблену класифікацію атак подано в таблиці.

Класифікація атак на друковані документи

За ступенем загрози		За інструментальними засобами		За рівнем автоматизації
Державні Професійні Побутові		Репрографічні Поліграфічні Комбіновані		Ручні Автоматичні Автоматизовані
За рівнем складності		За типом атаки		За суб'єктами атаки
Імітаційні Технологічні Суперпідробки		Механічна Хімічна Пряма зміна Маскування Аплікація		Атаки на графічні елементи Атаки на захисти паперу Атаки на післядрукарські захисти Атаки на персоніфікувальні захисти Атаки на технологічні захисти
За спрямованістю результату		За рівнем організованості		Середовище обігу документів
Порушення свободи і прав людини Розкриття державної таємниці Уникнення покарання Привласнення чужого майна Нажива Пільги		Одноосібні Групові Мережеві Глобальні міжнародні		Контрольоване оточення Неконтрольоване оточення Професійне оточення

Графічні методи захисту – засіб протидії загрозам матеріальним носіям інформації

Група графічних захистів грунтується на труднощах відтворення і репродукування тонких графічних елементів, сіток, розеток, віньєток, прихованих елементів і мікрографіки. Труднощі репродукування пов'язані зі складною геометричною структурою і мінімально можливою товщиною ліній елементів тонкої графіки. З розвитком технологій фальсифікації тонка графіка не втратила своєї актуальності. Для найдосконаліших цифрових технологій достовірна підробка тонкої графіки і мікрографіки залишається недоступною [3].

Труднощі поліграфічного відтворення елементів тонкої графіки пов'язані зі специфічними технологічними умовами пристосування друкарських машин для відтворення такої графіки та використанням певних категорій специфічних "ноу-хау" в галузі друкарських технологій захисту та спеціальних видів друку [4].Фальсифікаторам недоступна ідентична підробка і, порівнявши з оригіналом, візуально можна побачити значні руйнування або спотворення оригінального зображення. Особливо очевидна підробка, виконана цифровими методами.

Графічні захисти цієї підгрупи можна поділити на такі види: гільйошні композиції, тангірні сітки, приховані елементи "*Latent image*", мікрографіка, призматичний друк. До гільйошних композицій належать системи кривих тонких ліній, що перетинаються й утворюють фонові малюнки, які через малу товщину ліній не можуть бути коректно зіскановані. Для того, щоб додатково ускладнити відтворення гільйошних композицій, використовують спеціальні технології друкування.

Однією операцією друкування є растрування. Відомимими є амплітудно-модульоване та стохастичне растрування [5]. При реалізації класичного методу амплітудного растрування (АМ) чорно-білого оригіналу розмір точки растра розраховується для кожного елемента і залежить від інтенсивності тону у кожній комірці. Що більшою є інтенсивність тону, то щільніше заповнюються елементи растра. Темніший тон створюється завдяки збільшенню розмірів точок і скорочення білого поля між ними за однакової відстані між центрами елементів растра.

Існує інший метод растрування з частотною модуляцією (ЧМ), коли інтенсивність тону регулюється зміною відстані між сусідніми крапками однакового розміру. Під час частотно-

модульованого растрування в комірках растра з різною інтенсивністю тону знаходиться різна кількість точок. Зображення, растроване частотною модуляцією, виглядає якісніше, оскільки розмір точок є значно меншим, аніж середній розмір точки у випадку амплітудної модуляції. У цьому випадку розраховується кількість точок, необхідна для відображення потрібної інтенсивності тону в комірці растра. Тому при стохастичному ЧМ-раструванні втрачає сенс поняття частоти растру, має значення лише роздільна здатність пристрою виведення. Такий спосіб вимагає великих витрат обчислювальних ресурсів і високої точності відтворювання.

Метою цього дослідження є розроблення модифікованого автотипного методу растрування для графічного захисту інформації на матеріальних носіях. Покращення процесу растрування дає змогу точніше відображати тонкі елементи зображення чи тексту, що підвищує ефективність захисту друкованої інформації на матеріальних носіях. У процесі досягнення мети поставлено та вирішено такі основні завдання:

1) побудовано захисні графічні елементи на основі спеціальних функцій; 2) розроблено метод модифікованого автотипного растрування, що дає змогу друкувати дрібні деталі та досягати півтонів з більшою чіткістю для підвищення ефективності захисту.

Технологічні характеристики розробленого методу захисту

Захищений документ повинен відповідати нормам Держстандарту [6], зокрема захисні елементи повинні бути виконані у межах 40–50 мкм позитивного відтворення і 60–80 мкм негативного відтворення, а величини мікрошрифтів повинні перебувати у межах 200–250 мкм, що гарантує високу якість поліграфічного друку та зменшує ймовірність підробки. Розроблено метод захисту інформації на матеріальних носіях [7]. За допомогою розробленого програмного забезпечення поєднується потрібна інформація з захисними елементами та створюється електронний файл у форматі PostScript із захищеною інформацією, що дає можливість друкувати із максимальною якістю, на яку здатний вивідний пристрій. Тобто можна друкувати захищену інформацію з роздільною здатністю 3000 dpi та вище. Обмежують роздільну здатність друку тільки можливості вивідного пристрою для друку. Структурну схему методу захисту наведено на рис. 1.

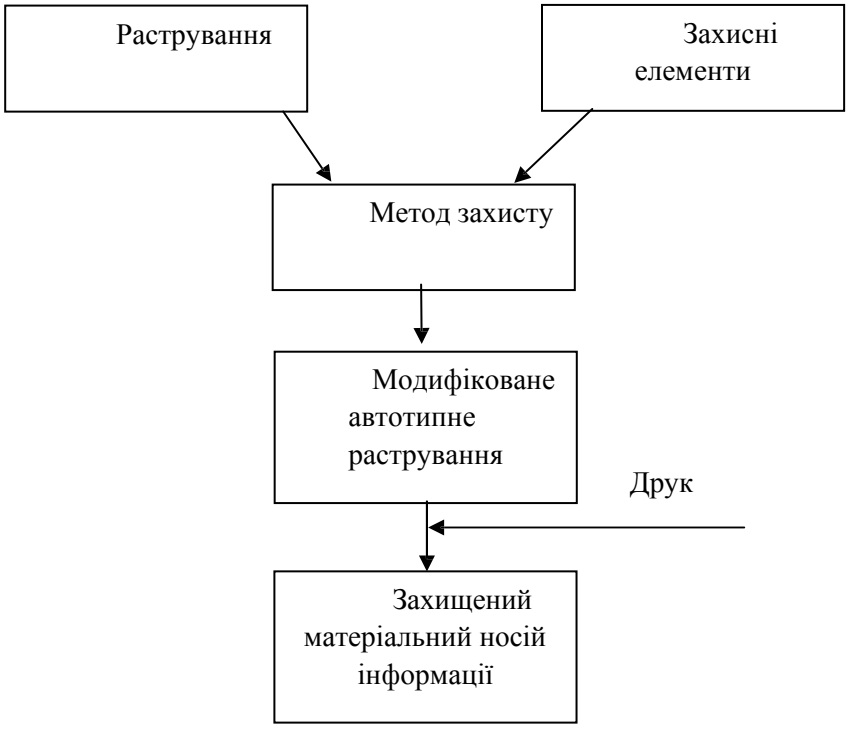


Рис. 1. Структурна схема методу захисту

Для ефективного захисту інформації на матеріальних носіях важливо забезпечити високу якість друкованого відбитку. Що якісніше надруковано інформацію, то важче її підробити. Сучасні технології дозволяють підробити все, але є економічні критерії створення підробки, тобто вартість та час створення підробки. Основна мета захисту – зробити підробку нерентабельною. Зрозуміло, що підвищення якості друку підвищує вартість друкованого відбитка, а отже, і вартість підробки. Це особливо важливо для повноколірних відбитків, якими є більшість важливих документів (паспорти, водійські посвідчення та ін.)

Існує проблема перетворення структури зображення в процесах поліграфічного відтворення, яка пов'язана із складністю відтворення дрібних деталей та півтонів. Одним з найбільших недоліків сучасних способів перетворення структури є значно менша роздільна здатність відбитків порівняно з роздільною здатністю друку. Причиною цього є амплітудно-модульований принцип відтворення півтонів бінарними засобами друку, в якому значення тону на певній ділянці оригіналу відтворюється відносною площею зафарбованої ділянки відбитка. Растрові точки руйнують контури і дрібні деталі напівтонового оригіналу, погіршуючи якість друкарського відбитка. Так утворюються растрові спотворення [8]. Величина і помітність растрових спотворень залежать від лініатури растра, частоти растрової функції та геометрії растрової структури і растрової точки. Ці растрові спотворення пов'язані з такими параметрами амплітудно-модульованого растрування, як тиск у друкарському апараті, подача фарби, розтискування, проковзування та двоїння.

Розроблено новий метод растрування, який дає змогу точніше відтворити тонкі елементи зображення, які є важливими для захисту. Покращення досягають завдяки спеціальній структурі растрової точки, яка краще адаптована для відображення півтонів. Формується растрова точка $T(i, j)$ за формулою

$$T(i, j) = f(m_1, n_1, i)g(m_2, n_2, j), \qquad (1)$$

де i, j – поточні координати растрової точки; m_1, n_1 – параметри спеціальної функції по горизонталі; m_2, n_2 – параметри спеціальної функції по вертикалі. Для передавання глибини кольору 8 бітів растрова точка може набувати від 1 до 256 значень, тобто $j = 1,...,16; i = 1,...,16$.

Приклад формування растрової точки на основі спеціальних функцій наведено на рис. 2.

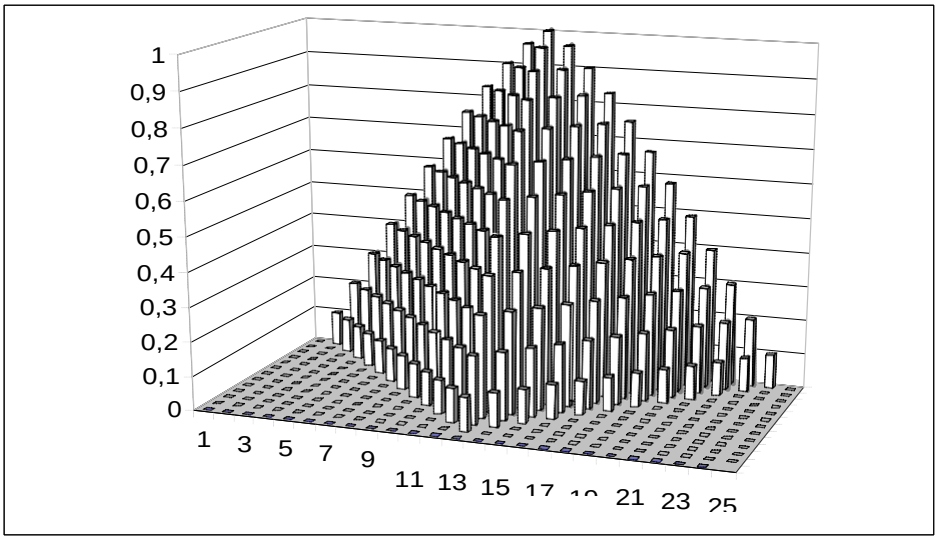
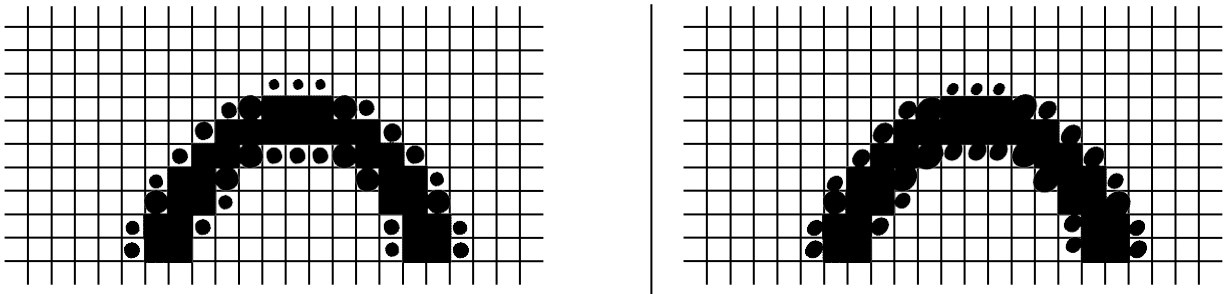


Рис. 2. Структура растрової точки, побудована на основі запропонованого методу

Модифікований метод автотипного растрування дає змогу точніше друкувати тонкі деталі та півтони для текстової або графічної інформації на матеріальних носіях. На рис. 3 зображено збільшений елемент тонкої графіки, надрукований двома способами. На рис. 3, а друк реалізовано

звійчаним методом растрування. На рис. 3, б елемент надруковано за розробленим методом, який дає можливість точніше відтворити тонкі деталі у звичайному растрованому зображенні.



а *б*

Рис. 3. Відтворення тонких деталей: а – звичайним методом; б – за модифікованим методом автотипного растрування

Висновки

Запропоновано метод формування растрової структури, оснований на спеціальній структурі растрової точки. Така структура спеціально адаптована для передавання у процесі друку тонких захисних графічних елементів та півтонів, що значно покращує якість друку. Переваги методу підтверджують проведені експерименти. Розроблений метод можна використати для підвищення ефективності графічного захисту інформації на паперових, пластикових та інших матеріальних носіях інформації.

1. Шевчук А. В., Музика В. П. Система захисту цінних паперів та документів суворого обліку – наукоємна проблема державного масштабу / А. В. Шевчук, В. П. Музика // Друкарство. – 2002. – № 4(45). – С. 72–74. 2. Запоточний В. Й. Технології захисту цінних паперів / В. Й. Запоточний. – Львів: Видавництво Львівської політехніки, 2011. – 128 с. 3. Киричок П. О. Захист цінних паперів та документів суворого обліку: монографія / П. О. Киричок, Ю. М. Коростіль, А. В. Шевчук. – К.: НТУУ "КПІ", 2008. – 368 с. 4. Коншин А. А. Защита полиграфической продукции от фальсификации / А. А. Коншин. – М.: Синус, 1999. – 160 с. 5. Кипхан Г. Энциклопедия по печатным средствам информации. Технологии и способы производства / Г. Кипхан [пер. с нем.]. – М.: МГУП, 2003. – 1280 с. 6. ДСТУ 4010-2001. Бланки цінних паперів і документів суворого обліку та звітності. Загальні технічні вимоги – К.: Держспоживстандарт України, 2001. – 38 с. 7. Грыцык В. В. Информационные технологии защиты документов средствами Ateb-функций. Ч. 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. 8. Kuznetsov Yuri V. Method of objective evaluation the fine detail distortion in process of screening / Yuri V. Kuznetsov, Denis E. Zheludev// IARIGAI. – 2008. – № 35. – С. 347–353.