УДК 531.36+534

О. Нечай[1], М. Назаркевич[2], Ю. Христиніна[3]
[1]Академія сухопутних військ імені гетьмана Петра Сагайдачного,
Національний університет "Львівська політехніка"
[2]кафедра інформаційних технологій видавничої справи,
[3]кафедра автоматизованих систем управління

РОЗРОБЛЕННЯ МОДЕЛЕЙ ЗАГРОЗ ДЛЯ ДРУКОВАНИХ ДОКУМЕНТІВ, ЗАХИЩЕНИХ ГРАФІЧНИМИ МЕТОДАМИ ЗАХИСТУ

Розроблено моделі загроз щодо друкованих документів. Проаналізовано графічні методи захисту документів. Розроблено метод ідентифікації документів, захищених за допомогою сіток Ateb-функцій.

Ключові слова: моделі загроз, ідентифікація, захист друкованих документів.

Models threats on printed documents. Graphical analysis methods of protecting documents. The method of identification documents protected by nets Ateb-functions.

Key words: Model threats, identification, protection printed documents

Вступ

На сучасному рівні інформаційного розвитку суспільства друковані документи відіграють важливу роль у функціонуванні держави. Розроблення нових та вдосконалення існуючих методів захисту друкованих документів має велике значення для безпеки функціонування інформаційних систем.

Державна, комерційна та будь-яка інша економічна діяльність неможливі без відповідного документообігу, тому захист документів від підробки регламентується відповідними нормативними документами [1]. До документів суворого обліку та звітності належать: 1) документи, що засвідчують особу, подію, право, освіту, трудовий стаж тощо (паспорт, свідоцтво про народження, одруження тощо, трудова книжка та вкладка до неї, посвідчення водія, службові, військові та інші посвідчення, дипломи про освіту, присвоєння звання, пенсійні документи і т.ін.); 2) проїзні документи (квитки на право проїзду у транспорті, документи на перевезення вантажів і т.ін.); 3) знаки поштової сплати (поштові марки, конверти та листівки з марками); 4) документи, що обслуговують грошовий обіг (ощадні, чекові та депозитні книжки; грошові, майнові та розрахункові чеки, бланки фінансування та страхування, акредитиви, податкові та митні марки, доручення на видачу коштів, пенсій та майна; сертифікати якості, ліцензії тощо) [2]. У [3] наведено вичерпний перелік документів, що підлягають захисту, та державних замовників, якими є МВС, Держмитслужба, ВАК, МОН, МОЗ, Мінпраці, Міноборони, Мінфін, Держпідприємництво, Нацбанк, Державна податкова адміністрація, Мінагрополітики, Держстат, Мінтранс. Захисту також підлягають службові посвідчення та посвідчення, які підтверджують право на отримання певних пільг, постійні перепустки до державних установ, окремі групи ліків, товарів народного вжитку тощо, які виготовляються за відповідним поданням центральних органів виконавчої влади.

Дослідження документів, які в сучасних умовах найчастіше змінюються та підробляються, є необхідним з метою подальшого удосконалення їхнього захисту, ефективного контролю їх достовірності [4].

Сучасний арсенал захисту документів від фальсифікації вагоміший від арсеналу фальсифікаторів [5]. Будь-який документ за правильного технологічного підходу можна захистити так, що фальсифікаторам буде дуже важко його підробити. Проте підробити можна будь-який найдосконаліший продукт. Якщо вартість підробки перевищує економічний ефект від її застосування, то тоді фальсифікація нерентабельна.

1. Аналіз методів захисту друкованих паперових носіїв інформації

Класифікацію методів графічного захисту показано на рис. 1. Серед методів графічного захисту слід виділити методи тангірних сіток, мікрографіку, гільйоші, скриті (приховані) зображення, наскрізні растрові елементи.

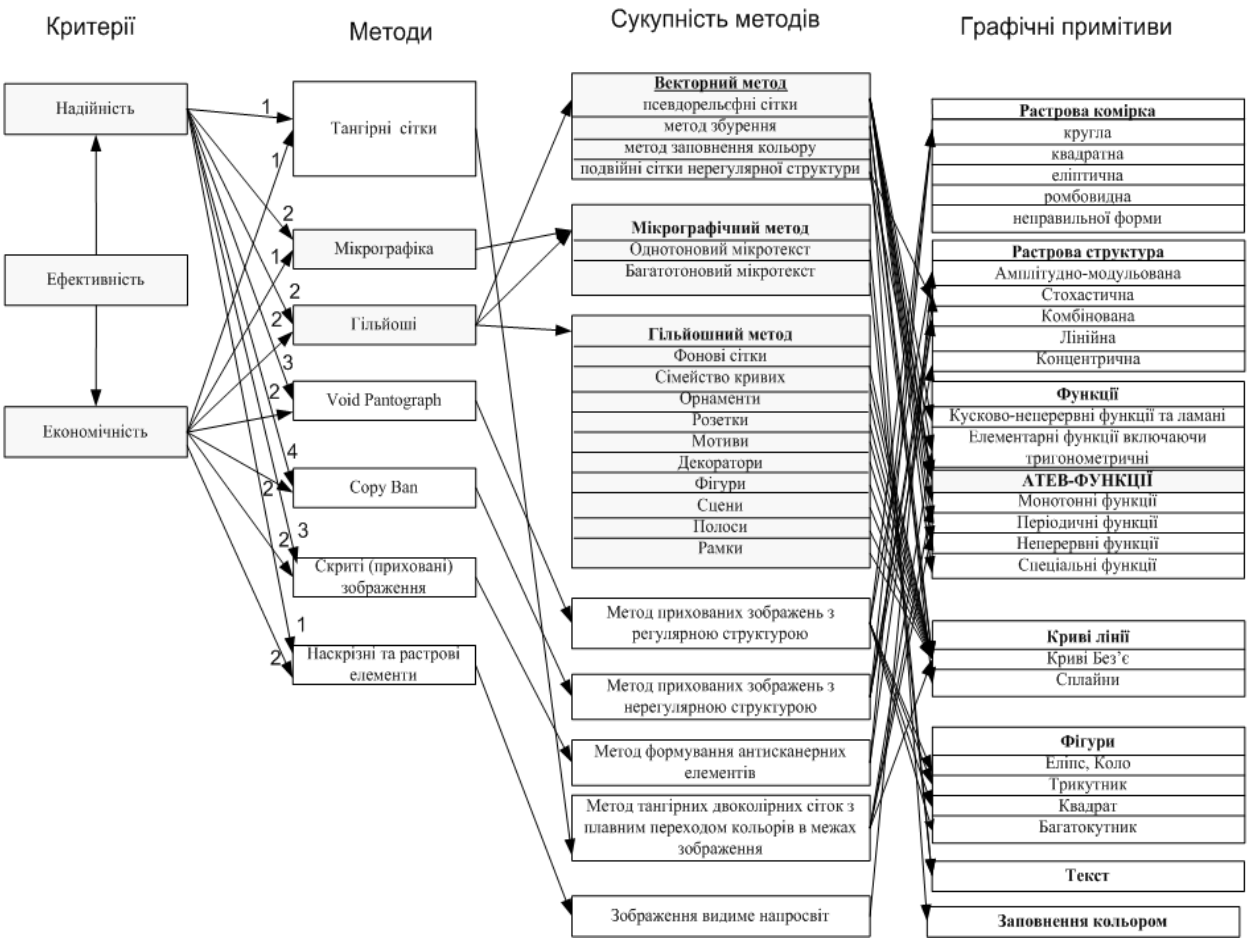

Рис. 1. Класифікація методів графічного захисту паперових носіїв

Створення зображень на цінних паперах у вигляді вигнутих ліній є достатньо надійним засобом захисту від підробок цінних паперів. Гільйоші є складним геометричним візерунком у вигляді сіток, бордюрів, розеток та інших фігурних композицій, що складаються з багаторазово повторюваних хвилястих та інших фігурних ліній. Гільйошні елементи можуть бути позитивними (див. фрагмент рис. 2, *е*) і негативними (див. фрагмент рис. 2, *д*). Позитивний гільйошний візерунок створюється темними кольоровими лініями, товщина яких значно менша за відстань між лініями гільйошу. Негативний гільйошний візерунок утворюється в результаті переважання світлих (незадрукованих) полів на захищеному папері, коли товщина задруковування візерунка значно ширша за відстань між найближчими лініями гільйошу.

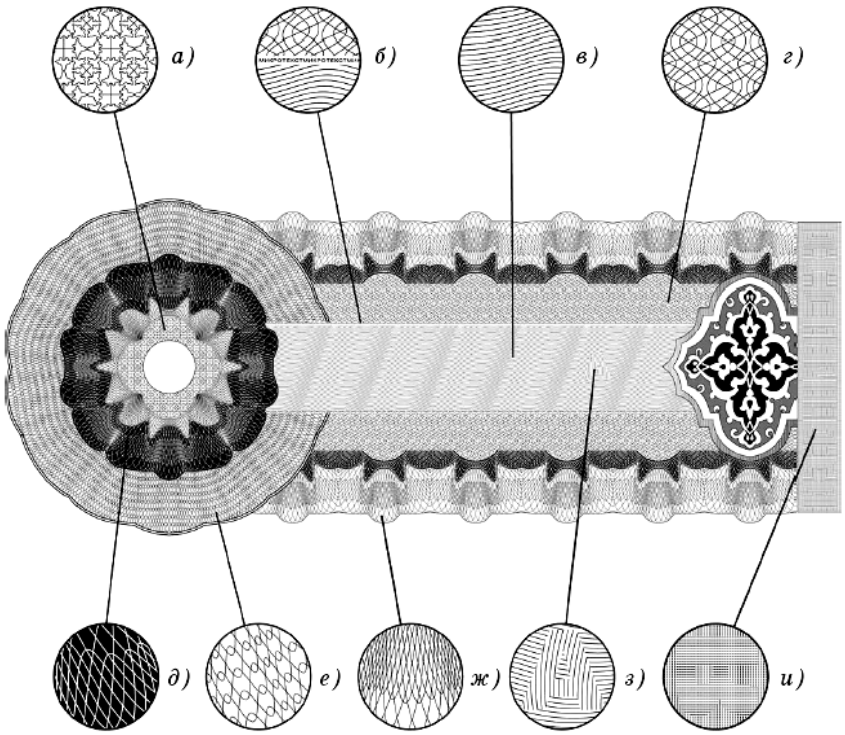

Рис. 2. Різновиди графічного захисту паперових носіїв

3. Основні види зловживань та фальсифікацій паперових носіїв інформації

Можна виділити п’ять основних видів зловживань для документів на паперових носіях (рис. 3):

1. Часткова підробка.
2. Повна підробка паперового носія.

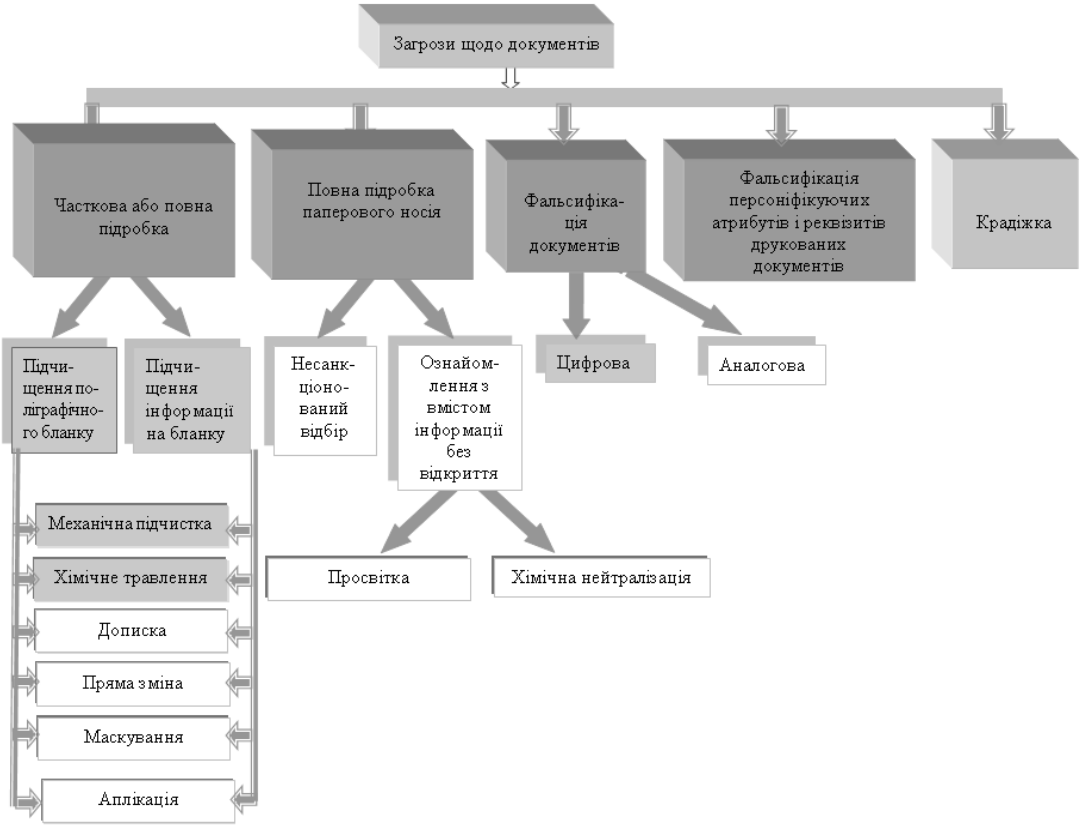

Рис. 3. Загрози інформаційним ресурсам на паперових носіях

3. Фальсифікація документів.

4. Фальсифікація персоніфікованих атрибутів та реквізитів друкованих документів.

5. Крадіжка.

Несанкціоновані заповнення та виправлення документів належать до найпростішого, дешевого та ефективного виду зловживань [5]. Найпоширенішим методом є підчистка первинної інформації документа і заміна її на фальсифіковану.

Такий вид зловживань можна поділити на два підвиди:

а) підчистка поліграфічного зображення. Цей вид фальсифікації використовується при підчистці і заміні номерів, серій та аналогічних атрибутів друкованих документів, цінних паперів, лотерейної продукції. Найпростішим прикладом такої фальсифікації є підчистка і заміна номеру в тиражних лотерейних квитках;

б) підчистка заповненої інформації. У такого виду фальсифікації об'єктом підчистки є змінна інформація в друкованих документах та цінних паперах, яка заповнюється на друкарських пристроях або вручну. Це найчастіше прізвища, імена, сума грошового виміру, особливі умови.

У розглянутих підвидах підробки достовірність паперового носія зберігається, але документ вже є фальсифікованим.

За всієї різноманітності специфіки кримінального інструментарія, який використовується для фальсифікації поліграфічної продукції, можна виділити такі методи технологічної підробки змінної інформації паперового носія [5]:

1) механічна підчистка основується на видаленні зображення з поверхні документа разом з мікрошаром поверхні паперу. Цей метод є доступний і економічний. Груба підчистка виявляється при перегляді паперового полотна під кутом до джерела світла у вигляді пошкодження фактури поверхні паперу. Професійну підчистку може встановити лише фахівець у лабораторних умовах. Найуразливіші для цього виду підчистки документи, які заповнюються на лазерному принтері. Тонер з незахищеної паперової поверхні видаляється легко і майже безслідно. При механічній підчистці особливо вразливою є група крейдованих глянцевих паперів. При всій естетичній привабливості цих паперів барвники найлегше і безслідно видаляються з її поверхні через низьку абсорбцію крейдованого шару. Встановлюють механічну підчистку шляхом вимірювання кольорів при кольороподілі, друкуванні фарб в ультрафіолетових, інфрачервоних променях, посиленні контрасту, виявлення слідів тиску. Однак зазначені способи є дієвими лише за умов контрольованого оточення за присутності спеціального інструментарію та кваліфікованого персоналу;

2) хімічне травлення застосовується в тих випадках, коли барвник глибоко абсорбує поверхню паперу або барвник має підвищену ефективність зчеплення з поверхневим шаром паперу.

Механічна підчистка в цьому випадку або неможлива, або занадто очевидні пошкодження поверхні паперу. Агресивні хімічні реагенти при хімічному травленні видаляють барвник з поверхні паперу шляхом розчинення або знебарвлюють його.

Залежно від хімічного складу барвника фальсифікатор підбирає відповідні хімічні реактиви для травлення. Сьогодні відомі сотні хімічних реактивів, а їх кількість постійно збільшується. Саме на обов'язковому застосуванні типових реагентів, що входять до складу хімреактивів для травлення, ґрунтується технологія захисту від хімічної підчистки.

Встановлюють хімічну реакцію візуально за допомогою лупи, мікроскопу або ж фотографують через сфітлофільтр в ультрафіолетових та інфрачервоних променях. Достовірність документа встановлюють на основі професійного приладового контролю;

3) фальсифікація зміною текстів домальовуванням окремих елементів букв, цифр, слів. Ознаками дописки є різні за шириною, кольорові елементи букв чи цифр; різна структура штрихів; присутність додаткових точок початку та закінчення рухів у дописаних елементах.

Способи встановлення аналогічні, як для травлення, а також зміна ширини штрихів.

4) пряма зміна здійснюється шляхом простого виконання на письмовому знаку іншого. Способи встановлення аналогічні вищевказаним;

5) маскування – пряме виконання за присутнім знаком іншого, ширшими штрихами і неодноразово повторюваними рухами або друком (друкарська машинка, принтер) або маскування за допомогою «чорнильної» плями. Способи встановлення аналогічні вищенаведеним.

Несанкціоноване ознайомлення з конфіденційною інформацією – такий вид зловживань поширюється на специфічні поліграфічні вироби, в яких частина або вся змістовна інформація є конфіденційною і несанкціоноване ознайомлення з нею є криміналом.

Умовно можна поділити цю продукцію за видом конфіденційної інформації:

а) персоніфікована інформація, що заноситься в поліграфічну продукцію в процесі обігу. До цієї групи поліграфічних виробів належать PIN-конверти, виписки рахунків, комерційна кореспонденція. До такої форми належить технологічна комбінація бланкової форми і конверту у вигляді готового поштового відправлення.

Практика показує, що для незахищеного від несанкціоного ознайомлення персоніфікованого документа загроза зловживання є надзвичайно великою.

Зазвичай несанкціоноване ознайомлення відбувається двома шляхами: відкриття документа з подальшим задруковуванням інформації та ознайомлення з вмістом персоніфікованого документа без відкриття шляхом просвічування або хімічної обробки паперового полотна з метою його знебарвлення;

б) індивідуальна інформація, що наноситься на кожен екземпляр і закривається від несанкціонованого ознайомлення при поліграфічному виконанні.

У цій групі документів найпоширенішими є лотерейні квитки. Конфіденційна інформація для цих документів – виграшні номери, номер, серія, контрольний розряд – наносяться в спеціальних полях, що закриваються спеціальною маскувальною фарбою scraping ink. Для ознайомлення з конфіденційною інформацією необхідно механічно видалити маскувальний шар, і тоді інформація стає помітною.

Відомо три методи фальсифікації маскуванням [5]:

1) хімічна нейтралізація (знебарвлення) маскує покриття з подальшим відновленням кольору покриття. Така технологія рідко вживається і є дорогою;

2) мікровідкриття маскувального шару, яке стає є помітним тільки за сильного збільшення;

3) поєднання несанкціонованого відбору інформації та прямої підчистки. Після видалення захисного шару і прямої підчистки змінної інформації аналоговим способом заповнюється нова інформація. Після цього захисний шар відновлюється.

Встановлення несанкціонованого втручання в персоніфікованих документах і лотерейних квитках ускладнюється тим, що в більшості випадків ця поліграфічна продукція імпортного виробництва і ідентифікація достовірності є складною.

Пряма підробка поліграфічної продукції – найефективніший і швидкий спосіб підробки друкованих документів, що досягає високої зовнішньої схожості або навіть претендує на ідентичність з оригіналом.

Пряма фальсифікація поділяється на «цифрову» та аналогову фальсифікацію [5].

«Цифрова» фальсифікація здійснюється методами цифрового репродукування. Цей метод дуже поширений та ефективний. Розвиток комп'ютерної техніки зробив цю технологію доступною. Сучасні настільні видавничі системи дають високий рівень репродукування, та подібності отриманої підробки до оригіналу [6]. Подібність до оригіналу – це характерна риса цифрової фальсифікації. Для великих тиражів цифрова фальсифікація непридатна через високу собівартість і низьку продуктивність.

Переважно об'єктом фальсифікації для цього способу підробок є документи, що є в обігу в неконтрольованій сфері.

Аналогова фальсифікація – найдорожча і найдосконаліша фальсифікація. Такий вид фальсифікації здійснюється тими самими методами, що і виготовлення оригіналу, або технологією, максимально наближеної до оригінальної. Цей вид фальсифікації передбачає застосування підробки в контрольованому оточенні, часто навіть пропущеної через приладовий контроль.

Отже, аналогова фальсифікація може бути в обігу на ринку нарівні з оригіналами. Впізнати професійну підробку можна тільки в умовах лабораторного контролю. Продукцію, підробка якої доцільна і економічно виправдана аналоговим методом, необхідно ретельно захищати від фальсифікації.

Крім того, у сфері аналогової фальсифікації склалася своєрідна практика «легальної» фальсифікації. Легально, шляхом розміщення замовлення на технологічно сильному підприємстві, виготовляються заготовки, напівфабрикати майбутніх підробок, які не мають персоніфікованої інформації, тобто, як правило, на заготовці відтворюється складна тонка графіка, а текст відсутній. Фальсифікатор, одержуючи у своє розпорядження напівфабрикат, виробляє "заготовку", тобто заповнює індивідуальною або змінною інформацією за допомогою найпростіших розмножувальних систем або поліграфічних технологій. У цьому випадку економічний ефект підробки особливо високий, а за правдоподібністю фальсифікації можна порівнювати з оригіналом.

Слід зазначити, що окремі види технології аналогової підробки в Україні неможливі через виняткову державну монополію на певні види друку: металографічний, орловський друк.

4. Аналіз основних видів зловживань щодо графічних методів захисту паперових носіїв

Група графічних захистів грунтується на складності 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.

Труднощі поліграфічного відтворення елементів тонкої графіки пов'язані зі специфічними технологічними умовами пристосування друкарських машин для відтворення такої графіки та з використанням низки специфічних «ноу-хау» в області друкарських технологій захисту [6]. Структурно групу графічних захистів можна підрозділити на наступні дві підгрупи за ознаками технологічної підробки:

1) графічні захисти, фальсифікація яких ґрунтується на спотворенні, руйнуванні або зникненні елементів тонкої графіки.

Тобто фальсифікаторам недоступна ідентична підробка, і при порівнянні з оригіналом візуально можна побачити значні руйнування або спотворення оригінального зображення. Особливо очевидна підробка, виконана цифровими методами.

Класифікація ступеня надійності технологій графічного захисту

Тип захисту	Ступінь надійності	Спосіб контролю			Технологічний ряд
		візуальний	приладами	лабораторний	
Графічні захисти					
Тангірні сітки	1	✓	✓	✓	1
Мікрографіка	2	✓	✓	✓	1
Void Pantograph	3	✓		✓	2
Copy Ban +	4	✓		✓	2
Гільйошні елементи	2	✓	✓	✓	1
Latent Image	3	✓	✓	✓	1
Маскувальні сітки і плашки	1	✓			11

У таблиці наведено класифікацію ступеня надійності захисних технологій [6]. Для надійного захисту існують графічні, хімічні захисти, захисти паперу, післядрукарські захисти, персоніфіковані та технологічні захисти. Кожному із зазначених способів захисту відповідає високотехнологічний ряд, зокрема найнадійнішими є технологічні захисти. Серед графічних способів захисту кращими є технології «Copy Ban», «Latent Image» та «Void Pantograph». Гільйошні елементи та мікрографіка мають дещо менший ступінь захищеності. Проте захищеність контролюється візуально та приладами, а також достовірність можна визначати у лабораторних умовах. За рядом технологій мікрографіка та гільйошні елементи займають перші позиції в технологічному ряді, що означає невисоку вартість та перспективу розвитку.

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 скановані. Для додаткового ускладнення відтворення гільйошних композицій використовують спеціальні технології друкування.

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

Приховані елементи «Latent image». При фальсифікації елементів тонкої графіки з прихованими зображеннями вони зникають або, навпаки, стають видимим. Такі ефекти ґрунтуються на виведенні зображень з високої роздільою здатністю ліній тонкої графіки.

Мікрографіка. Візуально мікрографіка сприймається як безперервна лінія. Тільки за 10–20-кратного збільшення видно, що безперервна лінія складається зі знаків і символів. Як правило, оптимальним елементом мікрографіки є шрифт. Тому найпоширенішим видом мікрографіки є мікрошрифт. Це зручно з погляду ідентифікації автентичності. Користувачеві не потрібно шукати руйнування або уривчастість елементів тонкої графіки (що для нефахівця важко зробити однозначно). Користувачеві достатньо перевірити присутність напису мікрошрифтом у заданому місці. Якщо мікротекст не читається або погано читається, є загроза фальсифікації продукції. Рекомендовані висоти мікрошрифта, що утворюють мікротекст для позитивного зображення – 200–300 мікрон, для негативного зображення – 300–400 мікрон. При ксерокопіюванні і скануванні мікротекст утворює неперервну лінію.

Навіть при розпізнанні фальсифікатором присутності мікрошрифта його відтворення аналоговим способом в заданих технічних параметрах вимагає найвищого технологічного оснаення та кваліфікації. Найбільш виправданим є застосування мікрошрифтів у сфері сертифікованих захистів, орієнтованих на умови контрольованого оточення.

Призматичний, або ірисний, друк – ще один спосіб захисту, де створюється багатофарбовий фон, який ускладнює кольорове ксерокопіювання або сканування. Такий плавний перехід не відтворюється копіюванням або скануванням. Відтворення призматичного ірисного друку вимагає не лише спеціалізованого обладнання, а й деякого «ноу-хау» в області захисних поліграфічних технологій.

З іншого боку, існує група захистів, при ксерокопіюванні або скануванні яких стає видимим приховане зображення в елементах тонкої графіки оригіналу. Ця група захистів орієнтована переважно на захист від цифрової фальсифікації. Хоча водночас висвітлення прихованих друкованих елементів при ксерокопіюванні оригіналу поліграфічного виробу може бути ознакою достовірності та способом ідентифікації автентичності. Отже, за першим варіантом цей захист ефективно працює в умовах неконтрольованого оточення, за другим варіантом – в умовах контрольованого оточення. В обох випадках практика показує доцільність використання цих захистів у вигляді оголошених. Найвідоміші два різновиди таких захистів [5]: «Void Pantograph» і «Copy ban +».

5. Метод повного повіксельного порівняння для визначення достовірності друкованих документів

Розглянутий метод ідентифікації можна використати для персоніфікації даних документів та для розпізнавання кривих, *виконаних графічними методами захисту* [8]. У багатьох задачах виникає проблема визначення достовірності документа загалом. Для розв'язання цієї задачі запропоновано метод повного попіксельного порівняння еталонного та контрольованого зображення. Нехай контрольоване зображення $P(x, y)$ та еталонне зображення $P_0(x, y)$ мають розмір $m_p n_p$ пікселів.

Як критерій порівняння вибрано метод попіксельного порівняння, який виражений через коефіцієнт *PSNR* [7]. Що більше значення коефіцієнта *PSNR*, то ближче контрольоване зображення до еталонного, який обчислюється за формулою

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

де $MaxP$ – максимальна кількість градацій сірого у контрольованому зображенні.

Результати ідентифікації наведено на рис. 5.

Рис. 5. Ідентифікація документа та встановлення його достовірності

Висновки

Розроблено моделі загроз для друкованих документів. Здійснено класифікацію методів графічного захисту. Проаналізовано методи графічного захисту, серед яких можна виділити тангірні сітки, мікрографіку, гільйоші, скриті (приховані) зображення, наскрізні растрові елементи Показано методи і засоби ефективної протидії загрозам для документів.

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 (нова редакція) // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. 2. Закон України "Про цінні папери і фондову біржу" // Відомості Верховної Ради, 1991. – №38. – Ст.508 (Із змінами, внесеними згідно із Законами... №1455-IV (1455-15) від 05.02.2004, ВВР, 2004. – №19. – Ст.271. 3. Постанова від 03.07.2006 № 895 (Редакція станом на 11.03.2011) "Про затвердження документів та груп товарів, що підлягають захисту голографічними елементами". 4. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко // Підручник МОН України. – К.: Видавництво DIRECTLINE, 2009. – 714 с. 5. Коншин А.А. Защита полиграфической продукции от фальсификации / А. А. Коншин. – М.: Синус, 1999. – 160 с. 6. 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. 7. Путятин Е.П., Аверин С.И. Обработка изображений в робото-технике. – М.: Машиностроение, 1990. – 320 с. 8. Назаркевич М. Ідентифікація даних кореляційними методами на основі Ateb-функцій/ М. Назаркевич, І. Вербенко. // Вісник Державного університету "Львівська політехніка". "Комп'ютерні науки та інформаційні технології". – 2011. – № 719. – С.308–313.