

УДК 004.056.5:655.25

АНАЛІЗ ПРОЦЕСУ РОЗРОБКИ ЕЛЕМЕНТА ЗАХИСТУ НА ДОДРУКАРСЬКІЙ СТАДІЇ ОПРАЦЮВАННЯ ЗОБРАЖЕНЬ

В. В. Семенів, М. Р. Семенів, Х. Б. Кульчицька

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Наявність невидимого елемента захисту Void Pantograph, який може бути закладений у структурі растрового фону, унеможливить відтворення оригіналу при скануванні, копіюванні чи фотографуванні. Виконується такий елемент на стадії дизайну продукції у програмі опрацювання растрової чи векторної графіки. Досліджено процес перетворення зображення фону та прихованого елемента із градацій сірого у бітовий режим. Визначено значення відносної площі растрових елементів залежно від кольору заливки фонового зображення та прихованого елемента. Залежність має нелінійних характер, отримана нелінійність характеризується показником степеня, що дорівнює 1,72. Здійснено тестовий друк зображення з прихованим елементом з різною лініатурою растра. За низьких лініатур отримано високий контраст між фоновим зображенням і прихованим елементом. Найменше значення контрасту спостерігалось при заданій лініатурі растра 105 lpi. Відсутність контрасту дає змогу приховати захисний елемент, а відмінна від фону форма растра — проявити його після копіювання та ускладнити процес фальсифікації документа.

Ключові слова: елемент захисту, зображення, растрування, лініатура.

Постановка проблеми. Високий рівень захисту поліграфічної продукції забезпечує комплекс заходів та технологій, спрямованих на запобігання фальсифікації та забезпечення конфіденційності, цілісності та автентичності документів та цінних паперів.

Проте розроблення і застосування спеціальних видів друку, використання спеціальних фарб і лаків, нанесення голограм не завжди є економічно вигідними. Застосування матеріалів зі спеціальними хімічними чи фізичними властивостями потребує спеціального обладнання, яке виявляє фальсифікати. Найпростішими, зручними та економічно доцільними є засоби захисту, що реалізуються на додрукарському етапі виготовлення поліграфічної продукції. Їх застосування не потребує спеціального устаткування і матеріалів. Водночас їх використання для створення комбінованих засобів захисту залишається можливим [1].

Захист поліграфічної продукції на додрукарській стадії реалізовується за допомогою елементів захисту: гільйошні елементи; спеціальні лінійні растри; графюри; спеціальні «дефекти»; мікротекст; об'ємні ефекти; приховані елементи; контрольні і штрихові коди і ноу-хау [1].

Сканери та кольорові копіювальні апарати мають обмеження щодо роздільної здатності та колірної гами. Якщо перевищити ці обмеження, тоді документи можна графічно захистити кількома способами. Одним із найефективніших графічних способів, стійких до копіювання, є створення фону документа за допомогою (самоскасовуваного) Void Pantograph (VP), який містить приховане повідомлення. Під час фотокопіювання або сканування повідомлення відображається на копії.

Незважаючи на те, що VP можна позбутися, змінивши параметри щільності копіювального апарату, у поєднанні з іншими перевіреними графічними ефектами, такими як мікротекст, тонкий рельєф, тонкий фантомний логотип і попереджувальна смуга, освітлена копія втратить багато деталей і виглядатиме підробленою [2].

Актуальність розробки елемента захисту VP полягає в його ефективності для підвищення безпеки документів. Використовуючи такі методи, організації можуть захистити конфіденційні документи, такі як сертифікати, ідентифікаційні картки, банкноти та інші цінні документи, від спроб шахрайського відтворення. Оскільки методи підробки стають дедалі витонченішими, функції безпеки, як-от VP, відіграють вирішальну роль у випередженні фальшивомонетників і збереженні цілісності важливих документів.

Важливо зазначити, що розробка захисних функцій, таких як VP, передбачає поєднання дизайну, технології друку та матеріалознавства для створення візерунків, які важко точно відтворити.

Аналіз останніх досліджень та публікацій. Захисні елементи тонкої графіки — це складні для копіювання та відтворення графічні елементи, такі як сітки, розетки, віньетки, приховані елементи, мікрографіка та мікротекст. Їх копії важко відтворити навіть за допомогою найсучасніших цифрових технологій. Проблема у тому, що ці елементи тонкої графіки мають складну структуру і формуються надзвичайно тонкими лініями та іншими графічними примітивами.

Результати патентного пошуку [3–6] свідчать про те, що є достатня кількість винаходів, що належать до способів створення, використання та генерування елементів захисту VP. У публікації [7] автори описують автоматизований процес оптимізації налаштувань VP. Шаблони фону та переднього плану, які використовуються у VP, — фон, що зникає під час копіювання, та передній план, що виділяється. Серед актуальних досліджень потрібно виокремити метод захисту цінних паперів за допомогою прихованих зображень з високою роздільною здатністю. Метод захисту полягає у застосуванні іншої, відмінної від основного рисунку, лініатури растра та фрактальних пасток [8].

Мета статті — враховуючи актуальність теми, метою роботи є розробити елемент захисту VP. Відповідно до мети сформульовано такі завдання: розробити прихований елемент захисту; визначити оптимальні параметри процесу для відтворення елемента захисту при копіюванні; проаналізувати технологічний процес розробки елемента захисту VP.

Виклад основного матеріалу дослідження. Захисний елемент VP належить до методу створення чітких та захищених від фальсифікацій шаблонів на задньому фоні документа. Зазвичай вони невидимі для ока, але стають очевидними, коли

документ копіюється. Наявність невидимого елемента захисту, який може бути закладений у структурі растрового фону, унеможливить відтворення оригіналу під час сканування, копіювання чи фотографування. Саме при цих діях на фоні проявляється прихований текст, який вказує на дублювання оригіналу. Якість відтворення елемента VP залежить від вихідних змінних, таких як лініатура, кут повороту растра, величина кута ліній, роздільної здатності зображення загалом, роздільної здатності вивідного пристрою. Виконується такий елемент на стадії дизайну продукції у програмі опрацювання растрової чи векторної графіки. Растрова структура елемента при друкуванні має повністю суміститись з растровою структурою фону і так приховати елемент захисту. Під час копіювання чи сканування оригінального документа растрові структури накладаються і в результаті отримаємо на фоні проявлений прихований елемент захисту.

Розміри такого елемента залежать від роздільної здатності пристрою виведення. Основними параметрами, які змінено у процесі створення елемента захисту, є лініатура та кут повороту растра фонового візерунку та лініатури та кут повороту растра для елемента захисту.

Для виведення тестового файлу на лазерному принтері застосовано програмне забезпечення для опрацювання растрової графіки Adobe PhotoShop. У цьому програмному забезпеченні є можливість перетворити зображення в бітовий режим. Для перетворення кольорового зображення у режим bitmap спершу потрібно перетворити його у градації сірого. Це означає, що ми видаляємо інформацію про кольори і лишаємо лише інформацію про яскравість пікселів. Але у бітовому режимі ми можемо використовувати лише два кольори: чорний і білий. Тому оптимальним рішенням є редагування у режимі градацій сірого і потім перетворення у режим bitmap. У діалоговому вікні налаштування бітового режиму є можливість обрати імітацію півтонових растрових елементів у конвертованому зображенні [9].

Зауважимо, що півтоновий растр стає частиною зображення. Якщо друкувати зображення на принтері, то при друкуванні буде застосований власний растровий візерунок. Результатом такого друку буде муаровий візерунок. Щоб цього уникнути необхідно в налаштуваннях принтера не обирати растровий візерунок.

Щоб надрукувати фотографію високої якості на принтері, роздільна здатність зображення має бути не менше 220 ppi [10], оптимальне значення 300 ppi. Зважаючи на роздільну здатність принтера $R_{\text{вив}} = 1200 \text{ dpi}$, при створенні документа задаємо роздільну здатність — 1200 ppi, необхідний розмір елемента захисту — $15 \times 8 \text{ см}$, режим кольору — градації сірого (8 біт).

За допомогою палітри Color Picker (Підбір кольору) обираємо рівень яскравості заливки фонового зображення та прихованого елемента VP: встановлюємо координати RGB (185, 185, 185), що відповідають координатам CIE Lab (75, 0, 0).

Перетворення зображення в бітовий режим виконуємо за допомогою команди Image (Зображення) → Mode (Режим) → Bitmap... (Бітове зображення). У налаштуваннях необхідно обрати роздільну здатність для виведення: 1200 ppi та обрати один з методів. Серед методів доступні: 50 % Threshold (50 % ізогелія), Pattern Dither (Регулярне змішування), Diffusion Dither (Невпорядковане змішування),

Halftone Screen... (Напівтоновий растр) та Custom Pattern (Власний візерунок). Обираємо Напівтоновий растр, що своєю чергою відкриє нове вікно налаштувань. Необхідно вказати Лініатуру растра (Frequency), кут повороту растра та форму растрового елемента: кругла — для фонового зображення, лінія — для прихованого елемента захисту.

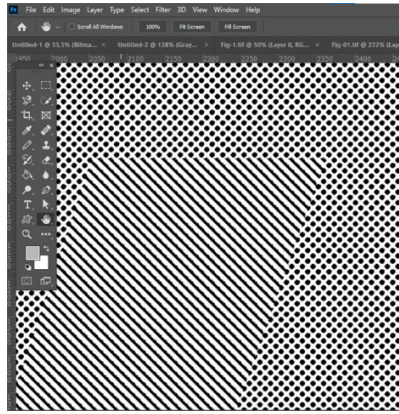


Рис. 1. Зображення прихованого елемента захисту Void Pantograph

Для порівняння результатів змінено параметри режиму Bitmap на такі: роздільна здатність виведення — 300 ppi, лініатура растра — 120 lpi. Такі значення з низькою роздільною здатністю виведення та високою лініатурою обрані для того, щоб зімітувати процес проявлення прихованого елемента. При зміні масштабу перегляду на Фактичний розмір (Actual Size) зникає фон і проявляється напис «VOID» (рис. 2, а). Якщо масштаб перегляду обрати Розмір Друку (Print Size), то спостерігатимемо на екрані лише фон з прихованим написом (рис. 2, б).



Рис. 2. Зображення прихованого елемента захисту:
а) — фактичний розмір; б) — розмір друку

Визначено значення відносної площі растрових елементів залежно від кольору заливки фонового зображення та прихованого елемента VP. Для цього перетворення в Bitmap здійснювалось для кожного досліджуваного значення кольору в моделі CIE Lab. Параметри перетворення були незмінні, відрізнялись лише формою растрового елемента: круглий та лінія. Збережені відрастровані bitmap-зображення проаналізовано в розробленій комп'ютерній програмі, яка зчитує кольори пікселів зображення та вираховує співвідношення кількості пікселів чорного кольору до кількості пікселів білого кольору. Результати подані у таблиці.

Таблиця

**Значення відносної площі растрових елементів
відповідно до яскравості пікселів**

Номер з/п	Яскравість L, од. CIE Lab	Відносна площа растрового елемента, $1-S_{відн}$ (%)
1	0	0
2	5	3,12
3	10	5,08
4	20	9,77
5	25	12,50
6	30	16,02
7	40	23,44
8	50	32,43
9	60	42,97
10	70	55,47
11	75	62,11
12	80	68,75
13	90	83,59
14	100	100,00

На основі отриманих результатів побудовано графік залежності значень відносної площі растрових елементів від рівнів яскравості пікселів зображення (рис. 3). Залежність має нелінійний характер, отримана нелінійність характеризується показником степеня, що дорівнює 1,72.

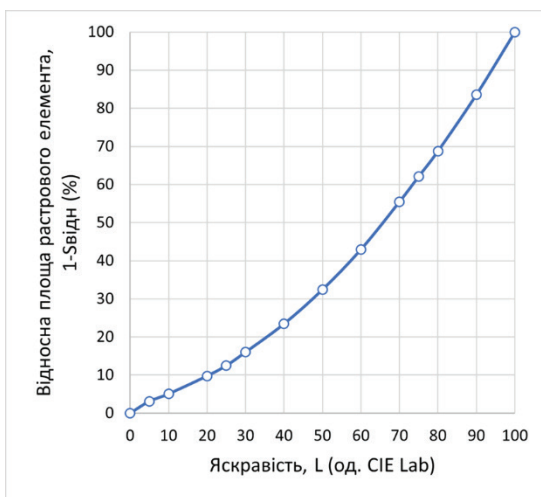


Рис. 3. Нелінійна залежність значень відносної площі растрових елементів від рівнів яскравості пікселів зображення

Співвідношення роздільної здатності зображення та лініатури растра визначає якість деталізації віддрукованого зображення. Для створення півтонового зображення найвищої якості зазвичай використовується роздільна здатність зображення, більша за лініатуру растра в 1,5–2 рази [10]. На вибір лініатури растра впливає: група складності зображень, спосіб друку, технологія і устаткування, задруковуваний матеріал. Якщо лініатура растра встановлена на 120 lpi, а роздільна здатність принтера становить 1200 dpi, тоді сторона комірки растра дорівнює $1200/120=10$ крапкам. У такому випадку растрова крапка формується з 10×10 крапок принтера [11].

Здійснено тестовий друк зображення з прихованим елементом VP з різною лініатурою растра: 60, 80, 90, 96, 100, 105, 110, 115, 120, 240 lpi. Для визначення оптимальної лініатури растра для заданих умов друку на відбитках визначено значення контрасту K (%) між фоновим зображенням і прихованим елементом за формулою (1).

$$K = \left(\frac{K_1 - K_2}{K_1} \right) \cdot 100\%, \quad (1)$$

де K_1 — рівень яскравості (L) фону; K_2 — рівень яскравості (L) елемента.

За низьких лініатур отримано високий контраст між фоновим зображенням і прихованим елементом. Найменше значення контрасту спостерігалось при заданій лініатурі растра 105 lpi. Також лініатури 96, 100, 115 lpi для заданих умов друку формують невисокий контраст між фоновим зображенням і прихованим елементом.

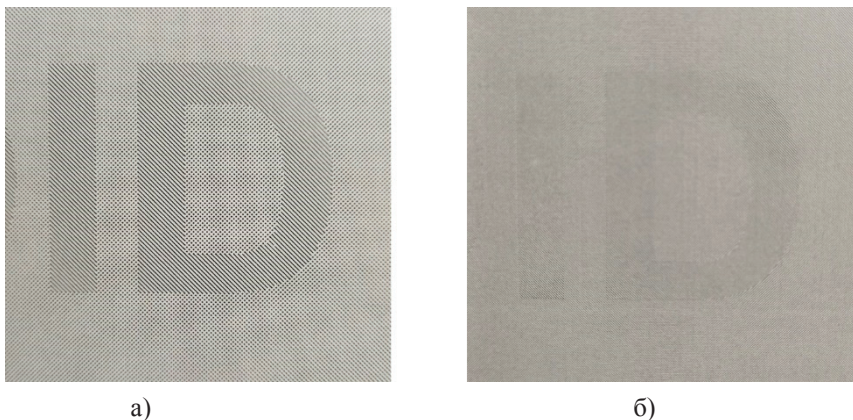


Рис. 4. Фотографії тестових відбитків з лініатурою растра: 60 (а) та 105 (б) lpi

Відсутність контрасту дає змогу приховати захисний елемент, а відмінна від фону форма растра — проявити його після копіювання та ускладнити процес фальсифікації документа.

За результатами досліджень побудовано графік залежності значення контрасту фонового зображення та прихованого елемента від лініатури растра. Оптимальною лініатурою растра серед досліджуваних значень є 105 lpi.



Рис. 5. Графік залежності величини контрасту зображень від лініатури растра

Здійснено копіювання документа з нанесеним прихованим елементом захисту за допомогою багатофункційного пристрою. Під час копіювання на фоні проявився напис «VOID». Узгодженість інтервалів оптичних густин сканера $\Delta D_{ск}$ та оригіналу $\Delta D_{ор}$ впливає на якість сканування. Якщо $\Delta D_{ск} < \Delta D_{ор}$, можлива втрата градації та елементів зображення. Також на якість сканованого зображення впливає розрядність або глибина кольору сканера.

Для друку кольорового документа, який потребує захисту, наприклад сертифікату, параметри режиму Vitmar будуть іншими. Оскільки цифрова друкарська машина забезпечує роздільну здатність виведення понад 2400 dpi. Необхідно врахувати, що друк здійснюється фарбами СМΥК. У такому випадку розроблений елемент захисту необхідно скопіювати в один з каналів фарб СМΥК.

Висновки. Отже, досліджуваний прихований елемент захисту VP може бути використаний для запобігання копіювання документів, друк яких здійснюється лазерним принтером. Прихований елемент захисту на роздрукованому документі зливається з фоном. Під час копіювання на фоні проявився напис «VOID». Якість відтворення елемента VP залежить від лініатури растра тексту та фонового малюнка, кута повороту растра, величини кута ліній, роздільної здатності зображення загалом, роздільної здатності вивідного пристрою. Визначена нелінійність процесу перетворення із градацій сірого у бітове зображення характеризується показником степеня, що дорівнює 1,72. За низьких лініатур отримано високий контраст між фоновим зображенням і прихованим елементом. Відсутність контрасту між фоновим зображенням і прихованим елементом дає змогу приховати його, а відмінна від фону форма растра — проявити захисний елемент після копіювання і у такий спосіб ускладнити процес фальсифікації документа.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Назаркевич М., Троян О. Розроблення програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням. *Вісник Національного*

- університету «Львівська політехніка». *Комп'ютерні системи та мережі*. 2014. № 806. С. 187–194.
2. Reputable Security Document Printers. URL: <https://www.amgraf.com/pages/voidmaker.html>.
 3. Method of generating void pantographs: EP 2783878B1. № 13190169.6; Date of filing: 24.10.2013; Date of publication: 01.10.2014, Bulletin 2014/40. 19 p.
 4. Automated calibration and optimized patch set creation for void pantograph: US20220398419A1. Date of filing: 10.06.2021; Date of publication: 15.12.2022.
 5. Full color, digitally printed copy evident documents: US10469706B2. № 13190169.616/146,477; Date of filing: 28.09.2018; Date of publication: 05.11.2019. 22 p.
 6. Verifying document security using an infrared VOID pantograph mark: US10812675B1; № 16/550,746; Date of filing: 26.08.2019; Date of publication: 20.10.2020. 14 p.
 7. Aronoff J. S., Simske S. J., Sturgill M. Automated Optimization of Void Pantograph Settings. URL: https://www.researchgate.net/publication/267232468_Automated_Optimization_of_Void_Pantograph_Settings.
 8. Назаркевич М., Возній Ю. Метод захисту матеріальних носіїв інформації латентними елементами. *Кібербезпека: освіта, наука, техніка*. 2019. № 3 (3). С. 27–41. Doi: <https://doi.org/10.28925/2663-4023.2019.3.2741>.
 9. Перетворення між колірними режимами. URL: <https://helpx.adobe.com/ua/photoshop/using/converting-color-modes.html>.
 10. Розмір і роздільна здатність зображення. URL: <https://helpx.adobe.com/ua/photoshop/using/image-size-resolution.html>.
 11. Предко Л. С. Проектування додрукарських процесів. навч. посіб. Львів : УАД, 2009. 352 с.

REFERENCES

1. Nazarkevych, M., & Troyan, O. (2014). Rozroblennia prohramnoho produktu dlia zakhystu informatsii na osnovi plivok iz prykhovanyum latentnym zobrazhenniam: Visnyk Natsionalnoho universytetu «Lvivska politekhnika». *Kompiuterni systemy ta merezhi*, 806, 187–194 (in Ukrainian).
2. Reputable Security Document Printers. Retrieved from <https://www.amgraf.com/pages/voidmaker.html> (in English).
3. Method of generating void pantographs: EP 2783878B1. № 13190169.6; Date of filing: 24.10.2013; Date of publication: 01.10.2014, Bulletin 2014/40. 19 p. (in English).
4. Automated calibration and optimized patch set creation for void pantograph: US20220398419A1. Date of filing: 10.06.2021; Date of publication: 15.12.2022 (in English).
5. Full color, digitally printed copy evident documents: US10469706B2. № 13190169.616/146,477; Date of filing: 28.09.2018; Date of publication: 05.11.2019. 22 p. (in English).
6. Verifying document security using an infrared VOID pantograph mark: US10812675B1; № 16/550,746; Date of filing: 26.08.2019; Date of publication: 20.10.2020. 14 p. (in English).
7. Aronoff, J. S., Simske, S. J., & Sturgill, M. Automated Optimization of Void Pantograph Settings. Retrieved from https://www.researchgate.net/publication/267232468_Automated_Optimization_of_Void_Pantograph_Settings (in English).
8. Nazarkevych, M., & Voznyi, Y. (2019). Metod zakhystu materialnykh nosiiv informatsii latentnyimi elementamy: *Kiberbezpeka: osvita, nauka, tekhnika*, 3(3), 27–41. Doi: <https://doi.org/10.28925/2663-4023.2019.3.2741> (in Ukrainian).

9. Peretvorennia mizh kolirnymy rezhymamy. Retrieved from: <https://helpx.adobe.com/ua/photoshop/using/converting-color-modes.html> (in Ukrainian).
10. Rozmir i rozdilna zdatnist zobrazhennia. Retrieved from: <https://helpx.adobe.com/ua/photoshop/using/image-size-resolution.html> (in Ukrainian)
11. Predko, L. S. (2009). Proektuvannia dodrukarskykh protsesiv. Lviv (in Ukrainian).

doi: 10.32403/2411-3611-2023-1-43-40-48

ANALYSIS OF THE PROTECTION ELEMENT DEVELOPMENT PROCESS AT THE PREPRESS STAGE OF IMAGE PROCESSING

M. R. Semeniv, V. V. Semeniv, Kh. B. Kulchytska

*Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
krykm@ukr.net*

The presence of an invisible Void Pantograph security element, which can be embedded in the structure of the image background, will make it impossible to reproduce the original when scanning, copying or photographing. The quality of the reproduction of the element depends on the output variables, such as: frequency, halftone screen rotation angle, line angle, image resolution in general, resolution of the output device. Such an element is performed at the stage of product design in a graphics processing program. The process of converting the background image and the hidden element from grayscale to bitmap mode is studied. The value of the relative area of raster elements depending on the fill color of the background image and the hidden element is determined. The dependence has a non-linear character; the resulting non-linearity is characterized by a power factor equal to 1.72. The ratio of the image resolution and the halftone screen frequency determines the quality of detail of the printed image. A test print of an image with a hidden element Void Pantograph with different halftone screen frequency is performed. To determine the optimal frequency for the given printing conditions on the imprints, the contrast value between the background image and the hidden element is determined. With low frequency, a high contrast between the background image and the hidden element is obtained. The lowest contrast value is observed at the given frequency of 105 lpi. The lack of contrast makes it possible to hide the security element, and the shape of the halftone screen, different from the background, makes it visible after copying and complicates the process of falsifying the document. Therefore, the researched hidden security element can be used to prevent copying of documents.

Keywords: security element, image, halftone screening, frequency.

Стаття надійшла до редакції 16.02.2023.

Received 16.02.2023.