

3. Стратегія державної міграційної політики України на період до 2025 р. Схвалено розпор. КМУ від 12.07.2017 р. № 482-р. // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/482-2017-%D1%80#n10/> (дата звернення: 09.10.2018).

4. Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Затверджено постановою КМУ від 27.12.2017 р. № 1073. // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/1073-2017-п> (дата звернення: 09.10.2018).

5. Волеводз А. Г. Удостоверяющие личность документы с биометрическими персональными данными: международные стандарты, иностранный опыт, ответственное правовое регулирование и его проблемы. *Ученые записки СПб филиала РТА*. 2015. № 1 (53). С. 87-117.

6. Doc 9303. Машиносчитываемые проездные документы Часть 3. Спецификации, общие для всех МСПД / ИКАО. URL: https://www.icao.int/publications/Documents/9303_p3_cons_ru.pdf (дата звернення: 09.10.2018).

7. ICAO. Security and Facilitation. Facilitation Programme. PKD. ePassport.Basics. URL: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx> (дата звернення: 10.10.2018).

8. EUROPOL and FRONTEX strengthen cooperation to tackle cross border crime / EUROPOL. 05 October 2018. URL: <https://www.europol.europa.eu/newsroom/news/europol-and-frontex-strengthen-cooperation-to-tackle-cross-border-crime> (дата звернення: 10.10.2018).

9. EUROPOL supports joint investigation into international human trafficking / EUROPOL. 15 February 2017. URL: <https://www.europol.europa.eu/newsroom/news/europol-supports-joint-investigation-international-human-trafficking> (дата звернення: 10.10.2018).

10. Resolution 2396 (2017) / adopted by the Security Council at its 8148th meeting, on 21 December 2017/ United Nations. Digital Library. URL: https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf (дата звернення: 09.10.2018).

Одержано 10.10.2018

УДК 004.93

Артем Олександрович ФРОЛОВ,

*аспірант кафедри твердотільної електроніки та інформаційної безпеки
фізичного факультету*

Ужгородського національного університету

ШИФРУВАННЯ КОЛЬОРОВИХ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ МАТРИЦЬ АДАМАРА

Сучасні поліграфічні і комп'ютерні технології стали загальнодоступними і дозволяють легко відтворювати зовнішній вигляд практично будь-якого документу. Навіть сама найскладніша поліграфія не в змозі самостійно забезпечити належний рівень захисту

від підробок. У зв'язку з цим, актуальним завданням є розробка принципово нових методів захисту інформації від кіберзлочинності, ефективність яких пов'язана з використанням сучасної комп'ютерної техніки та її поєднанням з високоточними математичними методами обробки зображень.

Об'єктом дослідження є технологічний процес виготовлення форм кодованого зображення для технології захисту інформації збереженої на кольорових зображеннях на основі впорядкованих неперіодичних кодуючих структур Адамара.

Предметом дослідження є методи, способи та алгоритми формування кодуючих структур Адамара, технологічні параметри та умови виготовлення форм кодованих зображень, створення нової інформаційної технології захисту кольорових зображень, яка забезпечує високий рівень захисту.

Розрізняють чотири основні типи матриць Адамара (Рис. 1):

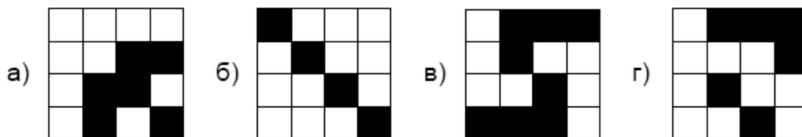


Рис. 1. Типи базових матриць Адамара.

Канонічні матриці Адамара (типу С), в яких всі елементи одного рядка і одного стовпця рівні 1. Типовим прикладом є симетрична канонічна матриця Адамара H_c .

«Світлі» матриці Адамара з мінімальною кількістю елементів рівних -1. Прикладом є діагональна матриця Адамара H_L (тип L).

Матриці Адамара «50/50» з однаковою кількістю елементів рівних 1 і -1 (тип M). Прикладом такої матриці є S-подібна матриця Адамара.

Напівканонічні матриці Адамара (тип D). Перший стовпець, що містить 4 елементи, характеризується співвідношенням «3/1», тобто має 3 світлих елементи і 1 темний, а наступні три стовпці – співвідношеннями «1/3».



Рис. 2. Принципова схема кодування зображень.

Спосіб виготовлення графічного елементу захисту кольорових зображень полягає в тому, що з вхідного зображення формують кодоване зображення з використанням спеціальної комп'ютерної

програми, за допомогою якої вхідне зображення перетворюють у багаторівневе графічне зображення, кожен рівень якого замінюють матрицею комірок впорядкованої неперіодичної структури. Кодоване зображення друкують на об'єкті захисту, а з другого його боку інверсно друкують ключ кодованого зображення, точно сумістивши його з кодованим зображенням. Внаслідок цього у відбитому світлі на документі кодоване зображення та його ключ візуально подібні і сприймаються як нейтрально сірий чи кольорового відтінку однорідний тон. У прохідному світлі спостерігається видиме зображення закодованої фігури графічного елемента, колір якого може бути відмінний від кольорів кодованого зображення та ключа, що служить критерієм оригінальності цінного паперу (рис. 2).

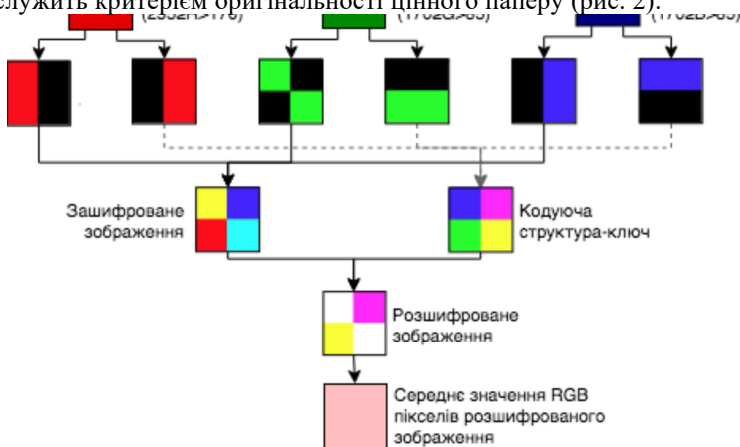


Рис. 3. Схема поділу кольорового пікселя.

Алгоритм кодування кольорових зображень складається з наступних кроків:

1. Зберегти в масив дані кожного пікселя кольорового зображення (R, G, B)
2. Створити зображення-ключ з випадково розставленими кольоровими кодуючими структурами Адамара.
3. Створити закодоване зображення базуючись на кольорі пікселя секретного зображення та зображенні-ключі.
4. Повторювати крок 3 для кожного пікселя секретного зображення до отримання шифрованого зображення.
5. Після накладання закодованого зображення на зображення-ключ, секретне зображення може бути розшифроване людським зором.

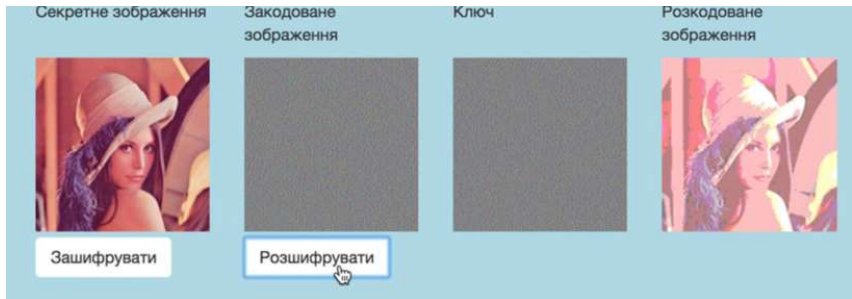


Рис. 4. Веб-застосунок для кодування та декодування кольорових зображень.

Даний метод шифрування інформації є ефективним способом протидії несанкціонованому викраденню інформації кіберзлочинцями, в даній роботі біло виконано наступні завдання:

1. Розроблено загальний алгоритм кодування кольорового зображення шляхом глобальної заміни зображення впорядкованою неперіодичною структурою Адамара, що забезпечує високу однорідність і візуальну нерозрізнимість кодованих зображень.

2. Вдосконалено алгоритм шифрування та використано RGB колірну модель для шифрування.

3. Розроблено веб-застосунок для шифрування кольорових зображень на базі мови JavaScript.

Список бібліографічних посилань

1. Дідух Л. А., Шовгенюк М. В., Писанчин Н. С. Комп'ютерні методи обробки зображень для сучасних технологій захисту цінних паперів. *Комп'ютерні технології друкарства*. 2006. № 15. С. 175-187.

2. Дідух Л. А., Шовгенюк М. В. Класи подібних матриць Адамара. *Комп'ютерні технології друкарства*. 2010. № 22. С. 54-64.

3. Christopher Swenson. *Modern Cryptanalysis: Techniques for Advanced Code Breaking* // Indianapolis, Wiley, 2008. 264 p.

4. Гантмахер Ф. Р. Теория матриц (вид. друге). Москва : Наука, 1967. 576 с.

5. Haralambos Evangelaras, Applications of Hadamard matrices. *Journal of Telecommunications and Information Technology*. 2003. P. 3-10.

Одержано 31.10.2018