

---

УДК 004.056.55

В.Г. Красиленко, С.К. Грабовляк

*Вінницький соціально-економічний інститут у-ту «Україна», Вінниця*

**МАТРИЧНІ АФІННІ ШИФРИ ДЛЯ СТВОРЕННЯ ЦИФРОВИХ СЛІПИХ ПІДПИСІВ  
НА ТЕКСТОГРАФІЧНІ ДОКУМЕНТИ**

**Вступ.** Використання комп'ютерних мереж стали причиною бурхливого розвитку криптографії. Існує багато криптографічних алгоритмів та протоколів [1, 2], які орієнтовані на послідовну обробку

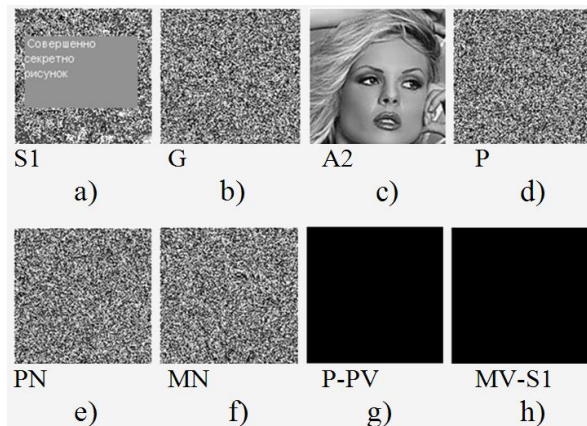
скалярних цифрових даних.

**Аналіз останніх досліджень, публікацій.** Для забезпечення більшої стійкості, порівняно з скалярними криптоперетвореннями, у роботах [3, 4] запропоновано модифіковані матричні алгоритми (МА) криптоперетворень 2-D масивів і зображень. Відомі також результати моделювання модифікованого МА створення 2-D ключа на основі протоколу Діффі-Хелмана [5].

**Постановка задачі.** Тому метою даної роботи є демонстрація можливостей застосування матричних афінних шифрів (МАШ) для створення сліпого цифрового підпису (СЦП) для даних, що представлені у вигляді зображень.

**Теоретичні основи та результати.** Процес шифрування та дешифрування для матричного повідомлення  $M$  та криптограми  $S$  може бути виражений такими матричними формулами [4]:  $S = (M \odot A + S) \bmod N$ ;  $M = (S \odot AD + SD) \bmod N$ , де  $A$  та  $S$  – два ключі шифрування у вигляді матриць,  $AD$  та  $SD$  – ключі дешифрування,  $N$  – матриця, всі елементи якої дорівнюють числу  $n$  (просте велике число), а компоненти всіх матриць вибираються з діапазону  $1 \div (n - 1)$ , крім того, символами  $\odot$  та  $+$  позначені операції поелементного множення та додавання матриць за модулем. Специфіка зображень та кодування яскравості напівтонового зображення чи основної кольорової складової ( $R, G, B$ ) байтом

дозволяє шляхом додавання фону ( $+ 1$  градація) перетворити діапазон значень елементів матриці  $M$  в діапазон  $1 \div 256$ , при цьому  $n = 257$  (просте число). Для моделювання процесу створення СЦП на базі МАШ ми використовували вхідне зображення  $S1$  (рис. 1, а), ключ  $G$  (рис. 1, б) шифрування (власником  $M$ , що є  $S1$  з фоном), ключ  $A$  (рис. 1, с) шифрування нотаріусом. Для дешифрування нотаріус використовує поелементно обернену за модулем матрицю-ключ  $OA$ , а власник має ключ  $OG$  дешифрування, взаємопов'язаний з ключем  $G$ . Процес створення СЦП передбачає такі кроки: 1) власник закриває повідомлення  $M$  шифруючи ключем  $G$  і створене зображення  $P$  (рис. 1d) пересилає нотаріусу  $A$ ; 2) нотаріус своїм ключем  $A$  шифрує отримане закрите повідомлення  $P$  і утворює зображення  $PN$  (рис. 1, е) і цей підписаний ним документ відсилає власнику; 3) власник, використовуючи ключ  $OG$  отримує підписаний в розшифрованому вигляді документ  $MN$  (рис. 1, ф). Для верифікації підпису, використовуючи ключ  $OA$ , нотаріус може отримати повідомлення  $PV$ , яке порівнюється з отриманим закритим повідомленням  $P$ , а відкритий власником підписаний документ  $MN$  ключем  $OA$  дозволяє отримати верифікаційне зображення  $MV$ , тобто вхідне зображення  $S1$ . Для повної верифікації потрібні спільні дії як власника документа  $M$  так і нотаріуса.



$$M := S1 + R \quad D := G \quad A = A2 + R$$

$$P_{i,j} := \text{mod}\{M_{i,j} \cdot G_{i,j}, 257\} - 1$$

$$PN_{i,j} := \text{mod}\{[P_{i,j} + 1] \cdot A_{i,j}, 257\} - 1$$

$$PV_{i,j} := \text{mod}\{[PN_{i,j} + 1] \cdot OA_{i,j}, 257\} - 1$$

$$\max(PV - P) = 0$$

$$MN_{i,j} := \text{mod}\{[PN_{i,j} + 1] \cdot OG_{i,j}, 257\} - 1$$

$$MV_{i,j} := \text{mod}\{[MN_{i,j} + 1] \cdot OA_{i,j}, 257\} - 1$$

$$\max(MV - S1) = 0$$

Рис. 1. Формули СЦП на базі МАШ та результати моделювання

На рис. 1, g і 1, h показані різниці зображень, що підтверджують співпадання зображень, що порівнюються.

**Висновок.** Таким чином, нами розроблено матричну модель сліпого підпису на основі МАШ та продемонстровано її дію та правильність функціонування результатами моделювання в MathCad. Результати моделювання підписування сліпим підписом кольорових зображень та інші будуть показані під час презентації.

### Список літератури

1. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.
2. Хорошко В.О. Методи та засоби захисту інфор-

мації: навч. посібник / В.О Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

3. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка». «Комп'ютерні системи та мережі». – 2009. – № 658. – С. 59-63.

4. Красиленко В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В.Г. Красиленко, К. Огородник, Ю. Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. наук.-пр. конф. – К., 2010. – С.120-124.

5. Красиленко В.Г. Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях / В.Г. Красиленко, О.І. Нікольський, О.О. Лазарев // Науково-методичний збірник науково-практичної конференції «Наука і навчальний процес». – Вінниця, 2008. – С.107-109.