УДК 004.056.55

В.Г. Красиленко, С.К. Грабовляк

Вінницький соціально-економічний інститут університету «Україна», Вінниця

МАТРИЧНІ АФІННІ ШИФРИ ДЛЯ СТВОРЕННЯ ЦИФРОВИХ СЛІПИХ ПІДПИСІВ НА ТЕКСТОГРАФІЧНІ ДОКУМЕНТИ

У статті розглядається процес створення сліпого цифрового підпису на текстографічні документи представлені у вигляді багатоградаційних зображень на основі матричних афінних шифрів. Запропоновано матричний алгоритм створення підпису, розроблено математичні моделі та матричні формули для криптографічних перетворень, включаючи шифрування і дешифрування. Розроблено процедури і програми генерування матричних ключів шифрування і дешифрування, а також продемонстровані результати моделювання алгоритму сліпого цифрового підпису на конкретних зображеннях розмірністю 704X572 пікселя в програмному середовищі MathCad.

Ключові слова: *криптографія, матричний афінний шифр, сліпий цифровий підпис, шифрування, дешифрування, зображення.*

Вступ

Постановка проблеми. Використання комп'ютерних мереж, по яких передають великі обсяги інформації державного, військового, комерційного та приватного змісту, що не допускають можливості доступу до неї сторонніх осіб, та поява потужних обчислювальних засобів стали причиною бурхливого розвитку криптографії. Існує багато криптографічних алгоритмів та протоколів, що використовуються для захисту інформації [1, 2], але більшість з них орієнтовані на послідовну обробку скалярних цифрових даних. В той же час з'являється все більше і більше задач, в яких необхідно виконувати криптографічні перетворення над багатовимірними сигналами, серед яких особливе місце займають двовимірні масиви та зображення, включаючи багатоградаційні та кольорові. Це і біометричні системи, в яких необхідно обробляти та зберігати велику кількість різноманітних зображень, наприклад, відбитки пальців, зображення рухомих об'єктів, обличчя, райдужної сітківки ока тощо. Вся ця інформація часто є конфіденційною, а тому є гостра необхідність в її криптографічному перетворенні з метою захисту від несанкціонованого доступу.

Аналіз останніх досліджень і публікацій. З метою забезпечення більшої стійкості у порівнянні з скалярними криптографічними перетвореннями та протоколами у роботах [3, 4] було запропоновано модифіковані матричні алгоритми криптографічних перетворень 2-D масивів і зображень, що базуються на модифікації відомих афінних шифрів [1]. Відомі також результати моделювання модифікованого алгоритму створення 2-D ключа, в основу якого покладено математичні моделі та протокол Діффі-Хелмана [5]. Результати моделювання багатоградаційних та кольорових зображень на основі запропонованих матричних алгоритмів та моделей, що наведені в цих роботах, показують їх суттєві переваги порівняно з традиційним афінним асиметричним шифром. Здійснення електронних комерційних платежів та юридично значущих дій не можливо без цифрових електронних підписів, серед яких можна виділити відомі цифрові підписи Ель-Гамаля, Шнорра, DSA, на базі алгоритму RSA, незаперечні, сліпі та інші підписи [1].

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

Виклад основного матеріалу

Процес шифрування та дешифрування для матричного повідомлення **M** та криптограми **C** може бути виражений такими матричними формулами [4]:

$$\mathbf{C} = \left(\mathbf{M} \underset{N}{\otimes} \mathbf{A} \underset{N}{+} \mathbf{S} \right); \quad \mathbf{M} = \left(\mathbf{C} \underset{N}{\otimes} \mathbf{AD} \underset{N}{+} \mathbf{SD} \right),$$

де **A** та **S** – два ключі шифрування у вигляді матриць, **AD** та **SD** – ключі дешифрування, причому **AD** – відповідно мультиплікативна складова афінного шифру, а **SD** – адитивна складова, **N** – матриця, всі елементи якої дорівнюють числу n (просте велике число), а компоненти всіх матриць вибираються з діапазону 1÷(n–1), крім того, символами $\underset{N}{\otimes}$ та $\underset{N}{+}$ позначені відповідно поелементні множення та додавання матриць за модулем . Специфіка зображень та кодування яскравості напівтонового зображення чи однієї кольорової складової (R, G, B) байтом дозволяє шляхом додавання фону (+ 1 градація) перетворити діапазон значень елементів матриці **N** в

діапазон 1÷256, при цьому n = 257 (просте число).

Для генерування сліпих цифрових підписів підходить не лише алгоритм RSA [1], а також і матричний афінний шифр, з використанням або лише мультиплікативної складової або обох – і мультиплікативної і адитивної. В даній роботі ми розглянемо лише з мультиплікативною складовою.

Для моделювання процесу створення сліпого підпису на базі матричного афінного шифру ми використовували вхідне зображення S1 (вже підписане нотаріусом), що показано на рис. 1, a, але для відтворення кроків цього процесу ми формуємо початкове зображення SDI (рис. 1, d – документ, що потрібно підписати) ключ **G** для шифрування цього документа власником V та відповідний йому ключ дешифрування **OG**. Нотаріус W використовує свій підпис з печаткою (відповідно зображення ND або ND2-рис. 1f, g). В моделюванні ми використовували підпис ND. Для закриття свого підпису нотаріус W використовує матричний ключ **A** та відповідно до нього створює матричний ключ дешифрування – **OA**.

Для того, щоб зробити сліпий цифровий підпис потрібно здійснити такі кроки:

1) власник V генерує випадкове зображення GV1 (рис. 1, b), де піксель має випадкове значення яскравості, зміщує його на +1, додаючи одиничну матрицю $\mathbf{R}_{i,j}$, і таким чином отримує ключ шифрування **G** та взаємопов'язаний з ним ключ дешифрування **OG** елементи якого визначаються як обернені за модулем до елементів матриці **G**. Рис. 2 показує, що при зміщенні всі елементи відповідних матриць будуть мати обернені значення;

2) для зазначення місця підпису, власник формує з SDI зображення SD, виділяючи область для підпису (на рис. 1, e – темна полоса), робить зміщення додаючи матрицю **R**, в результаті чого отримує матрицю **MD**, яка відповідає вимогам для шифрування

$$\mathbf{MD} = \mathbf{SD} + \mathbf{R} ;$$

3) власник V закриває матрицю **MD** ключем G (ключ відповідає зображенню GV1 і за формулою

$$\mathbf{OMD} = \mathbf{MD} \underset{N}{\otimes} \mathbf{G}$$

закриває текстографічний документ у вигляді зображення OMD1 (матриця **OMD1 – R**) (рис. 1, h);

4) нотаріус W свій підпис у вигляді зображення ND (рис. 1, f) та відповідну йому матрицю **NP**, отриману зміщенням, закриває свої матричним ключем **A** (відповідне йому зображення A1 – рис. 1, c) свій підпис і формує матрицю **NPG**, якій відповідає зображення NPG1 (рис. 1, i);

5) отримавши від власника V OMD1, яке є закритим текстографічним документом, нотаріус W створює цифровий підпис у вигляді матриці **SS**:

$$\mathbf{SS} = \mathbf{OMD} \underset{N}{\otimes} \mathbf{SS}$$

(зображення SS1) (рис. 1, j) і відсилає цей підписаний ним документ у цифровому форматі власнику V;

6) власник V використовує цей підпис, а при нагоді він може відкрити, використовуючи ключ **OG**, підписаний документ і отримати відкритий підписаний документ у вигляді зображення SSN1 (рис. 1, k) за формулою:

$$\mathbf{SSN} = \mathbf{SS} \underset{N}{\otimes} \mathbf{OG} .$$

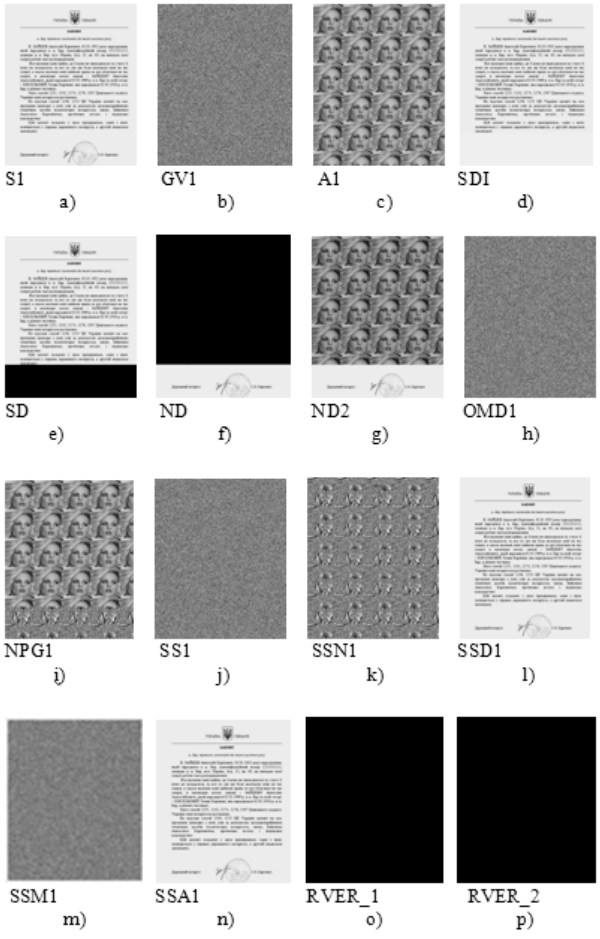

Рис. 1. Результати моделювання сліпого цифрового підпису на базі матричного афінного шифру

Для верифікації підпису зображення документа SSN1 (відповідно матриця **SSN**) розкривається оприлюдненим для верифікації ключем **OA** нотаріуса і отримується матриця **SSD**,

$$\mathbf{SSD} = \mathbf{SSN} \underset{N}{\otimes} \mathbf{OA} ,$$

або відповідне їй зображення SSD1 (рис. 1, l), яке свідчить, що саме той документ і саме тим підписом саме того нотаріуса він був підписаний.

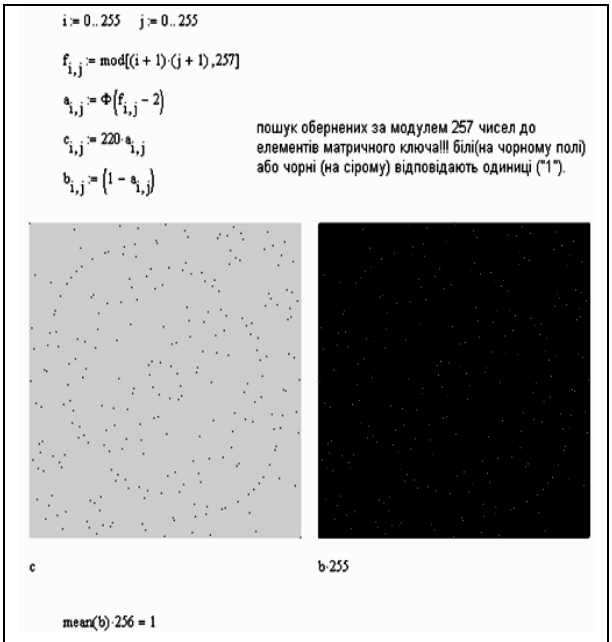

Рис. 2. Модель обернених чисел за mod 257

Якщо сліпий цифровий підпис у вигляді матриці **SS** розкриває ключем **OA** спочатку нотаріус W за формулою:

$$\mathbf{SSM} = \mathbf{SS} \underset{N}{\otimes} \mathbf{OA}$$

і отримує зображення SSM1 (рис. 1, m), то при наявності ключа дешифрування **OG** з матриці **SSM** формується аналогічним чином матриця **SSA** або відповідне їй зображення SSA1 (рис. 1, n)

В результаті спільних дій власника V документа, що підписується, та нотаріуса W можна отримати однакові зображення SSD1 та SSA1, які свідчать про те, що сліпий цифровий підпис створений саме цим нотаріусом на цьому конкретному документі. Різницеві зображення RVER_1 і RVER_2 (рис. 1, o, p) підтверджують правильну роботу запропонованого сліпого цифрового підпису на базі матричного афінного шифру.

Для моделювання сліпого цифрового підпису в середовищі MathCad нами використовувались зображення розмірністю 704X572 пікселя. Формули та інтерфейсні вікна з MathCad зображені на рис. 3, 4 в стисненому варіанті, оскільки формули та отримані шляхом моделювання всі необхідні початкові, проміжні та кінцеві результати у вигляді зображень, що показані на рис. 1, підтверджують правильну роботу запропонованого алгоритму. Час виконання всіх процедур і кроків при використанні раніше згенерованих ключів не перевищує хвилини.

Для оцінювання якості закриття документів при їх шифруванні нами розроблена підпрограма в MathCad, яка дозволяє обчислити середню ентропію на 1 піксель конкретних зображень. Деякі фрагменти показані на рис. 5.

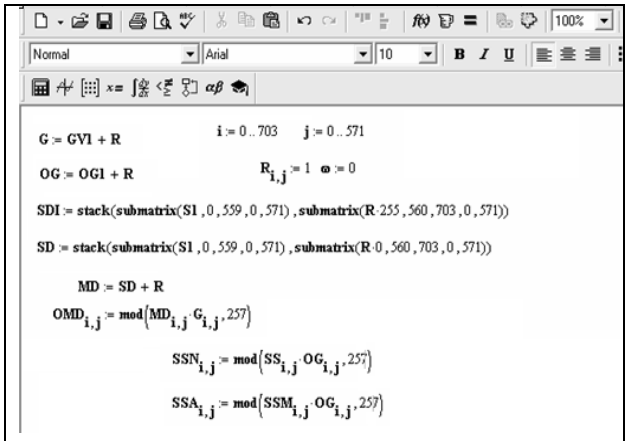

Рис. 3. Формули для обрахунку власником V

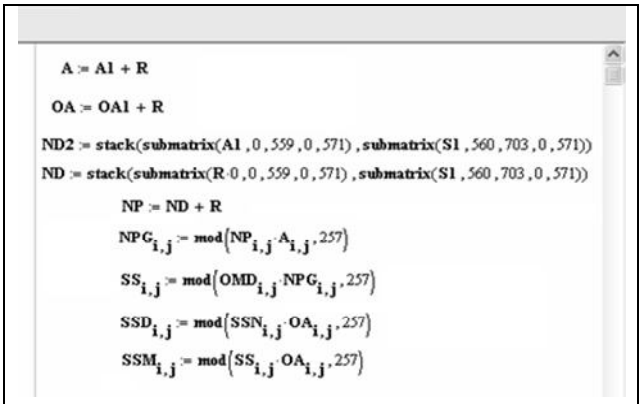

Рис. 4. Формули для обрахунку нотаріусом W

На цьому рисунку показані результати обробки зображень розмірністю 128X128, що використовуються як другий варіант презентації запропонованого сліпого цифрового підпису (тези доповіді).

Як видно з гістограмних розподілів ентропія початкового текстографічного документа SD є 3,447; для ND є 2,647, а ентропія зображення, що відповідає цифровому підпису SS є 7,96, тобто є дуже близькою до максимально можливої 8. Проміжні зображення, що відповідають проміжним матрицям SSA при верифікації мають відповідну ентропію рівну 5,057. Чим більша ентропія сліпого цифрового підпису, тим більша міра невизначеності відповідного зображення і тим складніше провести атаку на даний алгоритм.

Висновки

Запропоновано матричний алгоритм створення підпису, розроблено математичні моделі та матричні формули для криптографічних перетворень, включаючи шифрування і дешифрування. Розроблено процедури і програми генерування матричних ключів шифрування і дешифрування, а також продемонстровані результати моделювання алгоритму сліпого цифрового підпису на конкретних зображеннях розмірністю 704X572 пікселя в програмному середовищі MathCad.

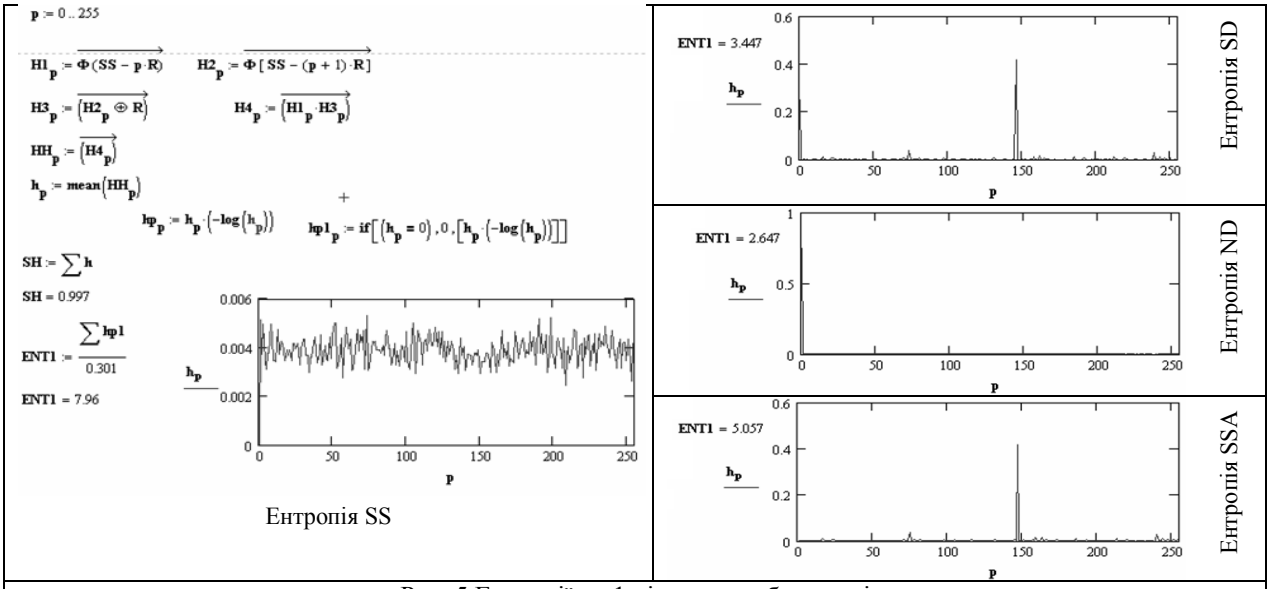

Рис. 5 Ентропії на 1 піксель в зображенні

Таким чином, нами розроблено матричну модель сліпого підпису на основі матричних афінних шифрів та продемонстровано її дію та правильність функціонування результатами моделювання в MathCad.

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 інформації: 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. Лазарєв // Наука і навчальний процес: науково-метод. збірник науково-практ. онф. – Вінниця, 2008. – С.107-109.

Надійшла до редколегії 3.10.2011

Рецензент: д-р техн. наук, проф. В.М. Лисогор, Вінницький соціально-економічний інститут Університету «Україна», Вінниця.

МАТРИЧНЫЕ АФФИННЫЕ ШИФРЫ ДЛЯ СОЗДАНИЯ ЦИФРОВЫХ СЛЕПЫХ ПОДПИСЕЙ НА ТЕКСТОГРАФИЧЕСКИЕ ДОКУМЕНТЫ

В.Г. Красиленко, С.К. Грабовляк

В статье рассматривается процесс создания слепой цифровой подписи на текстографические документы представленные многоградационными изображениями на основе матричных аффинных шифров. Предложен матричный алгоритм создания подписи, разработаны математические модели и матричные формулы для криптографических преобразований включая шифрование и дешифрование. Разработаны процедуры и программы генерирования матричных ключей шифрования и дешифрования и продемонстрированные результаты моделирования алгоритмов слепой цифровой подписи на конкретных изображениях размерностью 704X572 пикселя в программной среде MathCad.

Ключевые слова: *криптография, матричный аффинный шифр, слепая цифровая подпись, шифрование, дешифрование, изображение.*

MATRIX AFFINE CODES FOR CREATION OF DIGITAL BLIND SIGNATURES ON TEXT-GRAPHIC DOCUMENTS

V.G. Krasilenko, S.K. Grabovlyak

The article describes how to create a blind signature on the documents submitted text-graphic lot graded images based on the matrix affine ciphers. We propose a matrix algorithm for creating signatures, mathematical models and formulas for the matrix transformations including cryptographic encryption and decryption. The procedures and programs generating matrix of keys and the encryption and decryption algorithms for the simulation results demonstrated a blind signature on the specific dimension of the images 704X572 pixel in the software environment MathCad

Keywords: *cryptography, matrix affine code, blind digital signature, enciphering, desenciphering, image.*