УДК 004.056.55

І.О. РОЗЛОМІЙ, Г.В. КОСЕНЮК
Черкаський національний університет імені Богдана Хмельницького

СПОСІБ ФОРМУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ ДЛЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА ОСНОВІ ОПЕРАЦІЙ МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

В сучасному середовищі документована інформація, представлена в цифровій формі, має велике значення, рівно як і проблема її захисту від підробки, неконтрольованого поширення, знищення. Багато методів розроблено для захисту інформації, проте жоден з них не гарантує повної ефективності. Відсутність надійних засобів захисту електронних документів є основою для пошуку нових рішень, серед яких є комп'ютерна стеганографія. Стаття присвячена розгляду системи накладання цифрового водяного знаку. В статті запропонований спосіб формування цифрового водяного знаку для електронних документів, який ґрунтується на операціях матричного криптографічного перетворення. Використання розробленого алгоритму забезпечить достовірність електронного документу. Також даний алгоритм може бути використаний в комплексному методі захисту електронних документів разом з електронним цифровим підписом.

Ключові слова: електронний документ, стеганографія, цифровий водяний знак, інверсія бітів, матричні перетворення.

I.O. ROZLOMII, G.V. KOSENYUK
Cherkassy Bogdan Khmelnytsky National University

METHOD OF FORMING A DIGITAL WATERMARK FOR ELECTRONIC DOCUMENTS BASED ON OPERATIONS OF MATRIX CRYPTOGRAPHIC TRANSFORMATION

In a modern environment the documented information is presented in a digital form matters very much exactly, as well as problem of her protecting from an imitation, out-of-control distribution, elimination. Many methods are worked out for protection of information, however none of them guarantees complete efficiency. Absence of reliable facilities of defence of electronic documents is basis for the search of new decisions among that there is computer steganography. The article is sanctified to consideration of the system of imposition of digital watermark. In the article the offered method of forming of digital watermark for electronic documents based on operations of matrix cryptographic transformation. The use of the worked out algorithm will provide authenticity of electronic document. Also this algorithm can be used in the complex method of defence of electronic documents together with electronic digital signature.

Keywords: electronic document, steganography, digital watermark, inversion of bits, matrix transformation.

Вступ. Одним з напрямків захисту електронних документів, при збереженні, передачі комп'ютерною мережею є цифрова стеганографія [1]. Стеганографія в інформаційних системах зв'язку недостатньо розвинений напрямок, а існуючі методи мало пристосовані до завдань захисту електронних документів. Це пов'язано з властивими їй такими недоліками, як невисока надійність і стійкість. Проте, разом з цим, застосування стеганографічних систем в області електронного документообігу дозволить вирішити ряд важливих завдань. Серед яких варто відмітити забезпечення прихованого збереження і передачі електронного документу, зробити непомітними комунікації між відправником та отримувачем повідомлень, виявлення каналів витоку ЕД, а також внесення прихованого електронного цифрового підпису [2, 3]. Однак, в деяких випадках використання цифрового підпису для забезпечення інформаційної безпеки документів є недостатнім. Для підвищення надійності захисту ЕД від можливих порушень цілісності доречно вжити додаткового рівня захисту, наприклад, використанням засобів стеганографії.

Одним з механізмів стеганографії є цифровий водяний знак (ЦВЗ) [4]. Вбудовування в електронний документ невидимих міток, в якості яких можуть виступати послідовності символів чи графічні зображення є одним з розповсюджених способів захисту документів від підробки. Широке впровадження ЦВЗ для захисту авторських прав ЕД призводить до необхідності розробки методів побудови ЦВЗ, більш стійких до різного роду атак. Інформація, яку містять ЕД вразлива до неправомірних модифікацій: редагування, видалення фрагментів ЕД. Тому, розробка алгоритму побудови ЦВЗ для електронних документів є актуальною задачею.

Постановка проблеми. До цього відомі методи вбудовування ЦВЗ не можуть в повній мірі вирішити завдання захисту ЕД від фальсифікацій. Більшість розроблених на сьогодні методів побудови ЦВЗ, які можуть бути використані для задач захисту документів побудовані на основі методу LSB. Проте, для більшості з них характерна вразливість, низька стеганографічна стійкість. Враховуючи недоліки попередніх методів вбудовування ЦВЗ, можна запропонувати алгоритм побудови ЦВЗ, який базується на операціях матричного криптографічного перетворення.

Аналіз останніх досліджень та публікацій. Пошуком ефективних стеганографічних методів захисту інформації займалася велика кількість вчених, серед яких можна виділити: Д.В. Очнев, Е.С. Чиркін, Ю.А. Белобокова, А.В. Балакін, А.С. Єлисеєв, В.М. Зажома та інші. Щодо питань забезпечення достовірності електронних документів варто відмітити працю Д.А. Сагайдака та Р.Т. Файзуліна, в якій висунуто спосіб формування цифрового водяного знаку для фізичних та електронних документів [5]. Проте, ще залишаються питання, які потребують подальшого доопрацювання та вивчення.

Формулювання цілей статті. Метою роботи є розробка алгоритму побудови цифрового водяного знаку на основі використання операцій матричного криптографічного перетворення.

Виклад основного матеріалу. Зазвичай, в документованій інформації з метою захисту авторських прав використовуються цифрові водяні знаки – цифрові мітки, які впроваджуються в електронний документ за допомогою спеціальних стеганографічних перетворень [6]. Для побудови системи ЦВЗ до цього часу не використовувалися операції матричного криптографічного перетворення. Алгоритм накладання цифрового водяного знаку з використанням матричних перетворень можна описати такими кроками:

1) спочатку необхідно визначити проміжок числових значень, над якими буде здійснюватися матричне криптографічне перетворення;

2) ввести матрицю, на основі якої здійснюватиметься перетворення значень з проміжку;

3) визначити параметр інверсії;

4) обчислити результат матричного криптографічного перетворення вказаного числового значення;

5) на основі отриманого результату визначити байти інформації, в яких будуть інвертуватися біти;

6) збільшити значення лічильника, перейти до наступного значення з числового проміжку;

7) повторювати матричне криптографічне перетворення значень до кінця заданого числового проміжку;

8) цифровий водяний знак вбудований в ЕД.

Процес вбудовування цифрового водяного знаку в електронний документ може бути описаний наступним алгоритмом, рис. 1.

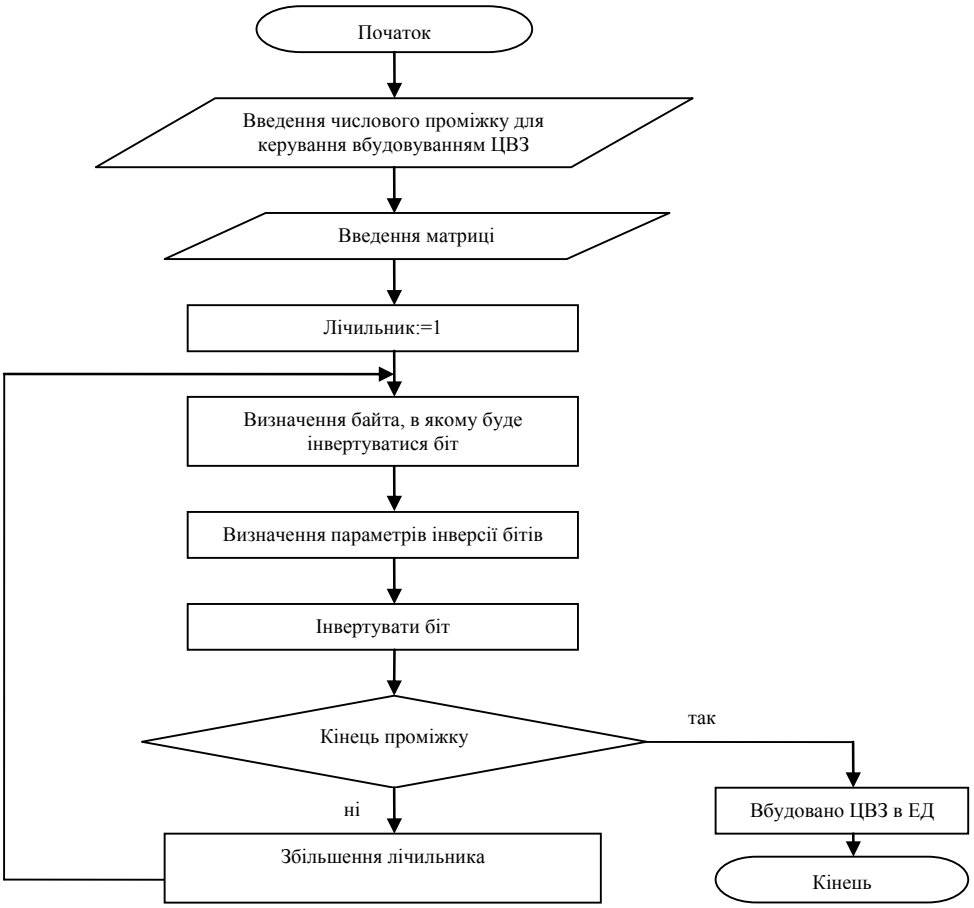

Рис. 1. Алгоритм накладання цифрового водяного знаку на електронний документ на основі матричних криптографічних перетворень

Розглянемо приклад матричного перетворення числових значень з заданого проміжку.

Нехай, заданий числовий проміжок від 15 до 19. Спочатку матричне криптографічне перетворення здійснюється над числом 15. Якщо операція матричного криптографічного прямого перетворення задана матрицею $\vec{F}_k = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$, для знаходження результату перетворення паролю, наприклад,

$15_{dec} = 00001111_{bin}$ необхідно підставити значення відповідних інформаційних бітів в систему рівнянь

$$F = \begin{cases} x_1 \oplus x_6 \oplus x_8 = y_1 \\ x_3 \oplus x_7 = y_2 \\ x_4 \oplus x_6 = y_3 \\ x_1 \oplus x_3 \oplus x_7 = y_4 \\ x_1 \oplus x_2 \oplus x_8 = y_5 \\ x_1 \oplus x_3 \oplus x_4 = y_6 \\ x_2 \oplus x_5 \oplus x_8 = y_7 \\ x_4 \oplus x_5 \oplus x_7 = y_8 \end{cases},$$

де $x_1,...,x_8$ – вихідний байт, $y_1,...,y_8$ – байт, отриманий в результаті матричного перетворення.

Підставивши відповідні значення отримаємо: $F = \begin{cases} x_1 \oplus x_6 \oplus x_8 \\ x_3 \oplus x_7 \\ x_4 \oplus x_6 \\ x_1 \oplus x_3 \oplus x_7 \\ x_1 \oplus x_2 \oplus x_8 \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_5 \oplus x_8 \\ x_4 \oplus x_5 \oplus x_7 \end{cases} = \begin{cases} y_1 = 0 \\ y_2 = 1 \\ y_3 = 1 \\ y_4 = 1 \\ y_5 = 1 \\ y_6 = 0 \\ y_7 = 0 \\ y_8 = 0 \end{cases}$.

Відповідно результатом перетворення буде значення $01111000_{bin} = 120_{dec}$. Аналогічним способом виконаємо матричні перетворення над кожним значенням з заданого проміжку, як показано в табл. 1.

Таблиця 1

Обчислення порядкових номерів байтів ЕД, де будуть інвертуватися біти

Операція матричного криптографічного перетворення значень 16-19	
$16_{dec} = 00010000_{bin}$ $F = \begin{cases} x_1 \oplus x_6 \oplus x_8 \\ x_3 \oplus x_7 \\ x_4 \oplus x_6 \\ x_1 \oplus x_3 \oplus x_7 \\ x_1 \oplus x_2 \oplus x_8 \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_5 \oplus x_8 \\ x_4 \oplus x_5 \oplus x_7 \end{cases} = \begin{cases} y_1 = 0 \\ y_2 = 0 \\ y_3 = 1 \\ y_4 = 0 \\ y_5 = 0 \\ y_6 = 1 \\ y_7 = 0 \\ y_8 = 1 \end{cases}$ Результат: $00100101_{bin} = 37_{dec}$	$17_{dec} = 00010001_{bin}$ $F = \begin{cases} x_1 \oplus x_6 \oplus x_8 \\ x_3 \oplus x_7 \\ x_4 \oplus x_6 \\ x_1 \oplus x_3 \oplus x_7 \\ x_1 \oplus x_2 \oplus x_8 \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_5 \oplus x_8 \\ x_4 \oplus x_5 \oplus x_7 \end{cases} = \begin{cases} y_1 = 1 \\ y_2 = 0 \\ y_3 = 1 \\ y_4 = 0 \\ y_5 = 1 \\ y_6 = 1 \\ y_7 = 1 \\ y_8 = 1 \end{cases}$ Результат: $10101111_{bin} = 175_{dec}$
$18_{dec} = 00010010_{bin}$ $F = \begin{cases} x_1 \oplus x_6 \oplus x_8 \\ x_3 \oplus x_7 \\ x_4 \oplus x_6 \\ x_1 \oplus x_3 \oplus x_7 \\ x_1 \oplus x_2 \oplus x_8 \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_5 \oplus x_8 \\ x_4 \oplus x_5 \oplus x_7 \end{cases} = \begin{cases} y_1 = 0 \\ y_2 = 1 \\ y_3 = 1 \\ y_4 = 1 \\ y_5 = 0 \\ y_6 = 1 \\ y_7 = 0 \\ y_8 = 0 \end{cases}$ Результат: $01110100_{bin} = 116_{dec}$	$19_{dec} = 00010011_{bin}$ $F = \begin{cases} x_1 \oplus x_6 \oplus x_8 \\ x_3 \oplus x_7 \\ x_4 \oplus x_6 \\ x_1 \oplus x_3 \oplus x_7 \\ x_1 \oplus x_2 \oplus x_8 \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_5 \oplus x_8 \\ x_4 \oplus x_5 \oplus x_7 \end{cases} = \begin{cases} y_1 = 1 \\ y_2 = 1 \\ y_3 = 1 \\ y_4 = 1 \\ y_5 = 1 \\ y_6 = 1 \\ y_7 = 1 \\ y_8 = 0 \end{cases}$ Результат: $11111110_{bin} = 255_{dec}$

Отримані в результаті перетворення значення вкажуть на байт інформації електронного документа, в якому будуть інвертуватися біти. Згідно з обчисленнями, в байтах 37, 116, 120, 175, 254 будуть інвертуватися біти, рис. 2.

Електронний документ (байти інформації)										
1	2	…	…	…	…	…	…	…	…	…
…	…	…	37	…	…	…	…	…	…	…
…	…	…	…	…	116	…	…	…	…	120
…	…	…	…	…	…	…	175	…	…	…
…	…	…	…	…	…	…	…	…	254	255

Рис. 2. Значення байтів електронного документу, де виконуватиметься інверсія бітів

Інверсія може виконуватися над будь-яким бітом в байті чи кількома одразу. Найпростіший спосіб інвертувати молодший біт у байті, але для того щоб ускладнити завдання вибору параметру інверсії можна використати матричне криптографічне перетворення. Тобто, за допомогою матриці перетворювати задане число, таким чином результат перетворення вказуватиме на порядковий номер біта в байті, який буде інвертуватися. Розглянемо приклад вибору параметру інверсії на основі матричного криптографічного перетворення заданого числа.

Нехай, операція прямого криптографічного перетворення задана матрицею $\vec{F}_k = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Припустимо, потрібно інвертувати один біт в байті. Відповідно необхідно за допомогою матриці перетворити будь-яке значення з проміжку від 1 до 8. Для перетворення числа $2_{dec} = 010_{bin}$, необхідно розв'язати систему рівнянь: $\vec{F}_k = \begin{cases} x_2 \oplus x_3 = y_1 \\ x_1 \oplus x_3 = y_2 \\ x_2 = y_3 \end{cases}$. Підставивши відповідні значення в систему, отримаємо

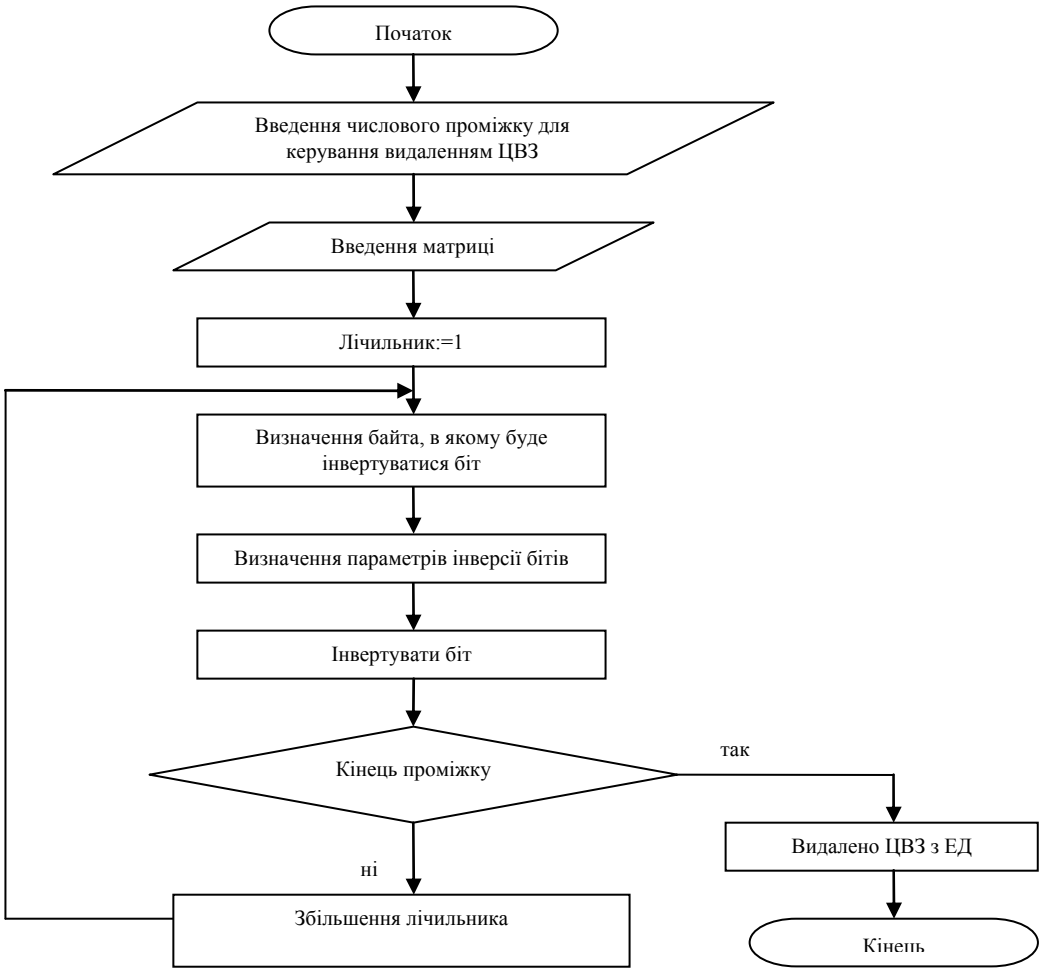

Рис. 3. Відновлення інформації в документі, видалення цифрового водяного знаку

$\vec{F}_k = \begin{cases} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \end{cases} = \begin{cases} y_1 = 1 \\ y_2 = 0 \\ y_3 = 1 \end{cases}$. Отриманий результат $101_{bin} = 5_{dec}$ вказує на те, що буде інвертуватися п'ятий біт в байті.

В результаті матричних криптографічних перетворень були знайдені байти, в яких відбулася інверсія бітів. Для того, щоб вилучити з ЦВЗ з електронного документу, тобто відновити інформацію в документі, необхідно виконати послідовність дій, аналогічну в процесі накладання ЦВЗ, як показано на рис. 3.

В результаті виконання алгоритму показаного на рис. 4, біти, які були інвертовані в процесі накладання ЦВЗ, повертають своє значення, документ набуває свого вихідного стану.

Висновки. В статті було розкрито питання захисту електронних документів засобами стеганографії, зокрема за допомогою цифрового водяного знаку. Таким чином, було запропоновано новий спосіб формування ЦВЗ для електронного документу на основі використання операцій матричного криптографічного перетворення. Алгоритм ґрунтується на матричному перетворенні числових значень з заданого проміжку, які вказують на порядкові номери байтів документу, в яких інвертуватимуться біти. Також показано, що за допомогою матричних перетворень можна визначити параметр інверсії. Сформовано послідовність кроків та структурну схему алгоритму. Запропонований алгоритм можна використовувати, як самостійно для забезпечення достовірності електронного документу, так і в комплексі з електронним цифровим підписом.

Література

1. Коханович Г.Ф. Компьютерная стеганография. Теория и практика / Коханович Г.Ф., Пузыренко А.Ю. – Киев : МК-Пресс, 2006. – 288 с.

2. Стеганография, цифровые водяные знаки и стегоанализ / Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. – М. : Вузовская книга, 2009. – 220 с.

3. Cox I.J. Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco : Morgan Kaufmann Publishing, 2008. – 624 p.

4. Балакин А.В. Использование стеганографических методов для защиты текстовой информации / А.В. Балакин, А.С. Елисеев // Спецвузавтоматика. Спецвыпуск. – 2009. – С. 183–184.

5. Сагайдак Д.А. Способ формирования цифрового водяного знака для физических и электронных документов / Д.А. Сагайдак, Р.Т. Файзуллин // Компьютерная оптика. – 2014. – № 1(38). – С. 94–104.

6. Очнев Д.В. Цифровые водяные знаки как метод защиты текстовых печатных документов / Д.В. Очнев, Е.С. Чиркин // Психолого-педагогический журнал Гаудеамус. – 2012. – № 2 (20). – С. 148–149.

References

1. Kokhanovich, G.F. and Pusyrenko, A.Y. (2006) Computer steganography. Theory and practice. Kiev: MK-Press, 288 p.

2. Agranovsky, A.V., Balakin, A.V., Gribunin, V.G. and Sapozhnikov, S.A. (2009) Steganography, digital watermarks and steganalysis. Moscow: University book, 220 p.

3. Cox, I., Miller, M., Bloom, J. and Fridrich, J. (2008) Digital watermarking and steganography. San Francisco: Morgan Kaufmann Publishing, 624 p.

4. Balakin, A.V and Yeliseyev, A.S. (2009) Using steganographic methods to protect text information. Spetsvuzavtomatika. Special issue, pp. 183–184.

5. Sagaidak, D.A. and Faizullin, R.T. (2014) Method for forming a digital watermark for physical and electronic documents. Computer optics, 1 (38), pp. 94–104.

6. Ochnev, D.V. and Chirkin, E.S. (2012) Digital watermarks as a method for protecting textual printed documents. Psychological and pedagogical journal Gaudeamus, 2 (20), pp. 148–149.

Рецензія/Peer review : 17.06.2017 р. Надрукована/Printed :13.09.2017 р.
Рецензент: д.т.н., проф. Рудницький В. М.