УДК 004.056.5

Б. В. Павленко

ПІДВИЩЕННЯ СТІЙКОСТІ МЕТОДУ ЗАБЕЗПЕЧЕННЯ АВТЕНТИЧНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ ДОКАЗОВОЇ БАЗИ СУДОВОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНИХ МОДИФІКАЦІЙ

Вінницький національний технічний університет

Анотація

Запропоновано вдосконалення методу забезпечення автентичності цифрових зображень доказової бази судової системи для підвищення стійкості від несанкціонованих модифікацій. Вдосконалення полягає у вдосконаленні стеганографічного методу щляхом використання трансформацій Арнольда та хаотичного кодування.

Ключові слова: інформація, захист інформації, доказова база, стеганографія.

Abstract

The report improving the method of providing authenticity of digital images of the evidence of the judiciary to increase stability against unauthorized modifications. The essence of perfection is using Arnold transformations and chaotic coding as modification of steganography method.

Keywords: information, information security, proof base (evidence), steganography.

Вступ

У слідчій і судовій практиці кримінального судочинства зустрічаються факти, коли процес доказування відбувається в умовах активної протидії встановленню об'єктивної істини у кримінальній справі з боку певного кола осіб, зацікавлених в бажаному для них результаті (уникнути відповідальності, залишити злочин нерозкритим т.д.) за рахунок знищення або підроблення доказів. Такі випадки найбільш характерні для досудового провадження, однак нерідко спостерігаються на інших стадіях кримінального процесу.

Оскільки цифрові зображення можуть відігравати роль основних доказів правопорушення, необхідно контролювати їх цілісність протягом усього часу їх зберігання.

Для вирішення задач перевірки автентичності файлів та їх цілісності використовується цифрові водяні знаки, хеш-функції. Одним з найрозповсюдженіших методів на сьогоднішній день є стеганографічні алгоритми накладання цифрових водяних знаків [1]. В цілому дані алгоритми широко застосовуються для вирішення наступних завдань:

– захисту конфіденційної інформації від несанкціонованого доступу;

– захисту авторського права на інтелектуальну власність;

– підтвердження автентичності файлу.

Найбільшої популярності здобули методи (алгоритми) цифрових водяних знаків, що використовують у якості контейнера зображення, оскільки даний контейнер є найбільш розповсюдженим у наш час. Наприклад одним із найбільш розповсюджених алгоритмів є стеганоалгоритми, які вбудовують інформацію в частотну область. Перевагами даного методу є стійкість до атак JPEG стисненням, обрізання країв, висока швидкодія, висока стійкість до частотного детектування, висока стійкість до руйнування молодших біт контейнера. Однак у методу є недоліки стійкості до атак зашумлення.

Тож, обрана тема є *актуальною* на сьогоднішній день, оскільки захист доказової бази судової системи, а саме цифрових зображень, як можливих основних доказів є важливою частиною комплексної системи захисту судової системи.

Результати дослідження

Запропонована система вбудовування ЦВЗ має дві основних частини: частина вбудовування та частина забезпечення надійності ЦВЗ. Під-система забезпечення надійності вбудовування ЦВЗ створена для покращення властивостей початкового методу Коха-Жао, а саме складності отримання цифрового водяного знаку навіть знаючи алгоритм вбудовування. Для цього буде використано хаотичний алгоритм шифрування та кодування Арнольда.

Хаотичний алгоритм шифрування є ефективним методом для шифрування даних. Хаотичні сигнали володіють якостями псевдовипадковості, незворотності і динамічної поведінки [3]. Системи, що мають хаотичний характер, мають високу чутливість до початкових параметрів. Вихідна хаотична послідовність схожа на білий шум, що має випадкову поведінку з покращеною кореляцією та складністю відтворення [34, 35]. і визначається так, як зазначено в формулі 1.

$$C_{n+1} = \mu \times C_n \times (1 - C_{n)} \quad (1)$$

Оскільки це пропонує спільну перевагу швидкості та безпеки, доведено, що використання хаотичного шифрування збільшує безпеку [63]. Безпека інформації може бути збільшена використовуючи різні методи шифрування, і один з ефективних методів – перетворення Арнольда [66-68]. Даний метод шифрування, є двомірним і добре працює у програмах для шифрування зображень типу N × N. Математична модель перетворення Арнольда представлена у формулі 2.

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (modN) \quad (2)$$

Результатами перетворення є зміна позицій пікселів для генерації зображення яке буде невпорядковане та буде відрізнятися від початкового. Результатом перетворення Арнольда є зашифроване зображення яке має відповідність один до одного з оригінальним зображенням. Псевдовипадковість перетворення Арнольда у результаті дає спотворене зображення, яке неможливо повернути до початкового стану без знання відповідної послідовності яка була використана[2]. Стійкість шифрування залежить від кількості ітерацій які можуть бути визначені окремо для кожного зображення при початку роботи алгоритму.

Для вбудовування ЦВЗ обирається блок 16x16 для вбудування 4 біт зашифрованого ЦВЗ як показано на рисунку 1.

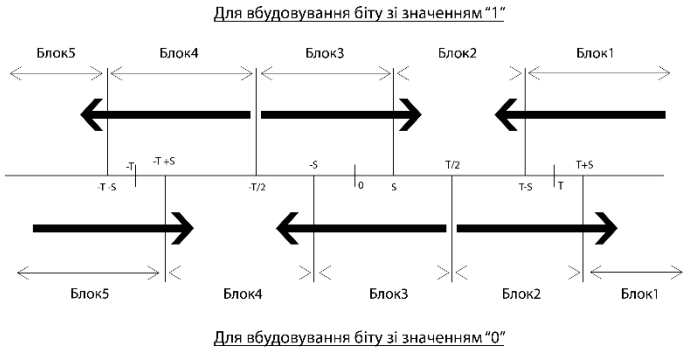

Рисунок 1 – Модифікації значень при вбудовуванні бітів 1 та 0

Для приховування біту зі значенням 1 відповідно до рисунка 1 обирається болк 2 або блок 5 відповідно до різниці між коефіцієнтами D до вбудовування. Якщо коефіцієнт D знаходиться в блоці 1 або 3, тоді коефіцієнти $C_{xy}(i,j)$ та $C_{xy+1}(k,l)$ модифікуються для того щоб увійти до блоку 2, яка є найближчою коректною зоною для вбудовування біту зі значенням 1. Якщо різниця між коефіцієнтами D належить до блоку 4, то коефіцієнти модифікуються так щоб різниця знаходилася у блоці 5. Виходячи з цього для вбудовування біту зі значенням 1 будуть використані блоки 2 та 5.

Для аналізу стеганографічних методів використовуються показники пікове відношення сигналу до шуму (PSNR), нормалізована крос-кореляція (NCC), відношення бітових помилок (BER), які

обчислюються за формулами:

$$BER = \frac{1}{mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} w_0(i,j) \oplus w_x(i,j)\right] \quad (3)$$

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w_0(i,j) w_x(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} [w_0(i,j)]^2} \quad (4)$$

Для оцінки якості зображення після вбудовування використовуються параметри SSIM та PSNR, як параметри які найкраще відображають зміни в початковому стеганоконтейнері. Модифікований метод в результаті вбудовування генерує високоякісні зображення, з високим рівнем PSNR від 39 до 47.7 децибел при тестуванні звичайних знімків, та від 40.6 до 51 децибел при використанні знімків документів. В таблиці 2.1 наведені значення метрик на еталонних зображеннях.

Таблиця 1– Результати тестування запропонованого алгоритму

Зображення	PSNR (db)	SSIM	BER (%)	NCC	Безпечність (в бітах)
Lena	46.31	0.9927	0	1	80
Pepper	46.30	0.9924	0.02	0.99	128
Plane	46.10	0.9920	0	1	192
Baboon	42.72	0.9940	0	1	256

Стійкість вдосконаленого є досить високою, оскільки виконується дотримання головної вимоги стеганографії – непомітності передавання інформації. Проведений тестування показало, що вбудовування інформації є більш стійким до модифікацій при використанні трансформації Арнольда та хаотичного кодування. Також було виконано реалізацію програмного додатку на основі вдосконаленого методу, а саме розроблено програму для вбудовування ЦВЗ у зображення. В програмі реалізовано функціонал до кожного з модулів, а саме: вибір зображення, вбудовування ЦВЗ та перевірка зображень на наявність модифікацій.

Висновки

Проаналізовано можливості вдосконалення методу забезпечення автентичності цифрових зображень доказової бази судової системи. Удосконалено стеганографічний метод Коха-Жао, а саме підвищено стійкість до несанкціонованих модифікацій за рахунок впровадження трансформацій Арнольда. Розроблено алгоритм та програмний засіб для реалізації вдосконаленого методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Владимир Федорович Шаньгин. – Москва: ДМК Пресс, 2013. – 593 с.

2. L. Wu, and J. Zhang, Arnold transformation algorithm and antiarnold transformation algorithm, in Proc ICISE, Nanjing, China, 2009, pp. 1164-1167.

3. A. Daneshgar, and B. Khadem, “A self-synchronized chaotic image encryption scheme,” Signal Processing Image Communication, vol. 36, pp. 106–114, Aug. 2015.

Павленко Богдан Володимирович – студент групи УБ-17м, факультет менеджменту, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: pavlenko.bohd@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** – канд.техн.наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Pavlenko Bohdan V. — student of group UB-17m, Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.

Supervisor: **Karpinets Vasyl V.** — Ph. D. Assistant professor, management and security of information Systems department; Vinnitsa, Ukraine;