УДК 004.056.5

М. О. Козіна[1]

МЕТОД ПЕРЕВІРКИ АВТЕНТИЧНОСТІ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ СТЕГАНОГРАФІЧНИМ КАНАЛОМ ЗВ'ЯЗКУ

[1]Одеський національний політехнічний університет

Запропоновано удосконалення стеганографічного методу, розробленого автором раніше, який не має аналогів серед сучасних стеганометодів, оскільки вирішує одночасно триєдину задачу: прихованої передачі даних (додаткової інформації), у якості яких виступає випадковим чином сформована бінарна послідовність, автентифікації та перевірки цілісності додаткової інформації. Як контейнер розглядається цифрове кольорове зображення. Наведено результати обчислювального експерименту, що підтверджують високу ефективність удосконаленого стеганометоду у разі виявлення порушень автентичності додаткової інформації.

Ключові слова: стеганографічний метод, цифрове зображення, дискретне перетворення Фур'є, автентичність.

Вступ

Зацікавленість наукової спільноти в стеганографії за декілька останніх десятиліть значно зросла. Для цього є багато причин, але одна з найголовніших — це широке розповсюдженням мультимедійних технологій у всіх сферах людського життя.

Інформаційні технології дали новий імпульс до розвитку та вдосконалення стеганографії, що привело до появи такого напряму у галузі захисту інформації, як комп'ютерна стеганографія.

Одною з причин широкого розповсюдження сьогодні наукових здобутків у сфері стеганографії є необхідність забезпечення надійного захисту інформації, яка має цифровий формат. Методи стеганографії не тільки дозволяють приховано зберігати та передавати інформацію, але і дуже вдало допомагають вирішувати питання захисту інформації від несанкціонованого копіювання, відстеження поширювання інформації у загальнодоступній мережі, пошуку даних в мультимедійних базах даних тощо.

Важливою та актуальною проблемою сьогодення є організація стеганографічного каналу зв'язку із забезпеченням автентичності та цілісності інформації, що передається приховано, а також встановлення їх порушень (якщо це відбулося). Зазвичай для автентифікації даних використовуються засоби цифрового підпису. Однак такі засоби не зовсім підходять для забезпечення автентифікації мультимедійної інформації. Справа в тому, що повідомлення, позначене електронним цифровим підписом, має зберігатися й передаватися абсолютно точно, «біт у біт». Мультимедійні дані можуть незначно спотворюватися як при зберіганні (наприклад, за рахунок стискання), так і під час передавання каналом зв'язку. При цьому якість цих даних залишається припустимою для користувача, але цифровий підпис працювати не буде. Одержувач не зможе відрізнити справжнє, хоча і трохи змінене, повідомлення, від «атакованого» зловмисником. Крім того, мультимедійні дані можуть бути перезбережені з одного формату в інший. Ще один дуже важливий недолік цифрового підпису полягає у тому, що його легко видалити із завіреного ним повідомлення, після чого прилаштувати до нього новий підпис. Видалення підпису дозволить зловмиснику відмовитися від авторства або ввести в оману законного одержувача щодо авторства повідомлення [1, 2].

Вирішення таких завдань, як приховане передавання даних та перевірка їх автентичності, не є новими, але спроби їх розв'язку [3—5] не дали належного результату. Так у [3, 4] запропоновано стеганографічні методи для перевірки автентичності, де додаткова інформація вбудовується у частотній області цифрового зображення-контейнеру, які є нестійкими до збурювальних дій у каналі зв'язку, що пов'язано з використанням методу найменшого значущого біта [2]. Крім того, стеганографічні методи у роботах [4, 5] працюють тільки з цифровими зображеннями (ЦЗ) у градаціях сірого, що значно зменшує область їх застосування. Стеганографічний алгоритм, який запропоновано в [5], організує вбудову додаткової інформації у коефіцієнти дискретного косинусного перет-

ворення блоків стандартного розбиття матриці зображення таким чином, що сприяє накопиченню обчислювальної похибки, а тому зменшенню ефективності декодування додаткової інформації.

Нерідко в наукових роботах, які розглядають означені питання, не розрізняють належним чином поняття цілісності та автентичності прихованої інформації, які є одними з основних категорій сучасної комп'ютерної стеганографії [2].

У роботі [6] розроблено основні кроки стеганометоду $SM3$ для вирішення триєдиної задачі стеганографії: прихованого передавання додаткової інформації, перевірки її цілісності та автентичності. Але організація автентифікації потребує уточнення та деталізації.

Метою роботи є удосконалення процесу автентифікації додаткової інформації у стеганографічному методі, запропонованому в роботі [6].

Задачі, які потрібно вирішити для досягнення мети:

— вибір та обґрунтування доцільності способу розбиття множини ЦЗ на підмножини;

— визначення порогового значення для відношення кількості блоків матриці ЦЗ, в яких порушення автентичності не було виявлено, до загальної кількості блоків для вирішення задачі забезпечення автентичності додаткової інформації, що передається приховано.

Основна частина

У якості контейнера в $SM3$ виступає кольорове ЦЗ в схемі RGB. Безпосередня вбудова додаткової інформації проводиться у синю кольорову складову — $M \times N$ -матрицю B.

Стеганоперетворення в $SM3$, враховуючи вимогу стійкості до атак проти вбудованого повідомлення, що висувається до будь-якого сучасного стеганографічного алгоритму [2], проводиться у частотній області зображення, а саме шляхом збурення коефіцієнтів дискретного перетворення Фур'є 2×2 — блоків матриці ЦЗ-контейнера, отриманих шляхом стандартного розбиття.

Множина контейнерів (МК) включає в себе 750 ЦЗ, які були взяті як з архіву непрофесійних фотографів, так і з традиційної при тестуванні алгоритмів, які працюють з ЦЗ, бази NRCS [7].

Пропонується МК розбити на l підмножин випадковим чином. Кожній з підмножин поставити у відповідність свій унікальний бінарний ключ K_i, $i = \overline{1,l}$. У якості ключа виступає випадковим чином сформована бінарна $R \times R$ -матриця з елементами $K_{nm}^{(i)}$, $n,m = \overline{1,R}$, $i = \overline{1,l}$. Результат розбиття є часткою секретного ключа стеганографічного методу $SM3$.

Запропонований спосіб має вагому перевагу над іншими способами розбиття [2]: вгадати або підібрати ключ, який відноситься до конкретної підмножини в обчислювальному сенсі дуже складно (так, якщо ключ має розміри 4×4, то загальна кількість можливих бінарних ключів буде 2^{16}), що забезпечує стійкість сформованої стеганографічної системи.

Для організації стеганоперетворення в $SM3$ значимим було питання вибору розміру блоку матриці ЦЗ-контейнера, який використовується для вбудови одного біту додаткової інформації. У роботі [8] обґрунтована доцільність розміру блоку 2×2, що дозволило забезпечити відсутність уявної частини в значеннях коефіцієнтів дискретного перетворення Фур'є; запропонувати спосіб позбутися дробової частини, при цьому не порушуючи надійність сприйняття стеганоповідомлення (первинне кодування інформації) — усі коефіцієнти дискретного перетворення Фур'є є цілими.

Додаткова інформація $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}$ [6], що є результатом попереднього первинного кодування конфіденційної інформації, зазнає вторинного кодування з використанням секретного ключа K_i, що відповідає підмножині обраного ЦЗ-контейнера, для забезпечення автентифікації відповідно до співвідношення:

$$p_j \otimes K_i = \begin{pmatrix} p_j \otimes K_{1,1}^{(i)} & p_j \otimes K_{1,2}^{(i)} & \dots & p_j \otimes K_{1,R}^{(i)} \\ p_j \otimes K_{2,1}^{(i)} & p_j \otimes K_{2,2}^{(i)} & \dots & p_j \otimes K_{2,R}^{(i)} \\ \dots & \dots & \dots & \dots \\ p_j \otimes K_{R,1}^{(i)} & p_j \otimes K_{R,2}^{(i)} & \dots & p_j \otimes K_{R,R}^{(i)} \end{pmatrix} = \begin{pmatrix} P_{1,1}^{j(K)} & P_{1,2}^{j(K)} & \dots & P_{1,R}^{j(K)} \\ P_{2,1}^{j(K)} & P_{2,2}^{j(K)} & \dots & P_{2,R}^{j(K)} \\ \dots & \dots & \dots & \dots \\ P_{R,1}^{j(K)} & P_{R,2}^{j(K)} & \dots & P_{R,R}^{j(K)} \end{pmatrix} = P^{j(K)}, \quad (1)$$

де p_j — один біт додаткової інформації, $\otimes$ — логічна операція «виключного АБО», $P^{j(K)}$ — матриця, що відповідає 1 біту p_j додаткової інформації після вторинного кодування.

Розмір ключа K_i не пов'язаний з довжиною t бінарної послідовності, яка вбудовується.

Позначимо: $F_{nm}^{(B)}$ — матрицю блоку частотних коефіцієнтів розміром 2×2, $n=\overline{1,\left[\frac{N}{2}\right]}$, $m=\overline{1,\left[\frac{M}{2}\right]}$, у яку відбувається вбудова 1 біта матриці $P^{j(K)}$. Результат — блок $FF_{nm}^{(B)}$ з елементами

$$FF_{nm}^{(B)}(u,v)=\text{bitset}\left(F_{nm}^{(B)}(u,v),\text{pos},P_{nm}^{j(K)}\right),\ u,v=\overline{0,1},$$

де bitset () — функція, яка встановлює значення $P_{nm}^{j(K)}$ у зазначеній позиції pos двійкового подання значення елементу $F_{nm}^{(B)}(u,v)$, $pos\in\{2,3,4\}$; реалізація цієї функції може здійснюватись у математичному пакеті Matlab (2009).

Після цього відбувається зворотне дискретне перетворення Фур'є, яке буде проходити без округлень, завдяки тому що кожний коефіцієнт дискретного перетворення Фур'є зміниться на $\{2^1, 2^2, 2^3\}$, залежно від позиції вбудови додаткової інформації, з урахуванням специфіки формування коефіцієнтів дискретного перетворення Фур'є для блоків 2×2 [6].

Декодування додаткової інформації починається з розбиття матриці $\overline{\overline{B}}$, де $\overline{\overline{B}}$ — матриця синьої складової отриманого можливо збуреного ЦЗ $\left(B\neq\overline{\overline{B}}\right)$, на блоки 2×2, що не перетинаються. Для кожного блока будується дискретне перетворення Фур'є з елементами $\overline{F}_{nm}^{(B)}(u,v),\ u,v=\overline{0,1}$. З елементів блоку матриці $\overline{F}_{nm}^{(B)}$ проходить виділення біта $\overline{P}_{nm}^{j(K)}$ можливо збуреної матриці $\overline{P}^{j(K)}$: нехай k_0, k_1 — кількість нулів та одиниць, які були виділені з позиції pos двійкового представлення цілих часток значень усіх чотирьох коефіцієнтів дискретного перетворення Фур'є блока $\overline{F}_{nm}^{(B)}$ [6]. Тоді

$$\overline{P}_{nm}^{j(K)}=\begin{cases}\text{bitget}\left(\left[\overline{F}_{nm}^{(B)}(1,1)\right],pos\right),\ \text{якщо } k_0=0\vee k_1=0;\\ 0,\ \text{якщо } k_0>k_1;\\ 1,\ \text{якщо } k_0\le k_1,\end{cases}$$

де bitget () — функція, яка видає значення, що стоять у позиції pos для $\left[\overline{F}_{nm}^{(B)}(1,1)\right]$; реалізація цієї функції може здійснюватись у математичному пакеті Matlab (2009).

Безпосередньо процес перевірки автентичності додаткової інформації реалізується таким чином.

З елементів $\overline{P}_{nm}^{j(K)}$, $n,m=\overline{1,R}$ побудувати матрицю $\overline{P}^{j(K)}$

Якщо

$$\overline{P}^{j(K)}=K_i\vee\overline{P}^{j(K)}=\overline{K_i},\ \text{де } \overline{K_i}\ \text{— інверсія матриці ключа } K_i,\ \vee\ \text{— або.}$$

Тоді

автентичність блока $\overline{B}$ не була порушена.

Припустимо, що було виділено Т1 блоків з Т2 загальної кількості блоків, в яких не було знайдено порушення автентичності, тоді :

Якщо

$$\frac{T1}{T2}*100>A,\ \text{де } A\ \text{— порогове значення,}$$

Тоді

автентичність переданої інформації не порушена,

Інакше

передана інформація не є автентичною.

Виникає питання, яке не було остаточно вирішено у [6], про визначення порогового значення A.

Результати

Порогове значення A має вагому роль у роботі запропонованого методу для перевірки автентичності ЦЗ. Для його визначення ЦЗ-стеганоповідомлення, сформовані за допомогою $SM3$, піддавалися збурювальним діям, які не приводили до порушення надійності сприйняття зображення:

а) накладанню гаусівського шуму з нульовим математичним очікуванням та дисперсією 0,0001 (табл. а);

б) гаусівського шуму з нульовим математичним очікуванням та дисперсією 0,001 (табл. б);

в) стиску з коефіцієнтом якості 90 (табл. в);

г) стиску з коефіцієнтом якості 100 (табл. г);

д) накладанню мультиплікативного шуму з дисперсією 0,0001 (табл. д);

е) мультиплікативного шуму з дисперсією 0.001 (табл. е);

ж) декількох збурювальних дій одночасно (табл. ж).

Після цього відбувалося декодування додаткової інформації. Для кожного зображення рахувалася кількість автентичних блоків, тобто блоків, у яких ключ, який відповідає підмножині цього зображення, збігається з виділеним ключем цього блоку. Результати наведені у таблиці, де використовуються такі позначки: ЗБ — збурення, які накладалися на ЦЗ для тестування роботи алгоритму, ЗН — значення отриманих оцінок H, $H = \frac{T1}{T2}100\ \%$, де $T1$ — кількість автентичних блоків для ЦЗ, $T2$ — загальна кількість блоків (в експериментах $T2 = 2500$), у таблиці виведені максимальна та середня оцінки H для усіх зображень.

Відсоток правильно декодованих автентичних блоків у цифрових зображеннях (H)

ЗН \ ЗБ	а	б	в	г	д	е	ж
максимум	12,8	6,92	5,64	7,44	13,32	11,28	6,36
середнє	10,11	6,15	0,57	1,66	7,47	6,84	4,14

Порогове значення визначалося за формулою

$$100\ \% - \max(H) = 100 - 13,32 \approx 87. \qquad (2)$$

Ефективність запропонованого стеганографічного методу перевірки автентичності оцінювалась за такими параметрами:

1. Кількість помилок при перевірці автентичності інформації, що передається, першого роду (пропуск порушення автентичності, яке має місце) — 0 %;

2. Кількість помилок при перевірці автентичності інформації, що передається, другого роду (помилкова констатація порушення автентичності) — 0,02 %.

Висновки

У роботі запропоновано удосконалення процесу автентифікації додаткової інформації в стеганографічному методі $SM3$, розробленому в [6].

Обґрунтовано доцільність випадкового розбиття множини ЦЗ-контейнерів на підмножини для організації автентифікації. Треба зазначити, що такий спосіб розбиття має недолік: значний розмір секретного ключа, який має бути переданий адресатові по захищеному каналу зв'язку, тому зусилля автора зараз спрямовані на пошук розв'язку задачі аутентифікації додаткової інформації, що дозволить зменшити розмір секретного ключа.

Результатом обчислювальних експериментів, проведених в роботі, стало визначення порогового значення $A = 87$ для відношення кількості блоків матриці ЦЗ, в яких порушення автентичності не було виявлено, до загальної кількості блоків. Це порогове значення забезпечило високу ефективність стеганометоду з погляду автентифікації додаткової інформації: помилки 1 роду склали 0 %, 2 роду — 0,002 %.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Кузнецов О. О. Стеганографія : навч. посіб. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. — Х. : Вид. ХНЕУ, 2011. — 232 с.

2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : СОЛОН-Пресс, 2009. — 272 с.

3. Inderjit Singh. DFT Based Image Enhancement and Steganography / Inderjit Singh, Sunil Khullar, Dr. S. C. Laroiya // International Journal of Computer Science and Communication Engineering. — 2013. — Vol. 2, Iss. 1. — P. 5—7.

4. Bhattacharyya D. Authentication and Secret Message Transmission / D. Bhattacharyya, J. Dutta, P. Das, S. K. Bandyopadhyay, T. Kim. // Int. J. Communications, Network and System Sciences. — 2009. — № 5. — P. 363—370.

5. Ritu Pareek Discrete Cosine Transformation based Image Watermarking for Authentication and Copyright Protection / Ritu Pareek, P. K. Ghosh // International Journal of Engineering and Advanced Technology (IJEAT). — 2012. — Vol. 1, Iss. 3. — P. 152—156.

6. Кобозева А. А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А. А. Кобозева, М. А. Козина. // Проблемы региональной энергетики : электронный журнал Академии наук Республики Молдова. — 2014. — № 3 (26). — С. 93—106.

7. Nrcs photo gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. — Режим доступу: http://photogallery.nrcs.usda.gov (дата звернення: 10.09.2014).

8. Kozina M. O. Discrete Fourier transform as a basis for steganography method / M. O. Kozina // Праці Одеського політехнічного університету. — 2014. — Вип. 2 (44). — С. 147—154.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 03.01.2015

Козіна Марія Олександрівна — аспірантка, асистент кафедри інформатики та управління захистом інформаційних систем, e-mail: mashaK1989@rambler.ru.

Одеський національний політехнічний університет, м. Одеса

M. O. Kozina[1]

Method of verification of authenticity of information that is passed by steganographic communication channel

[1]Odessa National Polytechnic University

The improvement of steganographic method which was developed earlier by the author, which has no analogues among modern steganomethods, as it solves simultaneously a triple task: secret data (additional information), as a random binary sequence — authentication and check the integrity of additional information. As a container it views digital color images. It shows the results of numerical experiments that confirm the high efficiency improved steganometod in identifying inauthentic of additional information.

Keywords: steganographic method, digital image, discrete fourier transform, authenticity.

Kozina Mariia — Post Graduate Student of the Chair of informatics and management the protection information systems, e-mail: mashaK1989@rambler.ru

М. А. Козина[1]

Метод проверки аутентичности информации, передаваемой стеганографическим каналом связи

[1]Одесский национальный политехнический университет

Предложено усовершенствование стеганографического метода, разработанного автором ранее, который не имеет аналогов среди современных стеганометодов, так как решает одновременно триединую задачу: секретной передачи данных (дополнительной информации), в качестве которых выступает случайный образом сформированная бинарная последовательность, аутентификации и проверки целостности дополнительной информации. В качестве контейнера рассматривается цифровое цветное изображение. Приведены результаты вычислительного эксперимента, которые подтверждают высокую эффективность усовершенствованного стеганометода при выявлении нарушений аутентичности дополнительной информации.

Ключевые слова: стеганографический метод, цифровое изображение, дискретное преобразование Фурье, аутентичность.

Козина Мария Александровна — аспирантка, ассистент кафедры информатики и управления защитой информационных систем, e-mail: mashaK1989@rambler.ru