УДК 004.003.26

Роман Михайлович Штонда *(старший науковий співробітник науково-дослідної лабораторії)*
Юрій Олександрович Процюк *(провідний науковий співробітник науково-дослідної лабораторії)*
Олег Миколайович Маковецький *(старший науковий співробітник науково-дослідної лабораторії)*
Ірина Робертівна Мальцева *(старший науковий співробітник науково-дослідного відділу)*

Військовий інститут телекомунікацій та інформатизації
Державного університету телекомунікацій, Київ, Україна

АНАЛІЗ МЕТОДІВ ЦИФРОВОЇ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ

В сучасному світі постійно відбувається прогрес в галузі комп'ютерних систем та мереж. Існуючі методи цифрової стеганографії зображень не враховують певною мірою таємність та робастність на етапі приховування, що не забезпечує реагування на активні атаки противника.

В статті наведені та проаналізовані методи стеганографічного захисту цифрових зображень, що дозволяє зауважити, якщо поєднати метод вбудовування в область коефіцієнтів дискретного косинусного перетворення F5 з методами шаблонного вбудовування, дане поєднання дозволить підвищити показники таємності та робастності.

Ключові слова: *методи стеганографічного захисту інформації; робастність та таємність.*

Вступ

Забезпечення стійкості стеганографічних перетворень до активних атак в комп'ютерних системах та мережах (КСМ) є актуальною практичною задачею стеганографії на сьогоднішній день. Методи цифрової стеганографії зображень здатні забезпечити високу робастність та таємність вбудовування, тому ці характеристики необхідно враховувати при забезпеченні стійкості до активних атак в КСМ.

Постановка проблеми. В сучасному світі постійно відбувається прогрес в галузі КСМ. Існуючі методи цифрової стеганографії зображень не враховують певною мірою таємність та робастність на етапі приховування, що не забезпечує реагування на активні атаки противника.

Аналіз останніх досліджень і публікацій. У розвиток стеганографії значний внесок зробили в своїх працях такі автори, як В.О.Хорошко [1], Г.Ф.Конахович [2], М.Є.Шелест [3], В.К.Задірака, Н.В.Кошкіна [4], А.В.Аграновський [5], В.Г.Грібунін [6] Бабич І.В., Паламарчук С.А., Паламарчук Н.А., Овсянніков В.В. [7] та інші Внесок зазначених досліджень полягає в розробці та вдосконалені методів приховування даних в зображеннях. Але в цих роботах розробка методів стеганографічного захисту інформації авторами відбувалася без врахування взаємозв'язку між вимогами таємності та робастості.

Метою статті є проведення аналізу методів цифрової стеганографії зображень, таких як методу стеганографічного захисту інформації F5 та методу шаблонного вбудовування даних на основі матричного представлення кодів Хеммінга.

Методи дослідження

У ході дослідження використовувалися наступні методи: аналізу теоретичних джерел та порівняльного аналізу.

Виклад основного матеріалу дослідження

Більшість методів стеганографічного захисту інформації, що вбудовують дані в просторову область зображень, забезпечують не високу робастість до будь-яких спотворень [2, 8]. Наприклад застосування операцій ущільнення з втратами призводить до повного знищення секретної інформації, яка прихована методом заміни наймолодших бітів (НБ) у просторовій області зображень. Більш робастними до різноманітних спотворень, у тому числі і ущільнення, є методи стеганографічного захисту інформації, що використовують для приховування даних у частотну область [1].

1. Методи приховування даних в частотній області зображення

Існує декілька способів представлення зображення у частотній області. *Наприклад,* з використанням дискретних косинусних перетворень (ДКП), швидкого перетворення Фур'є або вейвлет-перетворення [1]. Ці перетворення можуть застосовуватись як до всього зображення, так і до певних його частин.

Одним із сучасних, розповсюджених на сьогоднішній день методів, є метод стеганографічного захисту інформації F5 [2]. Даний метод був запропонований з метою підвищення обсягу даних, що вбудовуються у JPEG-зображення, за умови забезпечення захищеності. Замість вбудовування в НБ, операція вбудовування в F5 може лише зменшити абсолютне значення ДКП коефіцієнта на одиницю. Така операція не міняє форму ДКП гістограми, що після вбудовування виглядає як у випадку ущільнення оригінального зображення з меншим параметром якості.

Метод F5 вбудовує біти повідомлення у псевдо-випадково обрані коефіцієнти, ігноруючи

DC-коефіцієнт та коефіцієнти з нульовим значенням.

Якщо значення коефіцієнта змінюється з 1 або – 1 на 0 (“стягування”), то біт повідомлення, що в такому випадку завжди є нулем, заново вбудовується у наступний коефіцієнт. Це пояснюється врахуванням лише нульових коефіцієнтів при витяганні даних одержувачем. Однак, при повторному вбудовуванні нульового біта кількість нульових коефіцієнтів перевищує кількість одиничних, що може сприяти утворенню “східчастої” гістограми завдяки її монотонності на $(-\infty,0]$ та $[0,\infty)$. У F5 ця задача розв’язується шляхом повторного визначення НБ для від’ємних значень коефіцієнтів:

$$LSB(X) = 1 - x \bmod 2, \qquad (1)$$

для $x < 0$.

Максимальний обсяг даних, що можна вбудувати за допомогою F5, складає

$$n - Hist(0) - \frac{n}{64} - (Hist(-1) + Hist(1))/2, \qquad (2)$$

де n – загальна кількість ДКП-коефіцієнтів; Hist – гістограма ДКП-коефіцієнтів. Перші три складові n – Hist (0) – n/64 визначають кількість ненульових АС-коефіцієнтів, остання складова (Hist (-1) + Hist (1))/2 визначає втрати, обумовлені «стягуванням». Метод стеганографічного захисту інформації F5 є методом з відносно високою ємністю, що в середньому дозволяє вбудувати 0,75 біт на кожен ненульовий ДКП-коефіцієнт при якості JPEG-ущільнення 80%.

Незважаючи на зміну методом F5 гістограми ДКП-коефіцієнтів, деякі важливі характеристики гістограми зберігаються, як, наприклад, монотонність. Оскільки принцип F5 не ґрунтується на обміні значень коефіцієнтів в парах, він є стійким до атаки з використанням статистики (гістограм) першого порядку. Однак F5 може бути виявлено за допомогою стеганоаналітичної процедури калібрації.

У якості модифікації F5 для вбудовування коротких повідомлень додатково застосовується шаблонний метод, що підвищує питомий показник змін шляхом мінімізації кількості змін, які вносяться методом F5.

2. Методи шаблонного вбудовування даних на основі матричного представлення кодів Хеммінга

Змінюючи різні параметри зображення, можна вбудувати таємне повідомлення декількома способами. Наприклад, при НБ вбудовуванні [3, 6] змінюються відповідні наймолодші біти значень інтенсивності пікселів зображення. Для цього методу вбудовування ціною однієї зміни в середньому досягається вбудовування 2 бітів зображення. Однак зазначений показник змін можливо покращити за умови, якщо повідомлення, яке вбудовується, є набагато коротшим у порівняні з максимальною довжиною.

Надалі через β позначено функцію, що ставить у відповідність біти повідомлення певним параметрам зображення.

Передбачається, що існують такі функції вбудовування та витягування, які вимагають щонайбільше R змін для будь-якого повідомлення $m \in M$:

$$Emb: \{0,1\}^n \times M \to \{0,1\}^n; Ext: \{0,1\}^n \to M, \qquad (3)$$

причому для всіх $m \in M$ та $x \in \{0,1\}^n$ справедливо

$$Ext(Emb(x,m)) = m, \qquad (4)$$

$$d(x.Ed(x.m)) \le R. \qquad (5)$$

Враховуючи, що обсяг бітів повідомлення складає $\log_2|M|$ та за рівномірного розподілу повідомлення *m* в зображенні x, питомий показник змін для $R_a \le R$ визначається як $e=(\log_2|M|)/R_a$. Через $\underline{e}=(\log_2|M|)/R$ позначено нижню межу питомого показника змін [9].

Шаблонне вбудовування реалізується шляхом використання лінійного коду ζ, що описується параметрами [n, k], де n>k та позначається кодове слово і порція вбудовуваних даних, відповідно. Будь який лінійний [n, k] код ζ повністю описується його твірною матрицею G, що представляє собою регулярну бінарну матрицю з k рядками та n стовпчиками. Будь-яке кодове слово $c \in \zeta$ можна отримати як лінійну комбінацію рядків G, де коефіцієнти описуються k бітами.

Для матриці відповідності H розміром $(n - k)\times n$ та деякого кодового слова c' справедливо:

$$\begin{aligned} Hc' &= 0, \text{якщо} c' \in \zeta \\ Hc' &= 0, \text{якщо} c' \notin \zeta \end{aligned} \qquad (6)$$

Може існувати багато різних кодових слів c', що задають єдиний вектор s = Hc', і множину яких позначають ζ(s). Отже, використовуючи [n, k] код, можна вбудувати (n – k) бітів повідомлення.

Надалі m вважається (n – k)-бітним повідомленням. Вбудовування вимагає зміни певних бітів у послідовності x, отриманої з оригінального зображення за допомогою β. Результуюча послідовність y, одержана з x, має задовольняти Hy= m.

Якщо визначити y=x+e, де e – вектор змін, то вага за Хеммінгом для e рівна кількості внесених при вбудовуванні змін та визначається:

$$\begin{aligned} H(x+e) &= Hy = m \\ He &= m - Hx \end{aligned} \qquad (7)$$

Якщо (7) задовольняється будь-яким e з множини ζ(m – Hx). Отже, для лінійного [n, k] коду ζ з радіусом R необхідно обрати e_L з найменшою вагою за Хемінгом, що однозначно не перевищує R.

В залежності від вибору лінійного коду ζ, можна реалізувати різні методи шаблонного вбудовування. Найпростішим методом стеганографічного захисту інформації є застосований у стеганографічному методі F5, що полягає у використанні бінарних кодів Хеммінга з $n=2^p - 1$ та $k=2^p - 1 - p$, де p – додатне ціле.

Матриця відповідності H має розмірність $p\times(2^p-1)$, а її стовпці є бінарними представленнями чисел $1,\ldots, 2^p-1$. Отже, стеганографічне повідомлення m міститься серед стовпців H, наприклад, в і-му. Тоді, при вбудовуванні m визначається вектором e_L з єдиним нульовим бітом в і-й позиції, оскільки R=1.

На практиці відправник вбудовує K бітів повідомлення у N бітів, отриманих із зображення за допомогою β, отже відносна довжина повідомлення складає α= K/N. Оскільки при шаблонному вбудовуванні з використанням кодів Хеммінга p бітів вбудовуються в 2^p-1 бітів ціною максимум однієї зміни, мінімізація загальної кількості змін, обумовлених вбудовуванням, вимагає визначення найбільшого p, що задовольняє

$$\alpha_{p+1}=\frac{\rho+1}{2^{p+1}-1}<\alpha\le\frac{\rho}{2^p-1}=\alpha_p \qquad (8)$$

Таким чином, відправник використовує для вбудовування $N/(2^p-1)$ блоків з (2^p-1) бітами в кожному.

Вбудовування псевдо-випадкової послідовності m з p бітів у блок x, з ймовірністю $1/2^p$ не вимагає жодних змін. Отже, середня кількість змін складає $0\times1/2^p+1\times(1-1/2^p)=1-1/2^p$ і питомий показник змін

$$e_p=\frac{p}{1-2^{-p}} \qquad (9)$$

У таблиці 1 наведено відносні довжини повідомлення та відповідні питомі показники змін. Необхідно відмітити, що коди Хеммінга, не можуть бути застосовані для вбудовування при відносній довжині повідомлення більшій ніж 2/3.

Таблиця 1

Відносна довжина повідомлення та питомий показник змін при шаблонному вбудовуванні з використанням бінарних кодів Хеммінга

p	Відносна довжина повідомлення, α_p	Питомий показник змін, e_p
1	1,000	2,000
2	0,667	2,667
3	0,429	3,429
4	0,267	4,267
5	0,161	5,161
6	0,093	6,093
7	0,055	7,055
8	0,031	8,031
9	0,018	9,018

Для визначення максимальної відносної довжини повідомлення α необхідно зауважити, що максимальна кількість варіантів внесення не більше ніж R змін у послідовність з n біт, яку дозволяє оцінити

$$\log_2|M|\le\log_2\sum_{i=0}^{R}\binom{n}{i}2^i \qquad (10)$$

Для подальшого обчислення використовується відома з теорії інформація нерівність

$$\log_2\sum_{i=0}^{R}\binom{n}{i}2^i\le nH(R/n) \qquad (11)$$

де $H(x)= - x\log_2 x-(1- x)\log_2(1- x)$ – функція бінарної ентропії.

Таким чином, з (4), (5) та (6) випливає

$$\alpha_{max}=\frac{\log_2|M|}{n}\le H(R/n) \qquad (12)$$

При визначенні максимального питомого показника змін, за встановленого α, необхідно переписати (12) як $n/R\le1/H^{-1}(\alpha)$ або $(\log|M|/R)\times(n/\log_2|M|\le1/H^{-1}(\alpha)$, звідки

$$e=\frac{\log_2|M|}{R}\le\frac{\alpha}{H^{-1}(\alpha)} \qquad (13)$$

де множина значень оберненої функції H^{-1} відповідає інтервалу [0, 1/2]. Це дозволяє оцінити нижню межу питомого показника змін, яку можна досягти будь-яким методом шаблонного вбудовування.

На практиці складно знайти коди з питомим показником змін близьким до межі. Випадкові лінійні коди невеликої розмірності (n – k) дозволяють покращити питомий показник змін кодів Хеммінга. Нелінійні коди забезпечують вищий питомий показник змін, однак значно ускладнюють вбудовування.

Висновки й перспективи подальших досліджень

Хотілося б відмітити, що в теперішній час інформаційних технологій доцільним та актуальним захистом може бути застосування стеганографічного захисту інформації в КСМ. Зроблений аналіз методів цифрової стеганографії зображень дозволяє зауважити, що поєднання методу вбудовування в область коефіцієнтів ДКП F5 з методами шаблонного вбудовування дозволить підвищити показники таємності та робастності. Однак є і недоліки, до яких слід віднести можливість детектування методами стеганоаналізу стегозображень, отриманих за допомогою даного методу стеганографічного захисту інформації. Це пояснюється відсутністю оцінок допустимого обсягу вбудовуваних даних. Подальшим дослідженням підлягає розробка адаптивних методів шаблонного вбудовування зображень, що враховували б ці оцінки.

Література

1. Хорошко В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А.Чекатков. – К. : Юниор, 2003. – 504 с. **2. Конахович Г. Ф.** Компьютерная стеганография. Теория и практика/ Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с. **3. Хорошко В. О.** Основи комп'ютерної стеганографії: навч.пос. / В. О.Хорошко, В. О. Азаров, М. Є. Шелест. – Вінниця : ВДТУ, 2003. – 142 с.

4. **Задірака В. К.** Аналіз стійкості стеганографічних систем в моделі пасивного противника / В. К. Задіра, Н. В.Кошкіна, О. С. Олексюк // ИИ. – 2004. – №3. – С. 801–805. **5. Агрsuperновський А. В.** Основы компьютерной стеганографии / А. В. Агрsuperновський, П. Н. Девянин. – М. : Радио и связь, 2003. – 151 с. **6. Грибунин В. Г.** Теория и практика вейвлет-преобразования. [Електронный ресурс] / В. Г. Грибунин.- Режим доступу : http://autex.spb.ru/wavelet/books/wtp.htm **7. Бабич І. В.** Огляд стеганографічних методів перетворення інформації в зображеннях./ І. В. Бабич, С. А. Паламарчук, Н. А. Паламарчук, В. В. Овсянніков – К. : НАУ. 2012. – С. 29–36. **8. Мокін Б. І.** Математичні моделі робастної стійкості та чутливості нелінійних систем: моногр. / Б. І. Мокін, С. В. Юхимчук. – Вінниця : УНІВЕРСУМ-Вінниця, 1999. – 122 с. **9. Кларк Д.** Кодирование с исправлением ошибок в системах цифровой связи / Д. Кларк, Д. Кейн. – М. : Радио и связь, 1987. – 392 с.

АНАЛИЗ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ ИЗОБРАЖЕНИЙ

Роман Михайлович Штонда *(старший научный сотрудник научно-исследовательской лаборатории)*
Юрий Александрович Процюк *(ведущий научный сотрудник научно-исследовательской лаборатории)*
Олег Николаевич Маковецкий *(старший научный сотрудник научно-исследовательской лаборатории)*
Ирина Робертовна Мальцева *(старший научный сотрудник научно-исследовательского отдела)*

Военный институт телекоммуникаций и информатизации
Государственного университета телекоммуникаций, Киев, Украина

В современном мире постоянно происходит прогресс в области компьютерных систем и сетей. Существующие методы цифровой стеганографии изображений не учитывают, в определенной степени, секретности и робастности на этапе скрытия, что не обеспечивает реагирование на активные атаки противника.

В статье приведены и проанализированы методы стеганографической защиты цифровых изображений, что позволяет заметить, если совместить метод встраивания в область коэффициентов дискретного косинусного преобразования F5 с методами шаблонного встраивания, данное сочетание позволит повысить показатели секретности и робастности.

Ключевые слова: *методы стеганографической защиты информации; высокая робастность и секретность***.**

ANALYSIS OF DIGITAL IMAGES STEGANOGRAPHY METHODS

Roman M. Shtonda *(Senior Research Fellow of a Research Laboratory)*
Yurii O. Protsiuk *(Leading Research Fellow of a Research Laboratory)*
Oleh M. Makovetskyi *(Senior Research Fellow of a Research Laboratory)*
Iryna R. Maltseva *(Senior Research Fellow of a Research Section)*

Military Institute of Telecommunications and Informatization of
State University of Telecommunications, Kyiv, Ukraine

The progress in the area of computer systems and networks is always take place in the modern world. Existing methods of digital images steganographic don't take into account, to some extent, the privacy and robustness at the concealment stage that does not provide a response to active enemy attacks.

The methods of steganographic protect of digital images were presented and analyzed in the article, that allow to observe, if combine embedding method into the area of coefficients of discrete cosine F5 transformation with methods of pattern embedding, this combination will allow to improve the robustness and secrecy indicators.

Keywords: *methods of steganographic information security; high robustness and secrecy.*

References

1. Horoshko V.A., Chekatkov A.A. (2003), Methods and means of information protection. [*Metodyi i sredstva zaschityi informatsii*], Yunior, Kiev, 504 p. **2. Konahovich G.F.,** Puzyirenko A.Y. (2006) Computer steganography. Theory and practice. [*Kompyuternaya steganografiya. Teoriya i praktika*], MK-Press, Kiev, 288 p. **3. Khoroshko V.O.,** Azarov V.O., Shelest M.Y. (2003) Basics of komp'yuternoï steganografiï. [*Osnovy kompiuternoi stehanohrafii*], VDTU, Vinnytsia, 142 p. **4. Zadiraka V.K.,** Koshkina N.V., Oleksiuk O.S. (2004), Stability analysis of steganographic systems in passive attack. [*Analiz stiikosti stehanohrafichnykh system v modeli pasyvnoho protyvnyka*], YY, pp.801–805. **5. Agranovskiy A.V.,** Devyanin P.N. (2003), Fundamentals of Computer steganography. [*Osnovyi kompyuternoy steganografii*], Radio I svyaz, Moscow, 151 p. **6. Gribunin V.G.** Theory and Practice of wavelet transformation. [*Teoriya i praktika veyvlet-preobrazovaniya*]. Available at : http://autex.spb.ru/wavelet/books/wtp.htm. **7. Babich I.V.** PalamarchukS.A., PalamarchukN.A., OvsyannikovV.V. (2012), Review steganographic methods of converting information into images. [*Ohliad stehanohrafichnykh metodiv peretvorennia informatsii v zobrazhenniakh*], NAU, Kiev pp. 29-36. **8. Mokin B.I.,** Yuhimchuk S.V. (1999), Mathematical models of robust stability and sensitivity of nonlinear systems: the monogram. [*Matematichni modeli robastnoyi stiykosti ta chutlivosti neliniynih sistem: monogr*], UNIVERSUM, Vinnitsya, 122 p. **9. Klark D.,** Keyn D. (1987), Coding with yspravlenyem oshybok systems Digital Communications. [*Kodirovanie s ispravleniem oshibok v sistemah tsifrovoy svyazi*], Moscow, 392 p.

Отримано: 9.10.2014 року