УДК 004.056.5

СТЕГАНОГРАФІЧНИЙ МЕТОД ВИРІШЕННЯ ТРИЄДИНОЇ ЗАДАЧІ

М. О. Козіна

Одеський національний політехнічний університет
Україна, м. Одеса
mashaK1989@rambler.ru

Запропоновано новий стеганографічний метод, який одночасно забезпечує приховану передачу додаткової інформації, при цьому не порушує надійності сприйняття кольорового цифрового зображення, здійснює перевірку автентичності та цілісності інформації, що передається. У якості додаткової інформації виступає випадковим чином сформована бінарна послідовність.

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

Розробкою засобів і методів приховування факту передачі додаткової інформації займається стеганографія. Існуючі стеганографічні методи (СМ) приховування даних у просторовій області зображення часто не є стійкими до відомих видів спотворень. Традиційно, більш стійкими до різноманітних спотворень, в тому числі і стиснення, вважаються методи, які використовують для приховування даних не просторову, а частотну область контейнера [1].

Сьогодні актуальним напрямком розвитку цифрової стеганографії є розробка методів, які здійснюють організацію прихованого каналу зв'язку шляхом вбудови секретного повідомлення (СП) в область перетворення контейнера з одночасною перевіркою автентичності та цілісності СП, тобто розв'язують триєдину задачу стеганографії. Існуючі на сьогодні розробки [2, 3] не ідеальні та вимагають покращення. Таким чином метою роботи є розробка стеганографічного методу, який вирішує триєдину задачу, зазначену вище.

Для досягнення поставленої мети вирішуються наступні задачі:

— вибір розміру блоку розбиття матриці цифрового зображення (ЦЗ), використовуваного для вбудови додаткової інформації (ДІ);

— вирішення завдання забезпечення цілісності ДІ шляхом отримання цілих частотних коефіцієнтів;

— вибір розміру секретного ключа, використовуваного для попереднього кодування ДІ з метою забезпечення можливості перевірки автентичності інформації, що передається;

— вибір способу формування інформації, що безпосередньо вбудовується в контейнер, таким чином, щоб приховуване повідомлення несло в собі, поряд з переданою конфіденційною інформацією, інформацію для вирішення завдання аутентифікації;

— забезпечення аутентифікації переданої прихованої інформації;

— забезпечення стійкості розробленого СМ до збурних дій в каналі зв'язку.

У якості ключа виступає випадковим чином згенерована бінарна матриця розміру $L \times L$, яка далі буде включена в операцію попереднього кодування додаткові інформації. Також ключ буде відігравати важливу роль у процесі декодування при перевірці автентичності, цілісності, та при отриманні інформації, яка була вбудована, у разі її автентичності.

У роботі було запропоновано використання блоку розбиття розміром 2×2 для матриці контейнера довільного розміру $N \times M$. Вибір такого розміру пов'язаний з особливістю формування частотних коефіцієнтів дискретного перетворення Фур'є (ДПФ), а саме отримання дійсний частотних коефіцієнтів [4]. Запропонований стеганографічний алгоритм (СА) вбудовує СП у частотну область в цілі коефіцієнти ДПФ.

Одним з параметрів, який оцінює ефективність стеганографічного методу, а саме надійність сприйняття сформованого стеганоповідомлення, є пікове відношення сигналу до шуму, яке прийнято

позначати PSNR. Для розробленого СА встановлено PSNR>44, що свідчить про непорушення надійності сприйняття кольорового цифрового зображення після вбудови ДІ.

Побудований СА при декодуванні інформації забезпечує ефективну перевірку цілісності СП [5] завдяки забезпеченню приналежності коефіцієнтів перетворення Фур'є до множини цілих чисел.

У [6] для організації автентифікації інформації, що передається, обґрунтовано доцільність випадкового розбиття множини ЦЗ — контейнерів на підмножини, але значним недоліком запропонованого СМ є необхідність передачі ключа великого розміру по захищеному каналу.

Для вирішення задачі автентифікації пропонується у декілька блоків 8×8 (на практиці — 5 чи 7), що не перетинаються та випадковим чином обрані, вбудовувати у максимальні сингулярні числа блоків номер підмножини контейнерів таким чином, щоб це не спричинило порушення надійності сприйняття. Цей спосіб був обраний не випадково, а завдяки своїй завадостійкості. На етапі декодування відбувається порівняння пари — декодований номер підмножини контейнерів та відповідний йому ключ з парою, яку має утримувач у якості секретного ключа.

В результаті роботи отримані наступні результати:

— похибки першого та другого роду при перевірці автентичності інформації склали 0 та 0,001% відповідно;

— похибки першого та другого роду при перевірці цілісності інформації склали 0 та 0,01% відповідно.

Отримані результати свідчать про високу ефективність розробленого СМ для передачі конфіденційної інформації, перевірки автентичності та цілісності інформації, що передається.

Запропонований стеганографічний метод вирішує одночасно триєдину задачу, зазначену вище.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография.— Москва: СОЛОН-Пресс, 2009.

2. Кобозева А. А., Шовкун А. Д. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера // Науковий вісник Міжнародного гуманітарного університету.— 2012.— № 4.— С. 21—28.

3. Bhattacharyya D., Dutta J., Das P., Bandyopadhyay S. K., Kim T. Authentication and secret message transmission / Int. J. Communications, Network and System Sciences.— 2009.— N 5.— P. 363—370.

4. Козина М. А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации // Сучасна спеціальна техніка.— 2014.— № 4.— С. 91—98.

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

6. Козіна М. О. Метод перевірки автентичності інформації, що передається стеганографічним каналом зв'язку // Вісник Вінницького політехнічного інституту.— 2015.— № 1.— С. 9—13.

———————

M. O. Kozina

Steganographic methods for solving the triune problem.

The paper presents a new steganographic method that simultaneously provides hidden transmission of additional information, not affecting the reliability of perception of color digital images, and verifies the authenticity and integrity of information transmitted. As additional information stands randomly generated binary sequence.

Keywords: *steganographic method, authenticity, integrity, digital images, discrete Fourier transform, steganography method.*

———————