УДК 681.322:621.391

С. М. Білан, к.т.н, професор
(професор кафедри «Телекомунікаційні технології та автоматика» Державного економіко-технологічного університету транспорту, м. Київ)
О. О. Колочун
(студент Державного економіко-технологічного університету транспорту, м. Київ)

МЕТОД СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ МОДИФІКОВАНИХ КОНТЕЙНЕРІВ

У роботі розглядається та досліджується метод стеганографічного приховування інформації на основі контейнерів, які подані файлами зображень. Для збільшення обсягу повідомлення, що впроваджується у контейнер, зображення піддається шумовим спотворенням типу «сіль» та «перець». Біти повідомлення впроваджуються у молодші біти байтів коду зображення, а у пікселі, що спотворені шумом впроваджуються у декілька бітів залежно від обраного порогу яскравості. Використовуються додаткові операції з визначення шумових пікселів, за рахунок використання скануючого вікна заданих розмірів.

Ключові слова: *зображення, піксель, шум, стеганографія.*

В работе рассматривается и исследуется метод стеганографической защиты информации на основе контейнеров, которые поданы файлами изображений. Для увеличения объема сообщения, что внедряется в контейнер, изображение поддается шумовым искажениям типа «соль» и «перец». Биты сообщения внедряются в младшие биты байтов кода изображения, а в пиксели, которые искажены шумом, внедряются в несколько битов в зависимости от избранного порога яркости. Используются дополнительные операции по определению шумовых пикселей, за счет использования сканирующего окна заданных размеров.

Ключевые слова: *изображение, пиксель, шум, стеганография*.

Вступ.Сучасні системи передачі даних та засоби обробки цифрової інформації характеризуються широким впровадженням засобів інформаційного захисту [1-3]. Захист інформації, реалізований на комп'ютерній системі або на передавальній та приймальній частинах системи зв'язку запобігає несанкціонованому доступу до інформації. Особливо важливим є запобігання втручанню до баз даних з конфіденціальною та секретною інформацією. Інформація, яка зберігається на носіях може бути захищена як програмними так і апаратними засобами, які запобігають доступу до засобів зчитування з носія. Існує також інформація, яка передається по незахищених каналах зв'язку.

В першу чергу це стосується систем передачі даних масового користування. В таких системах дані передаються по різних середовищах (електричний кабель, оптичний кабель та радіоефір). У такій ситуації інформацію захищають двома підходами: криптографія та стеганографія [4 – 6]. Перший метод характеризується наявністю відомостей про зашифроване повідомлення, а другий метод характеризується приховуванням самого факту наявності повідомлення. Причому стеганографія використовує криптографію і приховує наперед зашифроване повідомлення.

Постановка задачі. Існуючі на даний момент стеганографічні підходи використовують контейнери різної природи. Одним з таких контейнерів є графічні файли, в байти яких записуються відповідні біти цифрового повідомлення. Причому накладаються вимоги щодо спотворення початкового зображення. Для зменшення видимих спотворень біти цифрового повідомлення записуються у молодші біти вибраних байтів файлу зображення, що значно зменшує об'єм можливого повідомлення та потребує графічних файлів великого об'єму.

Для зменшення об'єму впроваджуваного повідомлення без змін об'єму зображення ставиться задача пошуку таких зон зображення, значні спотворення яких не призводили б до спотворення загальної зорової картини. При цьому ставиться задача внесення таких спотворень у початкове зображення у вигляді шумів. Пікселі, які відображають, шум можуть бути більше спотворені без впливу на зображення в цілому. Вирішення такої задачі дозволить значно збільшити об'єм цифрового повідомлення, що впроваджується.

Загальні принципи стеганографічного захисту інформації на основі контейнера, що поданий графічним файлом. Стеганографічний принцип приховування повідомлень ґрунтується на впровадженні бітів повідомлення у існуючу структуру графічного файлу по заданому алгоритму. Загальна структура такої системи подана на рис. 1.

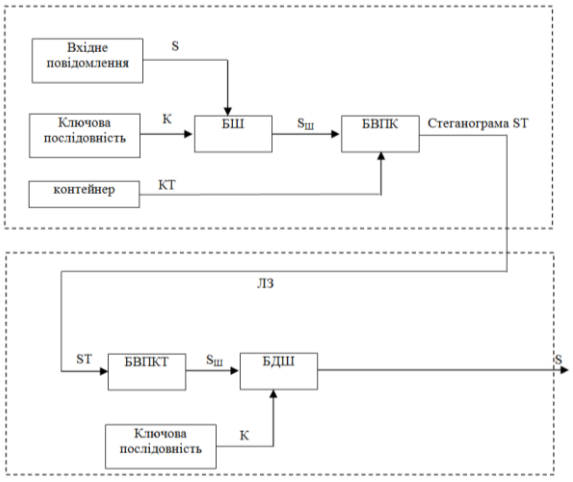


Рис. 1. **Загальна структура системи стеганографічного захисту повідомлень**

Вхідна цифрова послідовність S та ключова послідовність K подаються на відповідні входи блоку шифрування (БШ), який здійснює шифрування по заданому алгоритму. На виході БШ отримується зашифроване повідомлення $S_Ш$, яке подається на перший вхід блоку впровадження повідомлення у контейнер

(БВПК). Сам контейнер подається на другий вхід БВПК. В якості контейнера можуть виступати файли зображення, аудіо файли, текстові файли і т.п. БВПК по заданому закону здійснює впровадження бітів повідомлення у контейнер без зміни структури контейнера. На виході БВПК отримується стеганограма ST, яка передається по лінії зв'язку (ЛЗ) на вхід блоку витягання повідомлення з контейнеру (БВПКТ) приймальної частини. БВПКТ здійснює витягання зашифрованого повідомлення $S_Ш$, яке з його виходу подається на вхід блоку дешифрування (БДШ), який під дією ключової послідовності К дешифрує шифрограми і на його виході з'являється вихідне повідомлення S.

Ефективність функціонування такої системи залежить від вибраного алгоритму шифрування, а також від методу впровадження цифрового повідомлення у контейнер без спотворення останнього. Важливим є також вибір такого методу впровадження повідомлення у контейнер, який би дозволив здійснити впровадження як можна більшої кількості бітів.

Метод впровадження повідомлень у файли зображень, які спотворені шумом. Найрозповсюдженішим методом впровадження повідомлень є метод LSB, який реалізує впровадження у найменший значущий біт [7 – 9]. Даний метод не дає відчувати різницю між порожнім та заповненим контейнерами. Але він обмежує величину впровадженого повідомлення власним форматом. Збільшення повідомлення, впровадженого у контейнер може бути здійснене шляхом впровадження його бітів не тільки у найменші біти файлів контейнера.

Для вирішення цієї задачі пропонується вибирати контейнери у вигляді зашумлених зображень та впроваджувати біти повідомлення у пікселі, які відображають шум. Одним з таких шумів є шум «сіль» та «перець», який характеризується присутністю білих клітин на темному фоні, а також темних клітин на світлому фоні. Приклад зображення з таким шумом подано на рис. 2.

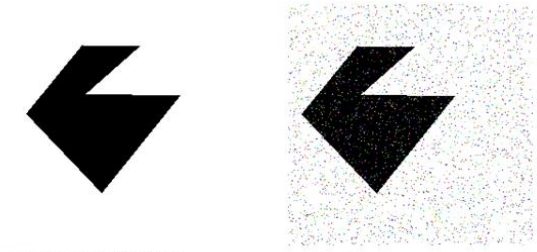
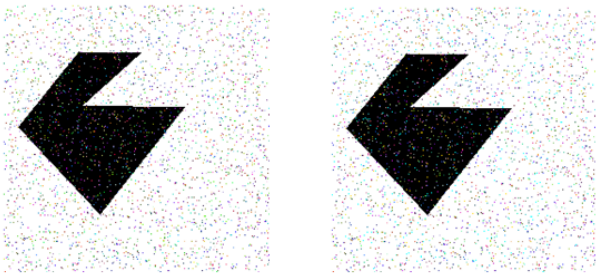


Рис. 2. **Приклад зображень, які спотворені шумом типу «сіль» та «перець»**

На рис. 2 *а* подано початкове зображення, а на рис. 2 *б* це ж зображення, яке спотворене шумом типу сіль та перець. Видно, що відтінки шумових пікселів при зміні їх яскравості, або колірності не впливає на відчуття різниці у отриманих спотворених зображеннях. Такий підхід до вибору та побудови контейнерів дозволяє збільшити об'єм впроваджуваного секретного повідомлення. Наприклад, якщо зображення містить N пікселів, які відображають шум, а все зображення складається з M пікселів, то кількість не спотворених пікселів складає $K=N-M$.

Приймемо, що у кожний неспотворений піксель записується по одному біту секретного повідомлення, а у пікселі шуму по два біти, то кількість бітів впроваджених у контейнер буде визначатись як $L_П=K+2N$. Приклад спотворених зображень, в яких шумові пікселі змінили код яскравості або кольору подані на рис. 3.

Як зображено на рис. 3 відчуття різниці не зафіксовано. Крім того, супротивник не має уяви про початкове зображення. Процес впровадження повідомлення базується на пошуку пікселів, що належать шуму. Для цього проводять попередню обробку зображення, яке вибране в якості контейнеру. Головною операцією такої обробки є виділення пікселів, які утворюють шум.



а) зображення, спотворене шумом

б) зображення, спотворене шумом, в якому зелені пікселі замінені на голубі, а червоні на оранжеві

Рис. 3. **Приклад зашумлених зображень із змінами атрибутів пікселів шуму**

Характеристикою таких пікселів є те, що вони мають у околі пікселі з іншими характеристиками, які мають досить велику різницю у кодуванні кольору та яскравості. Для їх виділення застосовуються різні види околиці сусідніх пікселів (рис. 4).

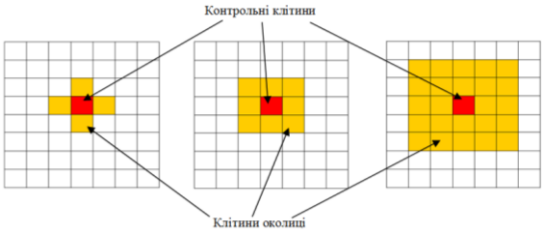


Рис. 4. **Види околиць, які можуть бути використані для визначення пікселів шуму**

Аналіз пікселів зображення здійснюється послідовним скануванням всього поля зображення за допомогою скануючого вікна із заданим кодуванням клітин (рис. 5).

X_{23}	X_{24}	X_9	X_{10}	X_{11}
X_{22}	X_8	X_1	X_2	X_{12}
X_{21}	X_7	X_0	X_3	X_{13}
X_{20}	X_6	X_5	X_4	X_{14}
X_{19}	X_{18}	X_{17}	X_{16}	X_{15}

Рис. 5. **Приклад кодування клітин скануючого вікна**

Клітина, яка кодується X_0 вибирається як контрольна клітина і виступає центром скануючого вікна. Саме контрольна клітина піддається аналізу на належність її шуму. При цьому визначається кількість сусідніх шумових клітин. Розглянемо умови, які визначають належність клітини (пікселя) шуму.

Якщо клітина фіксує шум і не є сусідньою для інших клітин шуму, то повинна виконуватись така умова

$$b_0 = \overline{(X_1 \vee X_2 \vee X_3 \vee X_4 \vee X_5 \vee X_6 \vee X_7 \vee X_8)} \wedge X_0 \vee (X_1 \wedge X_2 \wedge X_3 \wedge X_4 \wedge X_5 \wedge X_6 \wedge X_7 \wedge X_8) \wedge \overline{X_0} = 1 \quad (1)$$

Вираз (1) реалізується для бінаризованих клітин скануючого вікна. Бінаризація клітин здійснюється шляхом колірної обробки та порогової обробки по яскравості. Кожному кольору визначається порог по яскравості. Якщо яскравість клітини не перевищує поріг, то клітина кодується логічним «0», а якщо перевищує, то логічною «1».

У випадку наявності клітин шуму, які розташовані у найближчому сусідстві, умова (1) не виконується і проводиться аналіз клітин вікна наступного (3-го) порядку по даній моделі

$$b_0^1 = \overline{\left(\bigvee_{i=9}^{24} X_i \right)} \wedge X_0 \vee \left(\bigwedge_{i=9}^{24} X_i \right) \wedge \overline{X_0} = 1 \quad (2)$$

Таким чином, визначення клітин шуму, які утворюють шум в межах скануючого вікна 3×3 здійснюється за умовою (2). Обмежимося скануючим вікном розмірами 5×5 пікселів, оскільки більше групування пікселів може відображати корисну інформацію, що може призвести до реального спотворення нешумових пікселів.

Використовуючи даний метод на основі визначеного скануючого вікна дозволяє визначити та зафіксувати послідовність шумових пікселів, яка запам’ятовується і у подальшому піддається врахуванню для алгоритму розподілу бітів впроваджуваного повідомлення.

Кількість шумових пікселів у процентному співвідношенні може регулюватись спеціально розробленими програмно-апаратними засобами. Крім того, аналізуючи початкове зображення по розподілу кольорів, можна також наперед визначати пікселі, на які накладаються шумові спотворення.

Висновки. Запропонований метод використовує контейнери у вигляді файлів зображень, які піддаються спотворенням шуму типу сіль та перець. Таке спотворення контейнерів дозволяє збільшити об’єм повідомлення, що впроваджується,

який залежить від відсотку шумових пікселів, присутніх на зображенні. Даний метод потребує додаткових операцій та засобів їхньої реалізації, які націлені на аналіз зображення для пошуку шумових пікселів. Такі операції застосовуються як на приймальній, так і на передавальній частинах системи.

ЛІТЕРАТУРА

1. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях. –2 изд., перераб. и доп. – М.:Радио и связь, 2001. – 376 с.

2. *Грайворонський М. В., Новіков О. М.* Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.

3. *Андрончик А. Н.* Защита информации в компьютерных сетях. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

4. *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии и стеганографии. – 2-е изд. – М.: Горячая линия-Телеком, 2013. – 232 с.

5. *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

6. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. — М.: Солон-Пресс, 2002. – 272 с.

7. *Shilpa Gupta, Geeta Gujral and Neha Aggarwal*. Enhanced Least Significant Bit algorithm For Image Steganography.// IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 – P. 40 – 42.

8. *K.B.Raja, C. R.Chowdary, Venugopal K. R., and L. M. Patnaik*,» A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images» Department of Computer Science Engineering, Bangalore 2005 IEEE.

9. *V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P. Chenna Reddy*, «Implementation of LSB Steganography and its Evaluation for Various File Formats», Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, – 2011. – P. 868 – 872.

Stepan M. Bilan, PhD (Technical Sciences), Professor
(Professor Telecommunication Technology and AutomationChair, State University for Transport Economy and Technologies)
Oleksandr O. Kolochun
(Student of State University for Transport Economy and Technologies)

METHOD OF STEGANOGRAPHIC CONCEALING INFORMATION BASED ON MODIFIED CONTAINERS

This paper the method considers and investigated for steganography protect information based on containers that are filed image files. To increase the volume of the message that is being introduced into the container, the image lends itself to noise distortions of salt and pepper. Message bits embedded in the least significant bits of bytes of image code, and pixels that are corrupted by noise, take root into several bits, depending on the chosen threshold luminance. To implement steganographic protection are introduced additional operations that define the noise pixels by using a scanning window of specified sizes. The cells of the scanning window are encoded in a predetermined manner and their values are entered in the appropriate model for determining the membership of the cell noise. As a result of the scanning, sequence formed by cells that belong to noise. This sequence is taken into

account in the implementation of the encryption algorithm and implementation of message bits into bytes of noise pixels. At every pixel, which encodes the noise may be recorded several pixels messages that do not affect the overall contrast of the original image. The proposed method uses a container in the form of image files, which are amenable to noise distortions such as and salt and pepper. This distortion of containers can increase the volume of messages that is being implemented. This volume depends on the percentage of pixels of noise that are present in the image. This method needs the additional operations and their means of implementation that focus on the analysis of the image to search for noise pixels. Such operations are used as at the receiver and at the transmitting portions of the system.

Keywords: *image, pixel noise, steganography.*

REFERENCES

1. Romanetc U. V., Tymofeyev P. A., Shanygyn V. F. Zashita informaciy v komyuternih sysytemah I setyah.[Protection of information in computer systems and networks]. 2 izd. Pererab. I dopoln. – Moscow.: Radio I svyazy, 2001. – 376 p.

2. Grayvoronsky M. V., Novikov O. M. Bezpeka informaciyno-komunikacynih system.[Security of Information and Communication Systems]. – Kiev: Vydavnycha grupa VHU, 2009. – 608 p.

3. Andronchik A. N. Zashita informaciy v komyuternih setyah.[Protection of information in computer networks].– Ekaterinburg: UGTU-UPY, 2008. – 248 p.

4. *Ryabko B. Ya., Fionov A. N.* Osnovi sovremennoy kriptografiy b steganografiy. [Foundations of modern cryptography and steganography]. – 2-ye izd. –M.: Goryachaya liniya-Telecom, 2013.– 232 p.

5. *Konahovich G. F., Puzirenko A. U.* Kompyuternaya steganografiya. Teoriya I praktika.[Computer steganography. Theory and practice.]. – K.: MK-Press, 2006 – 288 p.

6. *Gribunin V. G., Okov I. N., Turincev I. V.* Cifrovaya steganografya. [Digital steganography]. – M.: Solon-Press, 2002. – 272 p.

7. *Shilpa Gupta, Geeta Gujral and Neha Aggarwal*. Enhanced Least Significant Bit algorithm For Image Steganography.// IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 – P. 40-42.

8. *K. B. Raja, C. R. Chowdary, Venugopal K. R., and L. M. Patnaik*,» A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images» Department of Computer Science Engineering, Bangalore 2005, IEEE.

9. V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P. Chenna Reddy. «Implementation of LSB Steganography and its Evaluation for Various File Formats», Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, – 2011. – P. 868 – 872.