УДК 004.056.5

А. А. Кобозева, д-р. техн. наук,
М. В. Ворникова,
А. Г. Шпортюк

ОСНОВЫ НОВОГО ПОДХОДА К СТЕГАНОАНАЛИЗУ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Аннотация. Предложены основы нового подхода к организации детектирования наличия вложения дополнительной информации методом модификации наименьшего значащего бита в цифровое изображение. Приведены результаты вычислительных экспериментов, подтверждающие эффективность предложенного подхода, в том числе при малой пропускной способности (менее 0.5 бит/пиксель) скрытого канала связи.

Ключевые слова: цифровое изображение, стеганоанализ, стеганометод, LSB-метод, дополнительная информация, матрица, частотная область, детектирование, пропускная способность, канал связи.

А. А. Кобозєва, д-р. техн. наук,
М. В. Ворнікова,
А. Г. Шпортюк

ОСНОВИ НОВОГО ПІДХОДУ ДО СТЕГАНОАНАЛІЗУ ЦИФРОВОГО ЗОБРАЖЕННЯ

Анотація. Запропоновано основи нового підходу до організації детектування наявності вкладення додаткової інформації методом модифікації найменшого значущого біта в цифрове зображення. Наведено результати обчислювальних експериментів, що підтверджують ефективність запропонованого підходу, у тому числі при малій пропускній спроможності (менше 0.5 біт/піксель) прихованого каналу зв'язку.се,

Ключові слова: *цифрове зображення, стеганоаналіз, стеганометод, LSB-метод, додаткова інформація, матриця, частотна область, детектування, пропускна здатність, канал зв'язку.*

A.A. Kobozeva, dr. tehn. sciences,
M.V. Vornikova,
A.G. Shportyuk

FUNDAMENTALS OF THE NEW APPROACH TO DIGITAL IMAGES OF STEGANALYSIS

Abstract. Proposed a new approach to the organization of detecting the presence of embedding additional information by modifying the least significant bit in the digital image. Given results of the computational experiments, confirming the effectiveness of the proposed approach, including at small bandwidth (less than 0.5 bit / pixel) of the hidden communication channel.

Keywords: digital image, steganoanalysis, stegometod, LSB-method, additional information, matrix, frequency domain, detection, embedded rate, communication channel.

Введение

В современном информационном пространстве значительное место занимают стеганографические методы [1-4]. Стеганографический канал связи организовывается, как правило, в канале общего пользования: скрываемое сообщение (дополнительная информация (ДИ)) встраивается в некоторый не привлекающий внимания объект – контейнер таким образом, чтобы результат этого встраивания – стеганосообщение (СС) зрительно никак не отличался от контейнера. Затем полученное СС пересылается по открытому каналу связи или хранится в полученном виде. Таким образом, при стеганографировании сам факт существования пересылаемой ДИ оказывается скрытым.

Активизация научных исследований в области стеганографии, в частности, цифровой, многочисленные публикации получаемых результатов в открытой печати дали возможность их использования различными антигосударственными элементами, цели которых связаны с дестабилизацией жизни общества. В связи с этим в настоящий момент чрезвычайно актуальным является повышение эффективности стеганоанализа (СА). Основная задача СА – выявление в информационном контенте, в качестве которого в настоящей работе рассматриваются цифровые изображения (ЦИ), скрыто передаваемой ДИ.

Наиболее широко используемым на сегодняшний день стеганографическим

методом остается метод модификации наименьшего значащего бита (LSB) [4]. Для этого существует множество причин, среди которых простота в реализации, возможность обеспечения большой пропускной способности скрытого канала связи (СПС), гарантированное обеспечение надежности восприятия формируемого СС. Для детектирования вложения ДИ методом LSB существуют многочисленные стеганоаналитические методы [5-12]. Однако, большинство из них, используя в своей основе статистические и вероятностные методы, проводят детектирование наличия ДИ, рассчитывая на значительную СПС [13-14], оказываясь недостаточно эффективными в случае СПС меньше 0.5 бит/пиксель, хотя малая СПС является характерной особенностью использования LSB-метода на сегодняшний день.

Цель статьи и постановка задач исследования

Целью работы является разработка основ стеганоаналитического подхода для детектирования наличия ДИ, вложенной методом LSB, эффективного, в том числе при малых значениях СПС (меньше 0.5 бит/пиксель).

Для достижения цели необходимо решить следующие *задачи*:

1. Определить область ЦИ (пространственную, преобразования) для проведения СА;
2. Выявить параметры ЦИ в выбранной области, наиболее чувствительные к погружению ДИ с учетом специфики формата хранения: с потерями, без потерь;
3. Выявить отличия в возмущении параметров ЦИ при первичном и вторичном стеганопреобразовании (СП).

Основная часть

Для стеганографирования могут использоваться различные области ЦИ-контейнера – пространственная, области преобразования. Чаще других для встраивания ДИ используется частотная область ЦИ [1,3,4], что обеспечивает устойчивость соответствующих алгоритмов к различным атакам. Кроме того, локализация возмущенных частотных коэффициентов при той или иной атаке на ЦИ позволяет сделать вывод о его свойствах после атаки, в частности, о степени его искажения. Многие методы обработки ЦИ также используют частотную область, в частности, один из наиболее распространенных алгоритмов сжатия с потерями – Jpeg использует область дискретного косинусного преобразования (ДКП). В связи с вышеперечисленным исследуем возможности использования области ДКП для СА.

Выделим наиболее чувствительные к малым возмущениям (происходящим в процессе СП) коэффициенты ДКП $8\times8-$ блоков матрицы ЦИ, полученных в результате ее стандартного разбиения. При этом необходимо учесть существующие различными между частотными коэффициентами ЦИ при их хранении в форматах с потерями и без потерь.

С учетом неустойчивости метода LSB к атакам против встроенного сообщения [5-8], СС целесообразно сохранять в формате без потерь. Таким образом, объектом анализа для разрабатываемого подхода будут ЦИ в формате без потерь (для определенности далее в качестве такого формата рассматривается формат Tif), при этом в качестве контейнера могут использоваться ЦИ как в формате с потерями (далее - Jpeg), так и без потерь.

Рассмотрим сначала ЦИ-контейнеры в формате без потерь. Для решения задачи 2 для таких ЦИ был проведен вычислительный эксперимент, в ходе которого в каждое из 200 Tif-изображений погружалась ДИ с различными значениями СПС (от 0.25 до 1 бит/пиксель), СС сохранялось в формате Tif, после чего его матрица и матрица отвечающего ему контейнера разбивались стандартным образом на $8\times8-$блоки, для каждого из которых строилось ДКП. Для каждого коэффициента ДКП в каждой паре соответствующих блоков находилось его относительное возмущение в результате СП. Найденные значения усреднялись для каждого конкретного коэффициента ДКП по всем блокам ЦИ. Затем аналогичное усреднение происходило по всем ЦИ, участвовавшим в вычислительном

эксперименте. Результаты описанного эксперимента, где нумерация коэффициентов ДКП в пределах блока происходила слева направо, сверху вниз, приведены на рис.1. В результате было определено, что наиболее чувствительными к операции СП являются коэффициенты ДКП, имеющие порядковые номера 25, 48, 57, 62. Ниже вектор, состоящий из наиболее чувствительных коэффициентов ДКП, обозначается v.

Рассмотрим теперь вариант Jpeg-контейнера. В этом случае при СА необходимо будет отличить оригинальное ЦИ в формате Tif (контейнер), от СС, полученного на основе Jpeg-контейнера, сохраненного в Tif. Поэтому для выявления наиболее чувствительных коэффициентов ДКП блоков в этом случае использовались изображения в форматах Tif и Jpeg. Сам эксперимент строился аналогично предыдущему. В результате эксперимента (рис.2) были установлены наиболее чувствительные коэффициенты ДКП блоков: 32,50,56,59,63, которые и составили вектор v.

При проведении СА естественным является отсутствие в распоряжении эксперта оригинального ЦИ-контейнера.

В силу этого предлагается идея проведения анализа ЦИ с использованием (повторного) внедрения в него ДИ с различной СПС в ходе экспертизы. Очевидно, что параметры ЦИ-контейнера и аналогичные параметры СС по-разному отреагируют на (повторное) внедрение ДИ.

Эти различия при их выявлении и будут основой для отделения контейнера от СС, а также, возможно, для оценки СПС, с которой проводилось первичное внедрение ДИ в контейнер.

Для подтверждения выдвинутой гипотезы был проведен вычислительный эксперимент, в ходе которого первоначально были сформированы 12 групп ЦИ: 1 - оригинальные ЦИ в формате без потерь (Tif); 2 – оригинальные ЦИ в формате с потерями (Jpeg); 3,4,5,6 – СС, сформированные на основе группы 1 методом LSB с СПС 0.25, 0.33, 0.75, 1 бит/пиксель соответственно (формат Tif); 7,8,9,10,11,12 - СС, сформированные на основе группы 2 методом LSB с СПС 0.05, 0.1, 0.25, 0.5, 0.75, 1 бит/пиксель соответственно (формат Tif).

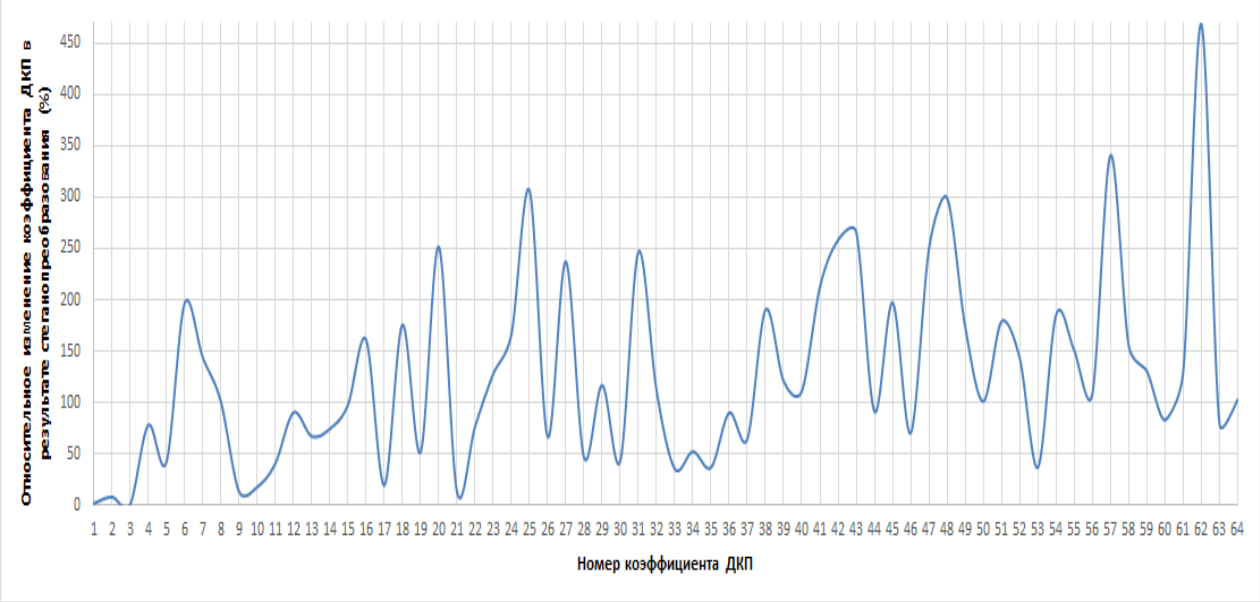

Рис.1 - Средние относительные возмущения коэффициентов ДКП 8×8 – блоков матрицы Tif-ЦИ в результате СП методом LSB со значениями СПС от 0.25 до 1 бит/пиксель (%)

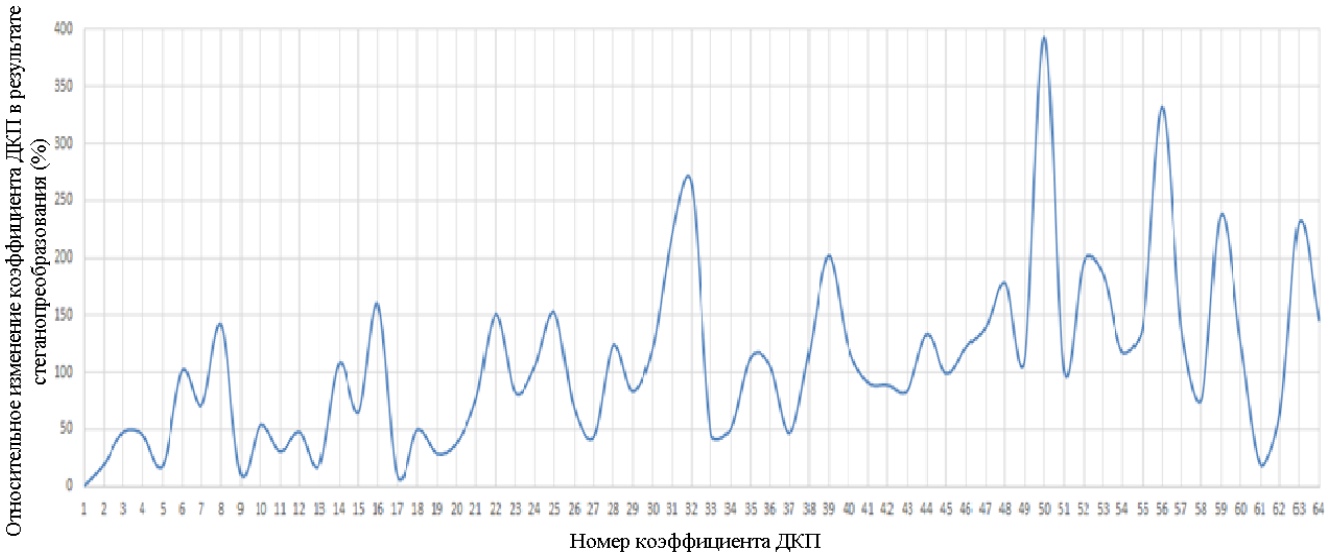

Рис.2 - Средние относительные возмущения коэффициентов ДКП 8×8 – блоков матриц Tif- и Jpeg-ЦИ в результате СП методом LSB со значениями СПС от 0.25 до 1 бит/пиксель (%)

В ходе первой части эксперимента ЦИ из групп 1,3-6 подвергались (повторному) стеганопреоразованию методом LSB с СПС 0.25, 0.33, 0.75, 1 бит/пиксель, после чего для каждой группы и каждого значения СПС. вычислялось среднее значение возмущения вектора v (с учетом его возмущения в каждой паре соответствующих блоков). Результаты приведены на рис.3.

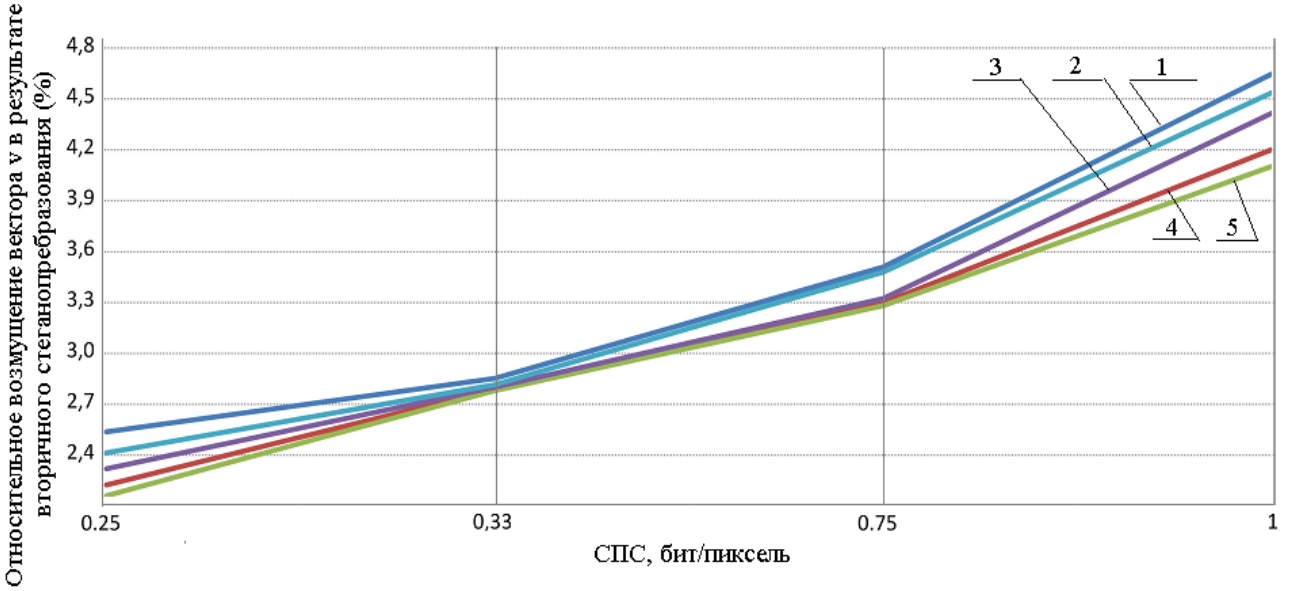

Рис.3 - Зависимость среднего значения относительного изменения вектора v при повторном внедрении ДИ для Tif-контейнеров: 1 – Tif-контейнер; 2 – СС с СПС 0.25 бит/пиксель; 3 – СС с СПС 0.33 бит/пиксель; 4 – СС с СПС 0.75 бит/пиксель; 5 – СС с СПС 1 бит/пиксель

В ходе второй части эксперимента ЦИ из групп 2,7-12 подвергались повторному стеганопреобразованию методом LSB с СПС 0.05, 0.1, 0.25, 0.5, 0.75, 1 бит/пиксель, после чего для каждой группы и каждого значения СПС вычислялось среднее значение возмущения вектора v. Результаты приведены на рис.4.

Как видно из полученных результатов, использование частотной области ЦИ принципиально позволяет отделить контейнер от СС, сформированного методом LSB, даже в случае, когда СПС меньше 0.5 бит/пиксель: при (повторном) внедрении ДИ графики зависимости относительного возмущения v от СПС, отвечающие СС и контейнеру, не пересекаются как в случае ЦИ-контейнера, хранимого без потерь, так и в случае ЦИ-контейнера, хранимого с потерями.

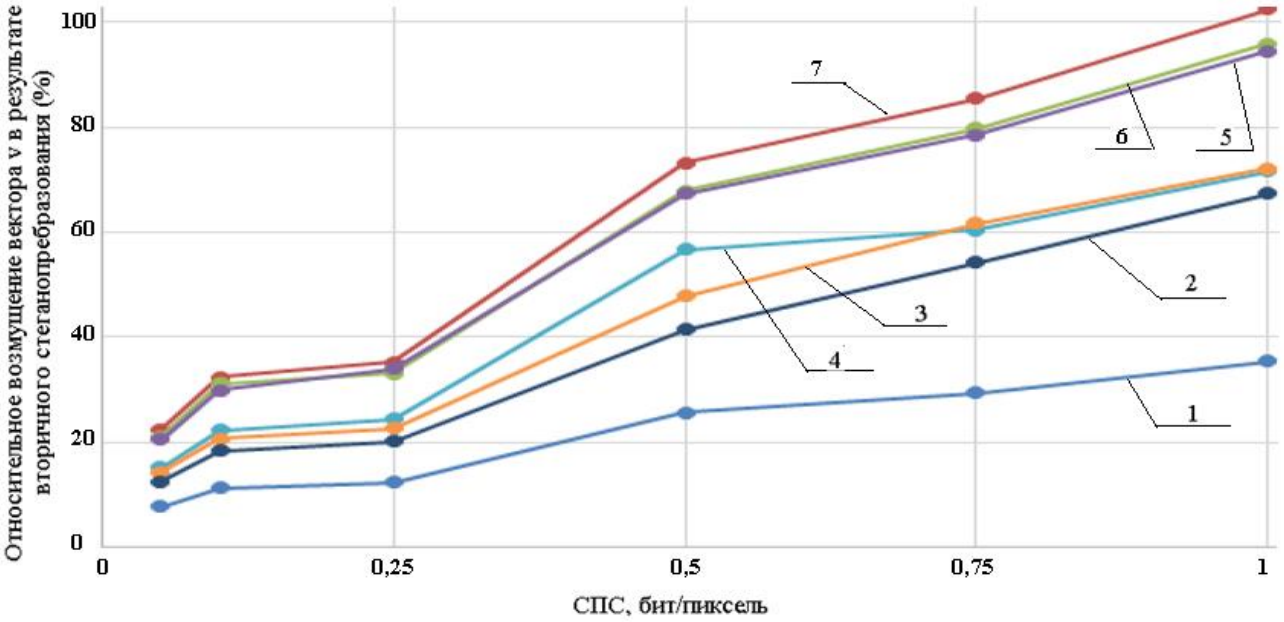

Рис.4 - Зависимость среднего значения относительного изменения вектора v при (повторном) внедрении ДИ для Jpeg-контейнеров; 1 - Tif-контейнер; 2 – СС с СПС 1 бит/пиксель; 3 – СС с СПС 0.75 бит/пиксель; 4 – СС с СПС 0.5 бит/пиксель; 5 – СС с СПС 0.25 бит/пиксель; 6 – СС с СПС 0.1 бит/пиксель; 7 – СС с СПС 0.05 бит/пиксель

Выводы

В работе предложены основы нового подхода для детектирования наличия ДИ, вложенной в ЦИ методом LSB. В качестве области анализа используется область ДКП блоков матрицы ЦИ, полученных ее стандартным разбиением. В ходе работы определены наиболее чувствительные к операции СП коэффициенты ДКП блоков, составляющие вектор v, являющийся объектом исследования. Относительные возмущения вектора v в процессе (повторного) внедрения ДИ в анализируемое ЦИ различаются по значению в случаях, когда исходное изображение являлось контейнером/СС. Установление точных количественных характеристик этого изменения даст возможность для разработки стеганоаналитического метода выявления наличия вложения ДИ в ЦИ. Более того, полученные качественные результаты говорят о потенциальной возможности использования предложенного аппарата исследования для оценки значения СПС при организации скрытого канала связи.

Список использованной литературы

1. Gkizeli M. Optimal Signature Design for Spread-Spectrum Steganography / M.Gkizeli, D.A.Pados, M.J.Medley // IEEE Trans. On Image Processing. — 2007. — Vol.16, (2). — P. 1021—1031.

2. Bergman C. Unitary embedding for data hiding with the SVD / C.Bergman, J.Davidson // Security, steganography and watermarking of multimedia contents VII, SPIE. — 2005. — Vol.5681. — P.619—630.

3. Katzenbeisser S. Information Techniques for Steganography and Digital

Watermarking / S.Katzenbeisser and F.A.P.Petitcolas. — Boston: Artech House, 2000. — 220 p.

4. Li, B. A Survey on Image Steganography and Steganalysis / B. Li, J. He, *et al.* // Journal of Information Hiding and Multimedia Signal Processing. — 2011. — Vol.2, No.2. — P.142–172.

5. Chandramouli, R. Analysis of LSB based Image Steganography Techniques / R. Chandramouli, N. Memon // Proceedings of ICIP, Thessaloniki, Greece, October 7-10, 2001. — 2001. — Vol.3. — P. 1019–1022.

6. Ker, A.D. A Weighted Stego Image Detector for Sequential LSB Replacement // Proceedings of the Third International Symposium on Information Assurance and Security, IAS 2007, August 29-31, 2007, Manchester, United Kingdom. — 2007. — P. 453–456.

7. Mitra, S. Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis / S. Mitra, T. Roy, D. Mazumdar and A.B. Saha // IIT Kanpur Hackers' Workshop 2004 (IITKHACK04), 23–24 Feb 2004, Kanpur, India. — Kanpur: Indian Institute of Technology Kanpur, 2004. — P. 23–24.

8. Bhattacharyya, S. Steganalysis of LSB Image Steganography using Multiple Regression and Auto Regressive (AR) Model // S. Bhattacharyya, G. Sanyal // International Journal of Computer Technology and Applications. — 2011. — Vol.2, Iss.4. — P. 1069–1077.

9. Gul, G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol.5, No.2. — P. 349–353.

10. Gul, G. Steganalytic Features for JPEG Compression-Based Perturbed Quantization / G. Gul, A.E. Dirik, I. Avcibas // IEEE Signal Processing Letters. — 2007. — Vol.14, Iss.3. — P. 205–208.

11. Natarajan, V. Blind Image Steganalysis Based on Contourlet Transform / V. Natarajan, R. Anitha // International Journal on Cryptography & Information Security. — 2012. — Vol.2, Iss.3. — P. 77–87.

12. Dumitrescu, S. Detection of Lsb Steganography via Sample Pair Analysis / S. Dumitrescu, X. Wu, Z. Wang // IEEE Transactions on Signal Processing. — 2003. — Vol.51, Iss.7. — P. 1995–2007.

13. StegAlyzerSS. Steganography Analyzer Signature Scanner // Backbone Security. Fairmont, WV, USA. Available at: http://www.sarc-wv.com/products/stegalyzerss/ (accessed 27.06.2012).

14. StegoHunt // WetStone Technologies. Cortland, NY, USA. Available at: http://www.wetstonetech.com/product/stegohunt/ (accessed 27.06.2012).

Получено 28.04.2016

Кобозева Алла Анатольевна
д-р техн наук, зав. кафедры ИУЗИС, ОНПУ,
проспект Шевченко, 1
+380953901845,
alla_kobozeva@ukr.net

Ворникова Мария Витальевна
студентка, ОНПУ,
проспект Шевченко, 1
+380688835219
vornikovamaha@gmail.com

Шпортюк Анастасия Геннадьевна
студентка,
ОНПУ, проспект Шевченко, 1
+380939826013,
nanami2995@gmail.com