Математические структуры и моделирование 2018. № 2(46). С. 157–166

УДК 004.056
DOI: 10.25513/2222-8772.2018.2.157-166

МЕТОД ПРИМЕНЕНИЯ (T, N) — ПОРОГОВОЙ СХЕМЫ В СТЕГАНОГАФИИ

А.Н. Мироненко
к.т.н., доцент, e-mail: mironim84@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Работа посвящена разработке метода скрытия информации в растровом изображении с использованием стеганографии совместно с криптографией. Предлагаемый метод позволяет решить проблему восстановления сообщения, если изображение, содержащее скрытые данные, было повреждено. Основная идея заключается в том, что данные с помощью стеганографии помещаются в изображение не целиком, а с использованием (t, n) — пороговой схемы, вставки каждой из частей происходит независимо. Разработано программное обеспечение для апробации предлагаемого метода. Проведена серия экспериментов, подтверждающих возможность применения предложенного метода.

Ключевые слова: схема разделения секрета, стеганография, LSB, схема Шамира.

Введение

Важным является вопрос сохранения и обеспечения конфиденциальности информации. С помощью специализированного программного обеспечения можно обеспечить надёжную передачу данных, зашифровав их. Однако в случае, когда злоумышленник не способен расшифровать данные, он может нарушить их целостность. Решением этой проблемы может быть использование стеганографии, т. е. сокрытие самого факта передачи секретной информации. Этой теме посвящено много научных работ, например [1–4]. В статье [5] рассмотрены основные тенденции в стеганографии.

В работе [6] описывается разработка защищённой системы передачи данных. Идея системы состоит в использовании на платформе Android двух криптографических алгоритмов: RSA и AES, совместно с LSB для реализации стеганографии. Объединение этих трёх алгоритмов позволяет создать защищённую систему связи на платформе Android.

В [7] предлагается стеганографическая система защиты информации на основе предлагаемого оригинального алгоритма для встраивания информации с перекрывающимися блоками изображений в строках и столбцах. Показано, что эта стеганографическая система сохраняет устойчивость к пассивным стегоаналитическим атакам с перекрытием блоков до 24×24 пикселей, и при этом

значение перекрытия более стабильно, чем стандартный и улучшенный метод стеганографии, основанный на прямом распространении спектра.

В статье [8] автор предлагает стеганографический алгоритм, использующий пару ключей: открытый и закрытый, чтобы генерировать псевдослучайную последовательность, которая указывает, где будет храниться секретная информация. Перед вставкой сообщения изображение претерпевает несколько преобразований. Для извлечения информация преобразования применяются в обратном порядке. В стеганографии можно выделить несколько проблем:

- обнаружение стеганографической вставки (стегоанализ);
- надёжность сокрытия информации при её передаче.

Решению первой проблемы посвящена работа [9]. Решение второй проблемы предлагается в [10], в этой работе основное внимание уделяется интеграционным схемам, таким как OFDM, CDMA и MC-CDMA, со стеганографией и методами шифрования изображений для создания беспроводных систем со встроенной функцией обеспечения безопасности. В статье [11] авторы рассматривают метод унификации криптографии и стеганографии. Эта работа также посвящена проблеме повышения надёжности скрытия информации при её передаче, т. е. решению задачи восстановления информации в случае повреждения изображения, содержащего скрытые данные. Рассмотрим возможность комбинирования стеганографического метода и (t,n)–пороговой схемы. Кроме того, проведём анализ существующих алгоритмов стеганографии и пороговых схем.

1. Постановка проблемы и её решение

Проведём анализ существующих методов стеганографии и выберем наиболее подходящий. Рассмотрим алгоритмы для встраивания информации в часть исходного изображения. Преимуществом этих алгоритмов является то, что для внедрения не нужно выполнять сложные линейные преобразования изображения. Информация внедряется путём манипуляции с яркостью или цветовыми компонентами изображения.

1. Алгоритм Каттера. В этом алгоритме информация будет встраиваться в канал синего цвета, т. к. изменения этого цвета наименее заметны для человеческого глаза. В изображении выбирается псевдослучайная позиция, в которую будет вставлена информация и далее — в канал синего цвета. Информация вносится путём изменения яркости. В работе [12] рассматривается возможность использования стеганографического метода Kutter–Jordan–Bossen, позволяющего скрыть информацию о видеопоследовательности. Кроме того, в работе предлагается критерий выбора изображения контейнера.

2. Алгоритм Лангелаара. Этот алгоритм работает с блоками размером 8x8 пикселей от исходного изображения. Первоначально создаётся псевдослучайная маска размером 8x8 пикселей, состоящая из нулей и единиц. На первом этапе каждый блок делится на пару подблоков в зависимости от значения маски. Затем для каждого из них вычисляется среднее значение яркости. На втором этапе выбирается произвольный порог, затем биты встраиваются следующим образом: 1 записывается, если разница между средними значениями

яркости больше, чем выбранный порог; 0 записывается, если разница между средними значениями яркости меньше выбранного порога. Если это условие не выполняется, изменения будут происходить в значениях пикселей второго субблока.

3. Алгоритм Ронгена. Встраиваемая информация представляется в виде двумерной матрицы, состоящей в равных частях из единиц и нулей. На основе некоторой характеристической функции, вычисленной локально в процессе анализа соседних пикселей, определяются те пиксели, в которые может быть встроена информация. Количество этих пикселей составляет около 0,01 от общего числа, поэтому не все единицы будут внедрены в эти пиксели. Чтобы увеличить количество этих пикселей, первоначально предлагаем осуществлять незначительное искажение изображения.

4. Встраивание в наименее значащие биты (LSB). Суть этого метода заключается в том, что наименее значащие биты изображения несут в себе наименьшую информацию. Когда они заменяются на биты скрываемого сообщения, отличие получившегося изображение от исходного практически незаметно человеческому глазу. Этот метод позволяет встраивать большие объёмы информации, что является значительным плюсом, кроме того, он легко реализуем [13–15]. После анализа известных методов сокрытия данных в растровых изображениях и изучения работ [16, 17] для решения поставленной задачи был выбран метод LSB.

Проанализируем существующие пороговые схемы.

1. Пороговая схема Шамиром [18]. Пусть задано конечное поле G. Фиксируем n разных ненулевых несекретных элементов этого поля. Каждый из этих элементов присваивается определённому члену группы. Далее берём произвольное множество t элементов поля G, из них строим многочлен $f(x)$ степени $t-1$, $1 < t \leqslant n$ над полем G. Получив многочлен, вычисляем его значение в несекретных точках и сообщаем результаты соответствующим членам группы. Чтобы восстановить секрет, можно использовать формулу интерполяции, например формулу Лагранжа.

2. Схема Блэкли. Секрет, который должны быть разделён в схеме Блэкли, является одной из координат точки в m-мерном пространстве. Доли секретов, распределённых между сторонам, являются уравнениями $(m-1)$–мерных гиперплоскостей. Чтобы восстановить точку, необходимо знать m уравнений гиперплоскостей.

3. Секретное разделение с использованием китайской теоремы об остатках (схема Миньотта, схема Асмута–Блума). Для некоторого числа (по схеме Миньотта это сам секрет, в схеме Асмута–Блума — некоторое производное число), рассчитываются остатки от деления на последовательность чисел, которые разделены между сторонами. Из-за ограничений на последовательность чисел только определённое количество сторон может восстановить секрет. Для дальнейшего анализа были выбраны две схемы: 1 и 3. Схема Блэкли не была включена в анализ, потому что она менее эффективна, чем схема Шамира: по схеме Шамира каждая доля такого же размера, как секрет, а по схеме Блэкли каждая доля в несколько раз больше. Результаты сравнения схем представлены

в таблицах 1 2. Была выбрана схема Шамира.

Таблица 1. Схема Шамира

Критерий сравнения	$t = 5$, $n = 3$, $\|M\| = 512$	$t = n = 32$, $\|M\| = 512$	$t = n = 128$, $\|M\| = 512$
Время разделения	5 мс	7 мс	75 мс
Время восстановления	1 мс	2 мс	27 мс
Объём требуемой памяти	1560 байт	6720 байт	100608 байт

Таблица 2. Схема Асмута–Блума

Критерий сравнения	$t = 5$, $n = 3$, $\|M\| = 512$	$t = n = 32$, $\|M\| = 512$	$t = n = 128$, $\|M\| = 512$
Время разделения	130 мс	145 мс	3032 мс
Время восстановления	1 мс	4 мс	97 мс
Объём требуемой памяти	3456 байт	274432 байт	4243456 байт

Идея предлагаемого в данной работе метода заключается в объединении стеганографического метода LSB с (t, n)–пороговой схемой, что позволяет при повреждении стегоконтейнера на $n - t$ частей, где $t \leqslant n$ и n — это общее количество долей секрета, а t — минимально необходимое количество долей секрета для его успешного восстановления, всё равно обеспечить надёжное восстановление секрета. Предлагаемый подход можно описать в два этапа:

- встраивание информации в изображение–контейнер, рис. 1;
- восстановление информации рис. 2.

Встраиваемая информация обрабатывается в соответствии с выбранной (t, n)–пороговой схемой, т. е. формируются доли секрета. Исходное изображение, в которое будет осуществляться вставка, делится на n частей (блоков) по ширине, в соответствии с (t, n)–пороговой схемой, используемой для формирования долей секрета. Каждая из полученных частей рассматривается как независимое изображение. Изображение представлено в виде массива бит, в котором для кодирования каждого цвета пикселя используется 8 бит. Секрет записывается внесением изменения в младшие разряды. В первый пиксель изображения пишем длину части секрета, а в последующие — саму часть секрета. Такие изменения произойдут со всеми n блоками. После завершения процедуры встраивания изображений контейнер формируется из n частей, которые уже содержат доли секрета. Чтобы извлечь информацию, необходимо знать количество частей, на которые было разделено исходное изображение, и

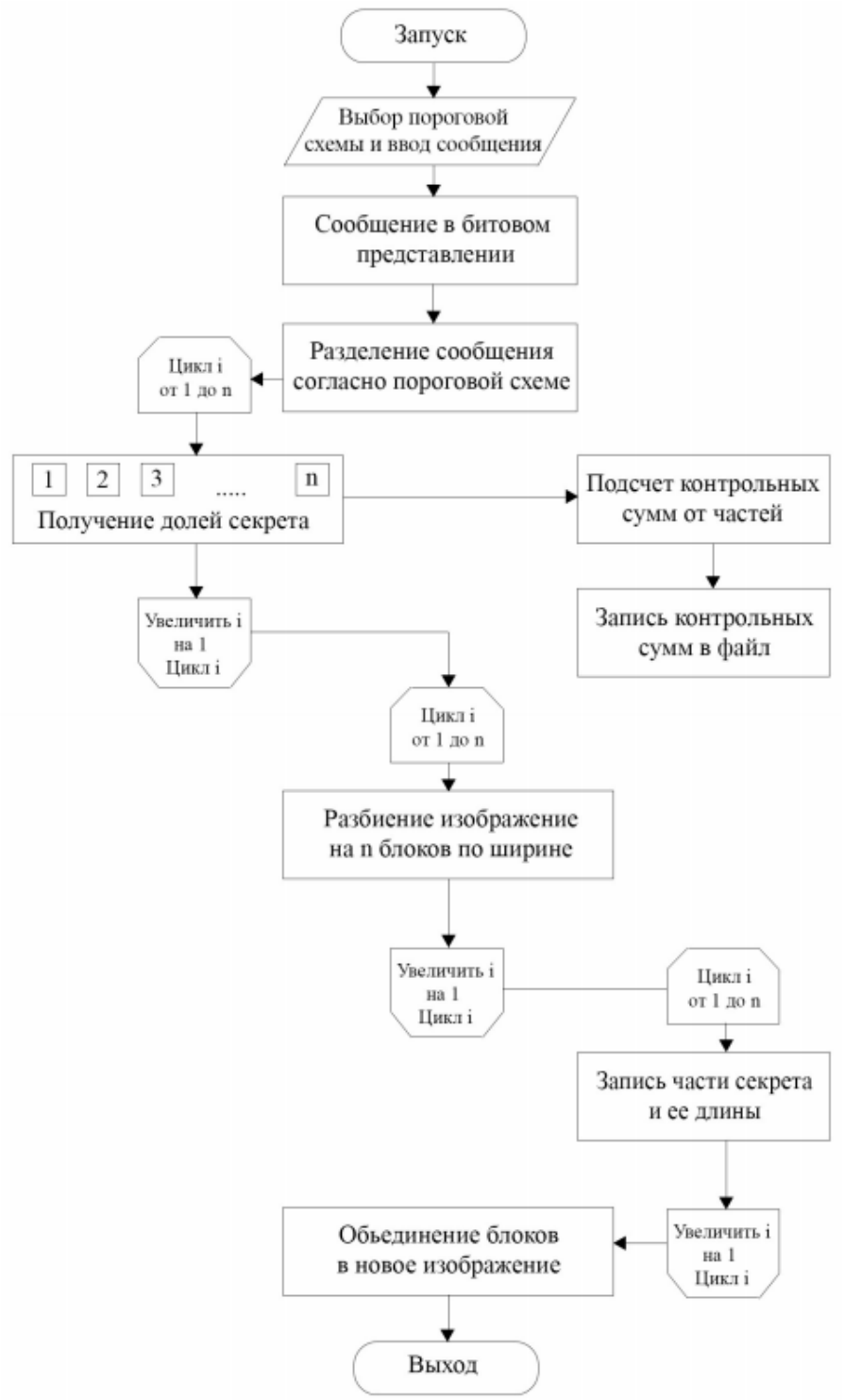

Рис. 1. Блок-схемы встраивания информации

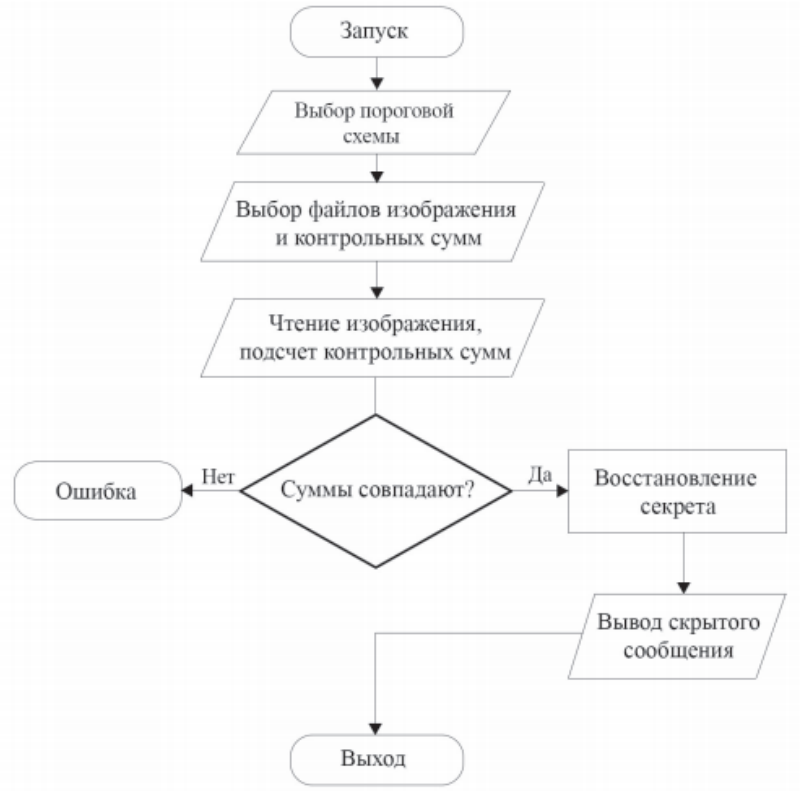

Рис. 2. Блок-схема работы алгоритма восстановления секрета

его длину. Затем из каждой части изображения-контейнера считывается первый пиксель и проверяется наличие записи длины секретной части скрытого сообщения. Если такая информация присутствует, то доля секрета считывается. Затем проверяются контрольные суммы. Они будут подсчитываться снова от каждой части изображения и будут сравниваться с теми, которые были записаны в файле. В случае их совпадения доля тайны будет записана в массив, который будет передан на вход функции восстановления секрета.

2. Апробация

Для апробации предложенного метода была реализована программа на языке C#. Блок-схемы работы программы представлены на рис. 3.

Был проведён ряд экспериментов. Для большей вероятности восстановления тайны лучше всего выбрать как можно меньше t и как можно больше n. На изображение-стегоконтейнер наносились следующие повреждения: наложение «шума», вырезание части картинки, наложение посторонних изображений. В случаях, когда изображение повреждалось путём вырезания его части или наложением посторонних изображений, эксперименты проходили удачно,

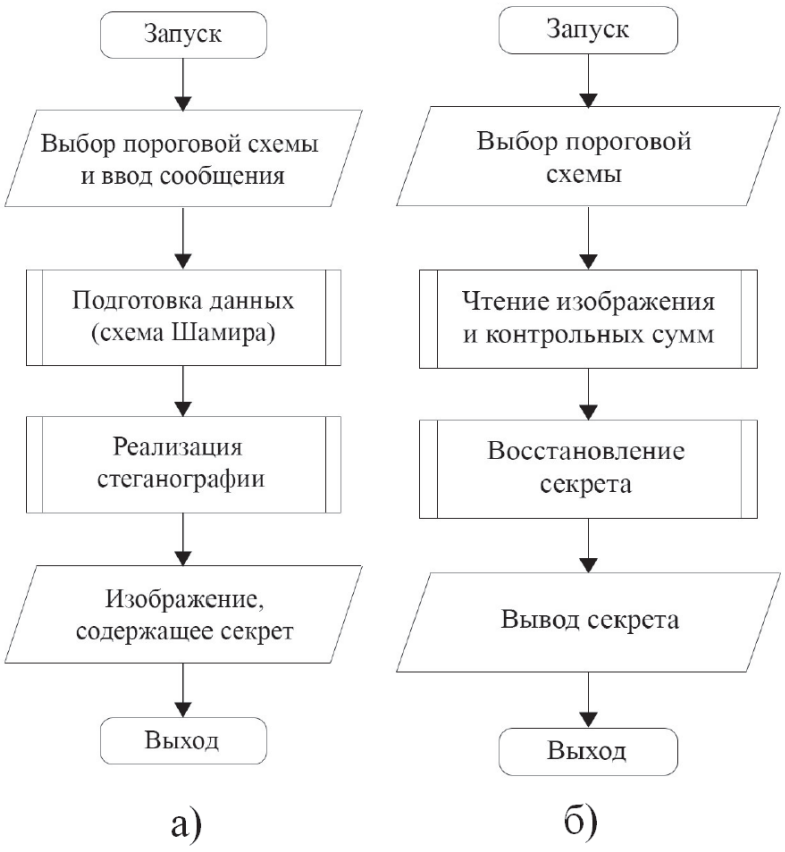

Рис. 3. Блок-схема работы программы: а) разделение секрета, б) восстановление секрета

т. е. изображение восстанавливалось при повреждении менее 60 % контейнера. Результат экспериментов, когда повреждение производилось путём нанесения «шума», представлен в таблице 3, где «+» — восстановить информацию удалось, «—» — восстановить информацию не удалось.

Таблица 3. Результаты эксперимента для различных значений t и n пороговой схемы

Уровень «шума» (%)	$t = 3$, $n = 10$	$t = 6$, $n = 10$	$t = 8$, $n = 10$	$t = 10$, $n = 10$
0,05	+	+	+	+
0,10	+	+	+	+
0,15 — 0,19	+	+	+	+
0,2	—	—	—	—

Значительно улучшить результаты можно путём выбора долей для восстановления информации по определённому алгоритму. Задача поиска алгоритма

выбора долей не ставилась в данной работе. Необходимо было проверить гипотезу о возможности объединения стеганографического метода LSB с (t, n)–пороговой схемой. Поиск алгоритма выбора долей может являться направлением последующих работ по данной теме.

3. Выводы

В работе был предложен метод объединения стеганографического метода LSB и (t, n)–пороговой схемы. Проведён анализ стеганографических методов и пороговых схем. Разработано программное обеспечение, проведена апробация. В ходе экспериментов было определено, что:

- в случае повреждения стегоконтейнера наложением постороннего изображения или путём удаления части изображения-стегоконтейнера порог успешного восстановления встраиваемой информации 60 %;
- в случае повреждения стегоконтейнера наложением «шума» порог успешного восстановления 0,19 %.

В целом можно говорить о возможности применения предлагаемого метода для повышения надёжности сокрытия информации при её передаче или порче стегоконтейнера.

Литература

1. Al-Afandy K., Faragallah O., Elmhalawy A. High security data hiding using image cropping and LSB least significant bit steganography // Information Science and Technology (CiSt). 4-th IEEE International Colloquium. 24–26 Oct., 2016. DOI: https://doi.org/10.1109/CIST.2016.7805079.
2. Chitradevi B., Thinaharan N., Vasanthi M. Data Hiding Using Least Significant Bit Steganography in Digital Images. 2017. DOI: http://doi.org/10.5281/zenodo.262996
3. Al-Dmour H., Al-Ani A., Nguyen H. An efficient steganography method for hiding patient confidential information // Conf Proc IEEE Eng Med Biol Soc. 2014. DOI: https://doi.org/10.1109/EMBC.2014.6943569.
4. Kaur S., Bansal S., Bansal R.K. Steganography and classification of image steganography techniques // Computing for Sustainable Global Development (INDIACom). International Conference. 5–7 March, 2014. DOI: https://doi.org/10.1109/IndiaCom.2014.6828087.
5. Zielinska E., Mazurczyk W., Szczypiorski K. Trends in Steganography // Communications of the ACM. 2014. No. 03, issue 57. P. 86–95. DOI: http://dx.doi.org/10.1145/2566590.2566610.
6. Kandul A., More A., Davalbhakta O., Artamwar R., Kulkarni D. Steganography with Cryptography in Android // Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Advances in Intelligent Systems and Computing. V. 328. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-12012-6_7.
7. Baltaev R.H., Lunegov I.V. Algoritm vstraivanija i izvlechenija informacii v nepodvizhnye cifrovye izobrazhenija stojkij k passivnym stegoanaliticheskim atakam

// Voprosy bezopasnosti. 2016. No. 6. P. 24–35. DOI: https://doi.org/10.7256/2409-7543.2016.6.21252. Available at: http://e-notabene.ru/nb/article_21252.html (accessed 10 January 2018).

8. Soria-Lorente A., Berres S. A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information // Security and Communication Networks. 2017. Article ID 5397082. 14 p. DOI: https://doi.org/10.1155/2017/5397082.
9. Belim S V., Vilkhovskiy D.E. Usage of analytic hierarchy process for steganographic inserts detection in images // Dynamics of Systems, Mechanisms and Machines (Dynamics). 2016. 15–17 Nov., 2016. DOI: https://doi.org/10.1109/Dynamics.2016.7818977.
10. Praveenkumar P., Thenmozhi K., Rayappan J.B.B., Amirtharajan R. Inbuilt Image Encryption and Steganography Security Solutions for Wireless Systems: A Survey // Research Journal of Information Technology. 2017. No. 9. P. 46–63. DOI: http://dx.doi.org/10.3923/rjit.2017.46.63.
11. Praveenkumar P., Thenmozhi K., Rayappan J.B.B., Amirtharajan R. Cryptic Cover for Covered Writing: A Pre-Layered Stego // Information Technology Journal. 2014. No. 13. P. 2524–2533. DOI: http://dx.doi.org/10.3923/itj.2014.2524.2533.
12. Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganographic algorithm in video sequences // Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE Conference of Russian. 1-3 Feb., 2017. DOI: https://doi.org/10.1109/EIConRus.2017.7910651.
13. Zeeshan M., Ullah S., Anayat S., Hussain R.G., Nasir N. A Review Study on Unique Way of Information Hiding: Steganography // International Journal on Data Science and Technology. 2017. V. 3, No. 5. P. 45–51. DOI: http://dx.doi.org/10.11648/j.ijdst.20170305.11.
14. Thangadurai K., Sudha D.G. An analysis of LSB based image steganography techniques // Computer Communication and Informatics (ICCCI). International Conference. 3-5 Jan., 2014. DOI: https://doi.org/10.1109/ICCCI.2014.6921751.
15. Liu J., Tian Y., Han T. et al. Stego key searching for LSB steganography on JPEG decompressed image // Sci. China Inf. Sci. 2016. No. 59. P. 32105. DOI: https://doi.org/10.1007/s11432-015-5367-x.
16. Fkirin A, Attiya G., El-Sayed A. Steganography Literature Survey, Classification and Comparative Study // Communications on Applied Electronics. 2016. No. 5(10). P. 13-22. DOI: https://doi.org/10.5120/cae2016652384.
17. Wiseman S.R. Defenders Guide to Steganography // Deep Secure Technical Report DS-2017-2. DOI: https://doi.org/10.13140/rg.2.2.21608.98561.
18. Luo P, Yu-Lun L.A., Wang Z. Hardware Implementation of Secure Shamir's Secret Sharing Scheme // High-Assurance Systems Engineering (HASE). IEEE 15th International Symposium. 9–11 Jan., 2014. DOI: https://doi.org/10.1109/HASE.2014.34.

THE METHOD OF APPLYING (T, N) — THRESHOLD SCHEME IN STEGANOGRAPHY

A.N. Mironenko
Ph.D. (Eng.), Associate Professor, e-mail: mironim84@mail.ru

Faculty of Computer Sciences, Dostoevsky Omsk State University, Omsk, Russia

Abstract. The work is devoted to the development of the method of information concealment in a raster image using steganography together with cryptography. The suggested method allows to solve the problem of message recovery if the image containing the hidden data was damaged. The basic idea is that the data with the help of steganography is not placed in the image entirely, but using the (t, n) — threshold scheme, the insertion of each part occurs independently. A software has been developed to test the proposed method. A series of experiments confirming the possibility of applying the proposed method is carried out.

Keywords: Threshold scheme, steganography, LSB, Shamir's secret sharing.

Дата поступления в редакцию: 03.05.2018