УДК 621.397 Вестник УрФО № 3(49) / 2023, с. 90–95

Щеголихин И.С., Жердев Д.А., Коновалов М.В. DOI: 10.14529/secur230309

РАЗРАБОТКА СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ, ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ ВНУТРИ ИЗОБРАЖЕНИЯ С АДДИТИВНОЙ ЦВЕТОВОЙ МОДЕЛЬЮ

Стеганография стремительно развивается в последние десятилетия, т.к. все чаще они находит своё применение в области защиты информации при её передаче по ненадежным каналам и при внедрении цифровых подписей [1]. Сей факт в свою очередь порождает множество стеганографических методов, которые провоцируют развитие стегоанализа, предназначенного для поиска сокрытого сообщения в стеганоконтейнере без знания стегоключа. Современные методы стеганографии, стойкие к стегоанализу, в большинстве своём базируются на псевдослучайных последовательностях [2], которые в свою очередь накладывают определенные требования и ограничения на стегосистему и средства вычислительной техники. Целью данной статьи является разработка стеганографического метода, который не использует случайные величины и их аналоги.

Ключевые слова: *информация, безопасность, стеганография, RGB, корреляция, изображение.*

DEVELOPMENT OF A STEGANOGRAPHIC METHOD OF INFORMATION PROTECTION, FOR THE TRANSFER OF INFORMATION WITHIN AN IMAGE WITH AN ADDITIVE COLOR MODEL

Steganography has developed rapidly in recent decades, as it is increasingly used in the field of information protection in its transmission over unreliable channels and in the implementation of digital signatures [1]. This fact in turn gives rise to many steganographic methods, which provoke the development of stegoanalysis, designed to find a hidden message in a stego–container without knowledge of the stego–key. Modern steganography methods resistant to stegoanalysis are mostly based on pseudorandom sequences [2], which in turn impose certain requirements and limitations on the stego system and computing facilities. The purpose of this paper is to develop a steganographic method, which does not use random variables and their analogs.

Keywords: *information, security, steganography, RGB, correlation, image.*

На сегодняшний день увеличение мощностей вычислительной техники влечет за собой необходимость развития ряда областей знаний, в том числе и стеганографии. Это не могло не отразиться на прикладных задачах, которые решает эта дисциплина.

Большинство стегостойких стеганографических методов полагаются на распределении информации не по всему стегоконтейнеру, а лишь по некоторым его частям [3]. Для решения задачи о выборе места сокрытия информации в этом стегоконтейнере зачастую специалисты выбирают псевдослучайные последовательности и/или функции их порождающие. В связи с этим возникает ряд требований к техническим средствам, реализующим подобные стеганографические методы, что в некоторых случаях влечет за собой поиск альтернатив.

Разработка стеганографического метода, предоставляющего возможность защититься от поиска по известным паттернам и ряда способов стегоанализа и является целью данной работы. Таковой метод может использоваться на равных с существующими в целях, например, добавления цифровых водяных знаков [4], защиты конфиденциальности информации и/или подтверждении её целостности.

В качестве контейнера для скрываемой информации было выбрано изображение, использующее аддитивную цветовую модель. Выбор основан на популярности подобных файлов как в сети интернет, так и в локальных вычислительных сетях.

Далее приводится описания необходимого мат аппарата, затем приведен пример конкретного алгоритма на основе полученных результатов применительно к RGB изображениям. После описания алгоритма следует конкретный пример сокрытия информации при помощи предложенного алгоритма.

Пусть X – двумерная матрица размера m на n, тогда X_{ij}, есть элемент этой матрицы рас-

положенный в i–ой строке в j–ом столбце, $i = \overline{1 \dots n}, j = \overline{1 \dots m}$ $X_{i,j}$.

Под блоком размером m^- на n^- матрицы X понимается множество её элементов $X_{i,\ j}$, $i = \overline{1 \dots n^-}, j = \overline{1 \dots m^-}$.

Пусть A – матрица размерности m на n. Также пусть k, l, h, w $\in \mathbb{N}$, удовлетворяющие следующему соотношению:

$$(\text{НОД}\left(\frac{m}{w}, k\right) = 1 \wedge \text{НОД}\left(\frac{n}{h}, k\right) = 1 \wedge \frac{m}{w} \in \mathbb{N} \wedge \frac{n}{h} \in \mathbb{N}). \quad (1)$$

Пусть $m_1 = \frac{m}{w}$ и $n_1 = \frac{n}{h}$. Сами числа h и w задают размер блока, который будет выделяться из матрицы A.

Если рассмотреть две последовательности:

$$r_i = (i * k) mod m_1, t_i = ((i-1) * l) mod n_1, i = \overline{1 \dots n_1}, \quad (2)$$

то соответствующие им пары (r_i, t_i), $i = \overline{1 \dots n_1}$ для заданных чисел k и l будут расположены в определенном порядке (считается, что $i > j \Longrightarrow$ (r_i, t_i) следует за (r_j, t_j)), который зависит от самих этих чисел [5]. Кроме того, при необходимости можно воспользоваться тем фактом, что

$$(k * i) mod m_1 = x \iff i = \left(x m_1^{|}\right) mod m_1, \quad (3)$$

где $m_1^{|}$ число, удовлетворяющее следующему равенству:

$$m_1^{|} * m1 + k^{|} * k = 1. \quad (4)$$

В силу сделанных допущений (1) такое число всегда существует [5]. Из (3) и (4) можно получить необходимые и достаточные условия для существования определенного порядка следования чисел в любой из последовательностей из равенств (2):

$$\begin{cases} kmodm_1 = a_1 * 1^{|} mod m_1 \\ kmodm_1 = a_2 * 2^{|} mod m_1 \\ \dots \\ kmodm_1 = a_{m-1} * (m-1)^{|} mod m_1 \end{cases},$$

где $a_i \in \mathbb{N} \wedge 1 \leq a_i \leq m-1 \wedge i \neq j \Longrightarrow a_i \neq a_j$.

Пусть f – функция, которая ставит в соответствие паре (r_i, t_i) множество элементов $A_{u,v}$, где $u = \overline{w * r_t \dots w * (r_t + 1)}, v = \overline{h * t_t \dots h * (t_t + 1)}$, тогда полученное множество f(i, j) будет блоком матрицы A, соответствующим паре (i, j) [6].

Пример: Случай для матрицы A, которая имеет размер 10 на 8, k = 11, l = 17, h = 2, w = 2 показан на рис. 1. В пункте б) отображены все упорядоченные пары $(i, j), i = \overline{1 \dots n_1} j = \overline{1 \dots m}$ в виде квадратов. Черным цветом выделены упорядоченные пары $(r_i, t_i), i = \overline{1 \dots n_1}$. Для матрицы A черным цветом показаны блоки $f(r_i, t_i), i = \overline{1 \dots n_1}$ т.е. группы элементов размерности w на h [7]. Элементы последовательностей (2) равны соответственно 3, 2, 1, 0 и 0, 2, 4, 1, что дает следующие пары (3,0), (2,2), (1,4), (0,1).

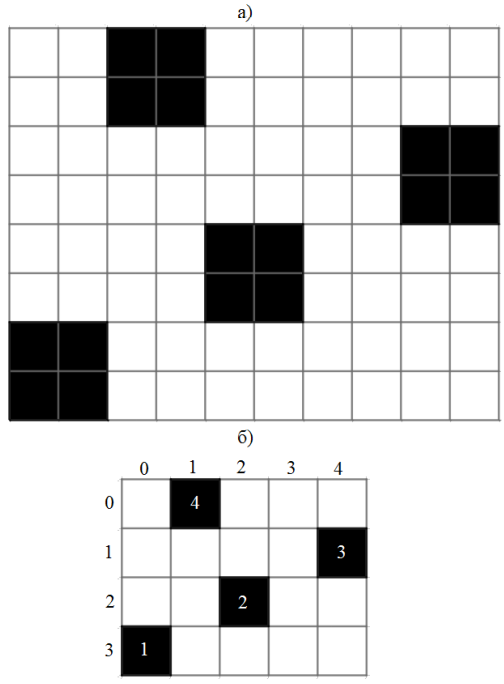

Рис. 1. а) Графическое изображение матрицы A; б) графическое изображение упорядоченных пар

Общее количество блоков элементов матрицы A = $m_1 * n_1$. Количество элементов матрицы, в которые записывается информация = n * w. Таким образом процент заполнения для данного метода = $\frac{w}{m} * 100\%$. Числа w, h, k, l являются стегоключом.

Полученный мат. аппарат можно применить для сокрытия информации в RGB изо-

бражении, например, формата PNG или JPG следующим образом:

1) открыть исходное изображение A шириной m и высотой n пикселей для внесения изменения в пиксели;

2) задать числа k, l, h, w, удовлетворяющие соотношению (1);

3) перевести сообщение в нижний регистр и удалить пробельные символы и знаки препинания;

4) разделить информационное сообщения на подстроки длинной w * h и обозначить эти подстроки d_i;

5) если количество подстрок D получилось меньше чем n_1, то добавить n_1 – D подстрок длинной w * h, состоящих из пробельных символов;

6) получить n_1 пар (r_i, t_i) из последовательностей (2);

7) для каждой пары из пункта 5 в порядке возрастания аргумента i записать сообщения d_i в блок f (r_i, t_i).

Считывание информационного сообщения происходит аналогично записи.

Шаг 7 может быть реализован следующим образом:

1) выбрать первый символ из сообщения d_i;

2) выбрать крайний левый пиксель блока (с наименьшими координатами);

3) закодировать выбранный символ в 5 битный код (заменив букву е на е);

4) записать в младшие разряды компонент RGB выбранного пикселя 1, 2 и 2 бита закодированного символа соответственно;

5) если символ сообщения d_i; не был последним, то выбрать следующий символ из d_i; иначе заполнение завершено;

6) если выбранный пиксель не является последним в строке, то выбрать следующий за ним пиксель, иначе выбрать первый пиксель следующей строки и перейти к шагу 3.

Не зная стегоключа невозможно выделить блоки, содержащие часть информационного сообщения, т.к. в зависимости от изображения, возможна ситуация, когда блок, который не содержит скрытой информации может показаться содержащим эту информацию (по аналогии с Шифром Вернама [8]) т.е. при стегоанализе нельзя быть уверенным в том, что блоки выбраны верно, кроме того неизвестен их размер (т.к. он является частью стегоключа), что также усложняет задачу перебора.

Результат работы алгоритма для m = 360, n = 256, w = h = 8, k = 13 и l = 41 показан на рис. 2. На изображении б) показаны красным цветом блоки пикселей, в которые будет производиться запись информационного сообщения. Изображение в) содержит в себе информационное сообщение, состоящее из 256 символов.

Человеческий глаз не сможет отличить изображение с информационным сообщени-

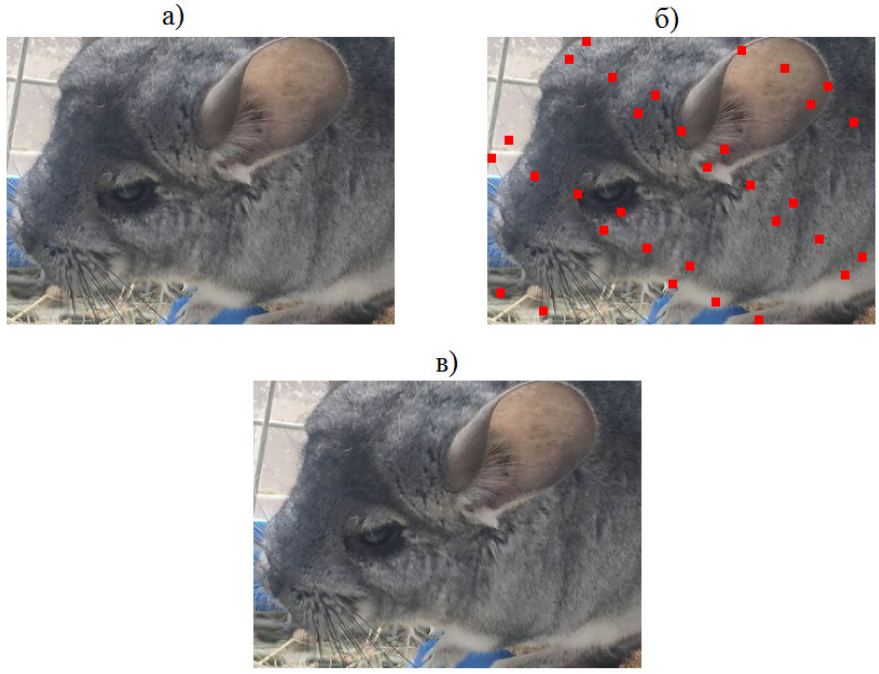

Рис. 2. а) Исходное изображение; б) Блоки пикселей на исходном изображении; в) Результирующее изображение

ем от оригинала [2], т.к. абсолютная погрешность для RGB компонент равняется самое большее 3 единицам, а максимальное значение относительной погрешности ≈ 1.8%. Рассмотренный алгоритм возможно адаптировать под любую аддитивную цветовую модель. Изменения затронут лишь шаги записи информации в компоненты основных цветов, для этого может потребоваться изменить способ кодирования символов информационного сообщения.

Для полученных изображений можно рассчитать коэффициенты диагональной, вертикальной и горизонтальной корреляции [9], которые показывают зависимость между соседними пикселями.

$$r_{XY} = \frac{\sum_{i=1}^{P}((x_i-\bar{X})(y_i-\bar{X}))}{\sum_{i=1}^{P}(x_i-\bar{X})^2},$$

где x_i – яркость текущего пиксела i, y_i – яркость соседнего по вертикали, диагонали или горизонтали пиксела по отношению к пикселу i, $\bar{X}$ – средняя яркость изображения.

Результат расчетов показан в Таблице 1.

Можно видеть, что соответствующие коэффициенты для двух изображений разнятся не более чем на 0.00001, т.е. зависимость соседних пикселей в этих изображениях практически идентична [9].

Таблица 1

Коэффициенты корреляции

Коэффициент	Исходное изображение	Результирующее изображение
Диагональная корреляция	0.93798	0.937979
Вертикальная корреляция	0.961882	0.96188
Горизонтальная корреляция	0.959322	0.959314

Разработанный механизм сокрытия информации устойчив к обнаружению сокрытого сообщения по известным паттернам, т.к. фиксированных позиций в изображении для записи информации нет, они зависят от заданных параметров (стегоключа) k, l, h, w, кроме того информационное сообщение распределяется не по всему изображению, а лишь по некоторым его блокам. Кроме того, рассмотренный алгоритм позволяет контролировать процент заполнения стегоконтейнера, что может способствовать повышению стойкости к стегоанализу.

Описанный метод сокрытия информации может использоваться, например, вместо классического LSB метода, т.к. обеспечивает большую конфиденциальность скрываемой информации.

Литература

1. Федорова А.Р., Шпак В.А., Лукьянов Г.И. Разработка программного модуля для выявленияконфиденциальной информации в звуковых файлах // Актуальные проблемы современной науки, техники и образования. –Магнитогорск, 2021. – No 1. – С. 48–50.

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

3. Герлинг Е.Ю. Обзор современного программного обеспечения, использующего методы стеганографии // Е.Ю. Герлинг, К.А. Ахрамеева // Экономика и качество систем связи. 2019 № 3 (13). С. 51–58.

4. Аграновский А.В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ. Монография. – М.: Вузовская книга, 2009. – 220 с

5. Грэхем Р.Л., Кнут Д.Э., Паташник О., Конкретная математика. Математические основы информатики, 2–е изд.: пер. с англ. – М.: ООО «И.Д. Вильямс», 2017. – 784 с.

6. Колмогоров А.Н., Драгалин А. Г. Математическая логика: введение в мат. логику. Учеб. пособие для студентов мат. специальностей вузов. М.: УРСС, с.: ил. (Классический университетский учебник).

7. Фомичев В.М. Дискретная математика и криптология: Курс лекций. М.: ДиалогМИФИ, 2003. 400 с

8. Основы криптографии: учеб. пособие / А.П. Алферов, А.Ю. Зубков, А.С. Кузьмин и др. 2–е изд. М.: Гелиос АРВ, 2002. 480 с.

9. Сидоренко А.В., Шишко М.С., Шифрование изображений на основе хаотических отображений с использованием параллельных вычислений // Информатика. – 2017. – №4. – С. 78–88.

References

1. FedorovaA.R., ShpakV.A., Luk'yanovG.I. Razrabotka programmnogo modulja dlja vyjavlenijakonfidencial'noj informacii v zvukovyh fajlah [Development of a software module for detectingconfidential information in audio files]// Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. – Magnitogorsk, 2021. – No 1. – S. 48–50.

2. Konahovich G.F., Puzyrenko A. Ju. Komp'juternaja steganografija. Teorija i praktika [Computer steganography. Theory and practice]. – K.: MC–Press, 2006. – 288 p.

3. Gerling E.Ju., Obzor sovremennogo programmnogo obespechenija, ispol'zujushhego metody steganografii [Review of modern software, using methods of steganography] // E.Yu. Gerling, K.A. Ahrameeva // Jekonomika i kachestvo sistem svjazi. 2019 № 3 (13). P. 51–58.

4. Agranovskij A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. Steganografija, cifrovye vodjanye znaki i stegoanaliz [Steganography, digital watermarks and stegoanalysis]. Monograph. – Moscow: Vuzovskaja kniga, 2009. – 220 p.

5. Grjehem R.L., Knut D.Je., Patashnik O., Konkretnaja matematika. Matematicheskie osnovy informatiki [Concrete Mathematics. Mathematical foundations of computer science], 2nd ed.: transl. from Engl. – M.: E. D. Williams LLC, 2017. – 784 p.

6. Kolmogorov A.N., Dragalin A.G. Matematicheskaja logika: vvedenie v mat. logiku [Mathematical logic: introduction to mathematical logic]. Textbook for students of mathematical specialties of universities. Moscow: URSS, p.: ill. (Classical University Textbook).

7. Fomichev V.M. Diskretnaja matematika i kriptologija: Kurs lekcij [Discrete Mathematics and Cryptology: Course of Lectures]. Moscow: DialogMIFI, 2003. 400 p.

8. Osnovy kriptografii: ucheb. posobie [Fundamentals of Cryptography: tutorial] / A.P. Alferov, A.Yu. Zubkov, A.S. Kuzmin etc. Zubkov A.S. Kuzmin et al. 2nd edition / M.: Helios ARV, 2002. 480 p.

9. Sidorenko A.V., Shishko M.S. Shifrovanie izobrazhenij na osnove haoticheskih otobrazhenij s ispol'zovaniem parallel'nyh vychislenij [Image encryption based on chaotic mappings using parallel computing] // Informatika. – 2017. – №4. – P. 78–88.

ЩЕГОЛИХИН Иван Сергеевич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: shchegolikhin.i@yandex.ru

SHCHEGOLIKHIN Ivan Sergeevich, student of the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenina avenue, 38. E-mail: shchegolikhin.i@yandex.ru

ЖЕРДЕВ Дмитрий Александрович, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: bulbamesh@bk.ru

ZHERDEV Dmitry Aleksandrovich, student of the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenina avenue, 38. E-mail: bulbamesh@bk.ru

КОНОВАЛОВ Максим Владимирович, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: konovalovm.mgn@yandex.ru

KONOVALOV Maxim Vladimirovich, Candidate of Technical Sciences, Associate Professor at the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenina avenue, 38. E-mail: konovalovm.mgn@yandex.ru