УДК 004.056

*Т. Г. Ажбаев, И. М. Ажмухамедов*

Астраханский государственный технический университет

# АНАЛИЗ СТОЙКОСТИ СОВРЕМЕННЫХ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ

**Введение**

В настоящее время в стеганографии наиболее распространенным является метод замены наименьших значащих битов – LSB-метод. Он заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях или аудио- и видеофайлах. Данный метод подробно описан в работе О. П. и П. О. Архиповых [1].

Достоинствами предложенного подхода являются простота реализации и большая вместимость (размер сообщения может составлять до 37,5 % от размера контейнера). Однако данный метод обладает серьезным недостатком: при просмотре битовых срезов изображения можно легко установить факт внедрения сообщения.

В работе А. Т. Алиева [2] опровергается предположение о том, что младшие биты изображения всегда случайны. Показано, что между младшими битами существуют некоторые статистические закономерности и их поведение вовсе не похоже на случайное, а изображение, построенное ими, на шум. В результате анализа более четырех сотен изображений, проведенного автором [2], выяснилось, что в них очень часто встречаются длинные серии из одинаковых бит и практически любое изображение содержит серию минимум из 14 одинаковых бит. В случае, если в младшие биты изображения происходит внедрение информации, эти закономерности нарушаются.

А. Т. Алиевым предложена модификация метода LSB, которая состоит в определении областей монотонной заливки в битовых срезах изображений и внедрении информации в изображение с сохранением этих областей. Для выделения монотонных областей предлагается использовать старшие разряды, которые не используются для сокрытия информации. Так как они не подвергаются изменению, то области, выделенные кодером, могут быть однозначно определены и декодером, т. е. исключается вероятность неоднозначного извлечения информации. В качестве алгоритма, отвечающего за выделение областей, рекомендуется использовать алгоритм выделения четырехсвязной области.

При использовании предложенного метода не нарушаются статистические характеристики изображения и значительно повышается стегостойкость, однако алгоритм не получил распространения из-за малой вместимости, т. к. количество скрываемых бит ограничено количеством областей монотонной заливки. Автором [2] не учитывается тот факт, что в реальных стеганографических системах обычно используются фотореалистичные изображения, содержащие текстурные области и области с плавными переходами цветов.

Альтернативный подход в решении данной проблемы предложили M. Kutter, F. Jordan, F. Bossen [3]: метод внедрения скрытых сообщений, основанный на изменении цвета пиксела в зависимости от его яркости. Предлагается встраивать сообщения в изображения с RGB-кодировкой. Встраивание выполняется в канал синего цвета, т. к. к синему цвету система человеческого зрения наименее чувствительна.

Извлечение бита получателем осуществляется без наличия у него исходного изображения, т. е. вслепую. Для этого выполняется предсказание значения исходного, немодифицированного пиксела на основании значений его соседей. Показано, что алгоритм является робастным ко многим из известных атак: низкочастотной фильтрации изображения, его сжатию в соответствии с алгоритмом JPEG, обрезанию краев.

Достоинством предложенного метода является то, что величина изменения цветовой составляющей каждого пиксела зависит от его яркости, поэтому в данном случае затруднено применение статистического стегоанализа. Недостаток данного метода заключается в процессе восстановления скрытого сообщения, а именно в использовании предсказания значения исходного, немодифицированного пиксела на основании значений его соседей. При неправильной оценке исходного значения сообщение может быть восстановлено с ошибками.

W. Bender, D. Gruhl, N. Morimoto, A. Lu [4] предложен алгоритм, основанный на копировании блоков из случайно выбранной текстурной области в другую, имеющую сходные статистические характеристики. Это приводит к появлению в изображении полностью одинаковых блоков. Эти блоки могут быть обнаружены следующим образом.

1. Анализ функции автокорреляции стегоизображения и нахождение ее пиков.

2. Сдвиг изображения в соответствии с этими пиками и вычитание изображения из его сдвинутой копии.

3. Разница в местоположениях копированных блоков должна быть близка к нулю. Поэтому можно выбрать некоторый порог и значения, меньшие этого порога по абсолютной величине, и считать их искомыми блоками.

Так как копии блоков идентичны, то они изменяются одинаково при преобразованиях всего изображения. Если сделать размер блоков достаточно большим, то алгоритм будет устойчивым по отношению к большинству из негеометрических искажений. В экспериментах показана робастность алгоритма к фильтрации, сжатию, поворотам изображения.

Основным недостатком алгоритма является исключительная сложность нахождения областей, блоки из которых могут быть заменены без заметного ухудшения качества изображения. Кроме того, в данном алгоритме в качестве контейнера могут использоваться только достаточно текстурные изображения.

Другим популярным методом встраивания сообщений является использование особенностей форматов данных, использующих сжатие с потерей данных (например, JPEG). Этот метод (в отличие от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, т. к. имеется возможность в широком диапазоне варьировать качество сжатого изображения, вследствие чего невозможно определить происхождение искажения.

В [5] рассматривается метод внедрения цифрового водяного знака (ЦВЗ) в графические файлы, сжатые алгоритмом JPEG с использованием эффекта пространственного маскирования. Предложенный алгоритм работает в области преобразования и может применяться в режиме реального времени (для обработки 24-битовой картинки размером 512 × 512 пикселей потребуется всего 50ms на компьютере с частотой процессора 700 MHz).

Для достижения быстродействия алгоритма авторы [5] предлагают не использовать многие операции, связанные с JPEG-сжатием, такие как прямое или обратное дискретное косинусное преобразование (ДКП) или квантование коэффициентов.

Суть предложенного метода состоит в изменении коэффициентов ДКП исходного изображения. Для внедрения битов ЦВЗ выбираются коэффициенты ДКП, удовлетворяющие следующим условиям:

– коэффициенты должны обладать некоторой визуальной значимостью (для обеспечения помехоустойчивости скрытия);

– коэффициенты не должны сильно изменяться при преобразованиях формата или добавлении шума.

Для внедрения одного бита ЦВЗ используется блок размером 8 × 8 пикселей, причем изменению подлежат только яркостные компоненты цветового пространства (более помехоустойчивые, чем хроматические).

Для обеспечения устойчивости к обрезанию краев используется двумерное пространственное преобразование ЦВЗ (диффеоморфизм Аносова), которое равномерно распределяет биты ЦВЗ по области преобразования с характеристиками близкими к случайным.

Обеспечивается устойчивость ЦВЗ к JPEG-сжатию, аддитивному шуму, атаке "salt and pepper" и обрезанию краев. Достоинством данного метода является то, что для выделения ЦВЗ не требуется исходный файл или любая другая информация, связанная с процессом внедрения ЦВЗ. Недостатком является неоднозначная функция восстановления данных, поэтому данный метод неприменим в стеганографических системах скрытой передачи данных.

Алгоритмы скрытия данных в пространственной области внедряют ЦВЗ в области исходного изображения [4, 6–8]. Их преимуществом является то, что для внедрения ЦВЗ нет необходимости выполнять вычислительно громоздкие линейные преобразования изображений. ЦВЗ внедряется за счет манипуляций яркостью или цветовыми составляющими.

Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразования и ДКП, что отчасти объясняется их успешным применением при сжатии изображений. Стегоалгоритм может быть весьма робастным к дальнейшей компрессии изображения, если он будет учитывать особенности алгоритма сжатия. При этом стегоалгоритм, использующий ДКП, вовсе не обязательно будет робастным по отношению к вейвлетному алгоритму сжатия, и наоборот.

Алгоритмы скрытия данных в области преобразования, описаны в [9–12] для ДКП и в [13–30] для вейвлет-преобразований. Впервые использование ДКП для скрытия информации было описано в [9]. При этом ДКП применялось ко всему изображению в целом. Обычно же контейнер разбивается на блоки размером 8 × 8 пикселов. Дискретное косинусное преобразование применяется к каждому блоку, в результате получаются матрицы коэффициентов ДКП также размером 8 × 8.

**Анализ стойкости стеганографических алгоритмов**

Рассмотрим критерии оценки стойкости стеганографических алгоритмов.

Под стойкостью стеганографических алгоритмов понимается вероятность успешного восстановления скрытого сообщения после воздействия атак на контейнер. Так как рассмотренные выше алгоритмы не предназначены для противодействия геометрическим атакам, добавлению шума, фильтрации, обрезанию краев и другим разнообразным искажениям, то в качестве атакующего воздействия рассмотрим сжатие изображения алгоритмами JPEG v.6b, Dartmouth Wavelet Image Compression и SPITH C++ v.8.01. Выбор алгоритмов сжатия обусловлен их широким использованием для обработки изображений в системах мультимедиа.

Данные алгоритмы осуществляют сжатие с потерями, поэтому изображение, восстановленное после сжатия, отличается от исходного. При прочих равных условиях чем больше сжатие, тем больше искажение. Для оценки качества восстановленного изображения можно использовать меру среднеквадратичного искажения, определяемую как

$$\text{СКО} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \hat{x}_i\right)^2,$$

где $N$ – число пикселов в изображении; $x_i$, $\hat{x}_i$ – значение пикселов исходного и восстановленного изображений. Гораздо чаще применяется модификация этой меры – пиковое отношение сигнал/шум (ПОСШ), определяемое как

$$\text{ПОСШ} = 10\log_2 \frac{N 255^2}{\sum_{i=1}^{N}\left(x_i - x_i\right)^2},$$

где 255 – максимальное значение яркости полутонового изображения (т. е. 8 бит/пиксел). Восстановленное изображение считается приемлемым, если ПОСШ $\geq$ 28–30 дБ (в среднем).

Качество алгоритмов сжатия обычно определяется как отношение уровня сжатия к значению ПОСШ, где уровень сжатия равен отношению размера исходного изображения к размеру сжатого изображения. На рис. 1 показан уровень сжатия и соответствующий ПОСШ для всех трех алгоритмов.

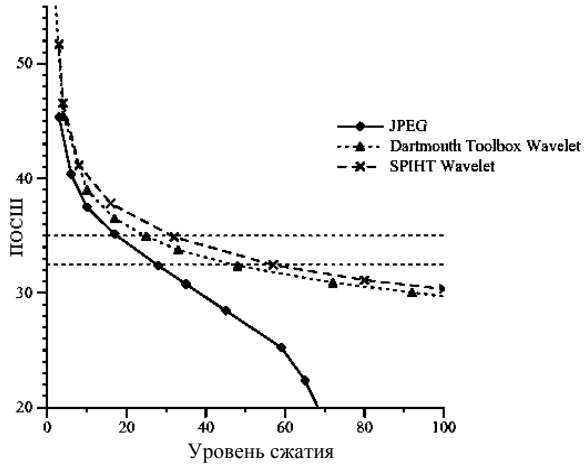


Рис. 1. Зависимость ПОСШ от уровня сжатия для рассматриваемых алгоритмов

Во всех экспериментах использовалось тестовое изображение размерами 512 × 512 пикселов с 256 градациями серого. Уровень сжатия выбран таким образом, чтобы значение ПОСШ составляло 30 дБ.

Для сравнения стойкости рассмотрим 6 стеганографических алгоритмов (по 2 из каждой группы по области преобразования), описания которых приведены в [5–30]. В табл. 1 перечислены сравниваемые алгоритмы, а также указаны параметры, выбранные при реализации этих алгоритмов.

*Таблица 1*

**Параметры сравниваемых алгоритмов**

| Алгоритм | Тип стегосистемы | ЦВЗ | Область преобразования | Другие параметры |
|---|---|---|---|---|
| Bruyndonckx | Открытая | Текстовая строка | Пространственная | $t_1 = 5$, $t_2 = 10$ |
| Pitas | Открытая | Текстовая строка | Пространственная | Размер блока = 16 |
| Koch | Открытая | Текстовая строка | Блоки ДКП 8 × 8 | Уровень квантования ДКП = 3 |
| Cox | Закрытая | Числовая последовательность | Блоки ДКП $n \times n$ | $n = 100$ |
| Barni | Закрытая | Числовая последовательность | Вейвлет-преобразования | $n = 100$ |
| Wang | Закрытая | Числовая последовательность | Вейвлет-преобразования | $n = 100$, $\beta = 1$ |

Для того чтобы оценить точность восстановления скрытого сообщения, введем коэффициент корреляции между исходным и восстановленным ЦВЗ:

$$C(S, S'') = \frac{\sum (s_i - \overline{s_i})(s_i'' - \overline{s_i''})}{\sqrt{(s_i - \overline{s_i})^2}\sqrt{(s_i'' - \overline{s_i''})^2}},$$

где $S$ и $S''$ – исходный и восстановленный ЦВЗ; $s_i$ и $s_i''$ – биты ЦВЗ; $\overline{s_i}$ и $\overline{s_i''}$ – средние значения битовых последовательностей ЦВЗ.

На рис. 2 показана корреляция между текстовой строкой и 100 случайно выбранными строками. Исходная строка является 50-й по счету.

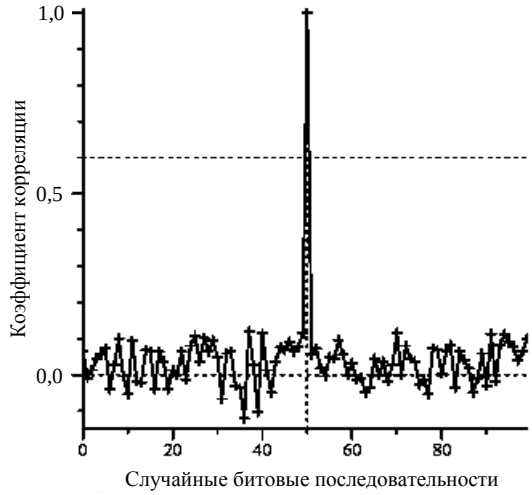


Рис. 2. Корреляция случайных битовых наборов

Так как все алгоритмы вносят разные искажения в изображение, то для чистоты эксперимента для каждого алгоритма необходимо выбрать те параметры, при которых ПОСШ изображений было бы одинаковым.

Для определения этого значения были построены графики зависимости корреляции исходного и извлеченного ЦВЗ от ПОСШ для каждого из алгоритмов. На основе полученных зависимостей значение ПОСШ, соответствующее максимальной корреляции для всех 6 алгоритмов, было выбрано равным 45 дБ.

Сравнение стеганографических алгоритмов проводилось по двум показателям:

– цифровой водяной знак, представленный как разность исходного и заполненного контейнера и дающий представление об уровне вносимых в изображение искажений;

– график зависимости корреляции извлеченного ЦВЗ от уровня сжатия, примененного к изображению.

Результаты исследования стойкости алгоритмов сведены в табл. 2.

*Таблица 2*

**Результаты исследования стойкости алгоритмов**

| Алгоритм | Однозначность восстановления | Устойчивость к фильтрации | Устойчивость к геометрическим преобразованиям | Устойчивость к сжатию | Устойчивость к средствам статистического стегоанализа |
|---|---|---|---|---|---|
| Bruyndonckx | + | – | – | – | + |
| Pitas | + | – | – | + | + |
| Koch | + | – | – | – | – |
| Cox | + | – | + | + | – |
| Barni | – | + | – | + | + |
| Wang | + | + | – | + | – |

Описанные выше алгоритмы лишь частично удовлетворяют набору требований, предъявляемых к системам скрытой передачи данных.

**Заключение**

Анализ стойкости стеганографических алгоритмов показал, что ни один из них не свободен от недостатков. Именно поэтому создание стойкого алгоритма, обладающего достаточной степенью робастности к различным преобразованиям и противостоящего средствам статистического и визуального стегоанализа, и разработка на его основе программного продукта для скрытия достаточно большого объема данных методами цифровой стеганографии являются весьма актуальной задачей.

*СПИСОК ЛИТЕРАТУРЫ*


1. *Архипов О. П., Архипов П. О.* Параметрический класс прямых прозрачных методов стегокодирования цветных изображений // Информационные технологии вычислительные системы. – 2003. – Вып. 1–2.
2. *Алиев А. Т.* О применении стеганографического метода LSB к большим областям монотонной заливки // Вестн. Дагестан. Гос. техн. ун-та. – 2004. – Т. 4, № 4 (22). – С. 67–72.
3. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation // Proceedings of SPIE: Security and Watermarking of Multimedia Content II. – 1999. – B. 3967.
4. *Techniques for Data Hiding* / W. Bender, D. Gruhl, N. Morimoto, A. Lu // IBM Systems Journal. – 1996. – B. 35.
5. *Luo W., Heileman G. L.* A fast and robust Watermarking method for jpeg images // IEEE Journal on Selected Areas of Communications. – 1998.
6. *Langelaar G., Lagendijk R., Biemond J.* Robust labeling methods for copy protection of images // Proc. of the SPIE Storage and Retrieval for Image and Video Databases V. – 1997. – B. 3022.
7. *Nikolaidis N., Pitas I.* Robust image watermarking in the spatial domain // Signal Processing, Special Issue on Copyright Protection and Control. – 1998. – B. 66, N 3. – P. 385–403.
8. *Low cost spatial watermarking* / V. Darmstaedter, J.-F. Delaigle, J. Quisquater, B. Macq // Computers and Graphics. – 1998. – B. 5. – P. 417–423.
9. *Koch E., Zhao J.* Towards Robust and Hidden Image Copyright Labeling // IEEE Workshop on Nonlinear Signal and Image Processing. – 1995. – P. 123–132.
10. *Hsu C.-T., Wu J.-L.* Hidden digital watermarks in images // IEEE Transactions on Image Processing. – 1999. – B. 8, N 1. – P. 58–68.
11. *Secure* spread spectrum watermarking for multimedia / I. Cox, J. Kilian, T. Leighton, T. Shamoon // IEEE Transactions on Image Processing. – 1997. – B. 6, N 12. – P. 1673–1687.
12. *Fridrich J.* Combining low-frequency and spread spectrum watermarking // Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression and Encryption. – 1998. – B. 3456. – P. 2–12.
13. *A DWT-based* technique for spatio-frequency masking of digital signatures / M. Barni, F. Bartolini, V. Cappellini et al. /// Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents. – 1999. – B. 3657.

14. *Lewis A. S., Knowles G.* Image compression using the 2-d wavelet transform // IEEE Transactions on Image Processing. – 1992. – N 1. – P. 244–250.
15. *Lu C.-S., Liao H.-Y. M.* Oblivious watermarking using generalized gaussian // Proceedings of the 7th International Conference on Fuzzy Theory and Technology. – 2000. – P. 260–263.
16. *A New* Watermarking Technique for Multimedia Protection / C.-S. Lu, S.-K. Huang, C.-J. Sze, H.-Y. M. Liao. – CRC Press, 2000.
17. *Cocktail* watermarking on images / C.-S. Lu, H.-Y. M. Liao, S.-K. Huang, C.-J. Sze // Proceedings of the 3rd Information Hiding Workshoстр. – 1999. – B. 1768. – P. 333–347.
18. *Highly robust image* watermarking using complementary modulations / C.-S. Lu, H.-Y. M. Liao, S.-K. Huang, C.-J. Sze // Proceedings of the 2nd International Information Security Workshoстр. – 1999. – P. 136–153.
19. *Visibility* of wavelet quantization noise / A. B. Watson, G. Y. Yang, J. A. Solomon, J. Villasenor // IEEE Transaction in Image Processing. – 1997. – N 6. – P. 1164–1175.
20. *Podilchuk C. I., Zeng W.* Digital image watermarking using visual models // Proceedings of the 2nd SPIE Human Vision and ElectronicImaging Conference. – 1997. – B. 3016. – P. 100–111.
21. *Podilchuk C. I., Zeng W.* Image-adaptive watermarking using visual models // IEEE Journal on Selected Areas in Communications, special issue on Copyright and Privacy Protection. – 1998. – N 16 (4). – P. 525–539.
22. *Wolfgang R. B., Podilchuk C. I., Delp E. J.* The effect of matching watermark and compression transforms in compressed color images // Proceedings of the IEEE International Conference on Image Processing. – 1998.
23. *Secure* spread spectrum watermarking for multimedia / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Proceedings of the IEEE International Conference on Image Processing. – 1997. – B. 6. – P. 1673–1687.
24. *Zeng W., Lei S.* Transform domain perceptual watermarking with scalable visual detection a proposal for JPEG2000 // Technical report, Digital Video Department,Sharp Laboratories of America, Inc., USA, 1998.
25. *Wang H.-J., Jay Kuo C.-C.* Image protection via watermarking on perceptually significant wavelet coefficients // Proceedings of the IEEE Workshop on Multimedia Signal Processing, 1998.
26. *Wang H.-J., Jay Kuo C.-C.* An integrated approach to embedded image coding and watermarking // Proceedings of IEEE ICASSCTP, 1998.
27. *Wang H.-J., Jay Kuo C.-C.* Watermark design for embedded wavelet image codec // Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing. – 1998. – B. 3460. – P. 388–398.
28. *Wang H.-J., Su C.-C., Jay Kuo C.-C.* Wavelet-based digital image watermarking // Optics Express. – 1998. – N 3. – P. 491–496.
29. *Multithreshold* wavelet codec (MTWC) / H.-J. Wang, Y.-L. Bao, C.-C. Jay Kuo, H. Chen // Technical report, Department of Electrical Engineering, University of Southern California, Switzerland, 1998.
30. *Wang H.-J., Jay Kuo C.-C.* High fidelity image compression with multithreshold wavelet coding (MTWC) // SPIE's Annual meeting – Application of Digital Image Processing XX, USA, 1997.

Статья поступила в редакцию 28.11.2007

## THE ANALYSIS OF RESISTANCE OF MODERN STEGANOS ALGORITHMS

*T. G. Azhbaev, I. M. Azhmukhamedov*

The results of the analysis of resistance of modern steganos algorithms to various attacks are given, the main principles of construction of steganographic systems of information introduction into the spatial area and the area of transformations are considered. The criteria of estimation of resistance of steganos algorithms are determined. The resistance of the various steganos systems is compared by the example of 6 algorithms. The necessity of creation of the resistant algorithm with sufficient power of robustness to various transformations and resistant to statistical and visual steganalyth is explained, and the development on its basis of the software product to conceal rather large data volume using methods of digital steganography is also of great importance.