УДК 004.56+003.26

МЕТОД ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ И КОДИРОВАНИЕ ИНФОРМАЦИИ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

А.А. Хартанович

Белорусский государственный технологический университет, Минск, Беларусь

Аннотация. В данной работе рассматривается метод стеганографии, основанный на дискретном вейвлет-преобразовании, и применение кодирования информации для повышения надежности скрытой передачи данных. Описывается процесс разложения изображения с использованием преобразования Хаара, который позволяет выделять поддиапазоны и встраивать секретные сообщения в наименее заметные области. Проведен сравнительный анализ методов стеганографии по показателям MSE и PSNR, а также исследовано влияние различных модификаций изображения на точность извлечения данных. Для повышения устойчивости к искажениям использован код Хемминга, который позволяет обнаруживать и исправлять ошибки при декодировании, однако предлагается применение более сложных конструкций кодирования и декодирования сообщения на основе комбинирования кодов. Результаты экспериментов подтверждают, что сочетание ДВП и методов кодирования обеспечивает высокую степень скрытности и надежности передачи информации.

Ключевые слова: стеганография; секретное сообщение; преобразование Хаара; дискретное вейвлет-преобразование (ДВП); поддиапазон; коэффициент битовых ошибок; отношение сигнал/шум; среднеквадратическая ошибка; кодирование; код Хемминга.

DISCRETE WAVELET TRANSFORM METHOD AND INFORMATION ENCODING IN STEGANOGRAPHIC APPLICATIONS

A.A. Khartanovich

Belarusian State Technological University, Minsk, Belarus

Abstract. This paper discusses a steganography method based on the discrete wavelet transform and the use of information coding to improve the reliability of hidden data transmission. It describes the process of image decomposition using the Haar transform, which allows you to select subranges and embed secret messages in the least noticeable areas. A comparative analysis of steganography methods is carried out based on MSE and PSNR indicators, and the effect of various image modifications on the accuracy of data extraction is studied. To improve resistance to distortion, the Hamming code is used, which allows detecting and correcting errors during decoding, but it is proposed to use more complex structures of encoding and decoding of the message

based on a combination of codes. The experimental results confirm that the combination of DWT and coding methods provides a high degree of secrecy and reliability of information transmission.
Keywords: steganography; secret message; Haar transform; discrete wavelet transform (DWT); subband; bit error rate; signal to noise ratio; root mean square error; coding; Hamming code.

Введение

Стеганография – наука о способах передачи (хранения) сокрытой информации, где скрытый канал организуется на базе и внутри открытого с использованием особенностей восприятия информации [1]. Стеганографическая система (стеганосистема) – совокупность средств и методов для формирования скрытого канала передачи информации. Стеганосистема образует стеганоканал, по которому передается (или в котором хранится) заполненный контейнер. Модель стеганосистемы представлена на рис. 1.

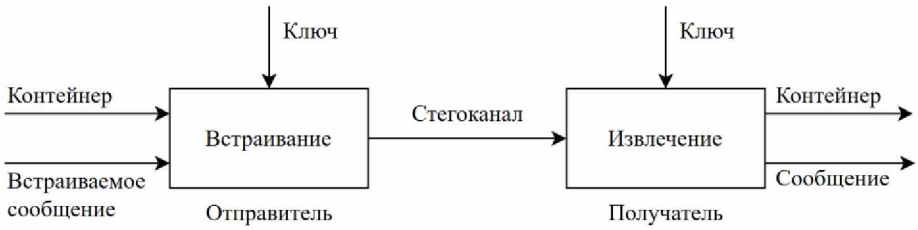


Рис. 1. Модель стеганографической системы
Fig. 1. Model of steganographic system

Стеганографические методы имеют свои достоинства и недостатки, но наибольшего внимания заслуживают в силу своих преимуществ методы частотной области, а именно – метод дискретного вейвлет-преобразования [2].

Основная часть

Дискретное вейвлет-преобразование (ДВП) – метод анализа и преобразования сигналов и изображений, использующий вейвлеты [3]. Процесс ДВП включает разложение изображения на набор коэффициентов различных масштабов и частот, который представляет собой различные детали изображения.

При разложении изображения методом ДВП применяется преобразование Хаара, которое использует двумерный матричный источник (канал RGB-изображения) и применяет вейвлет-преобразование, обрабатывая входное изображение, которое делится на неперекрывающиеся блоки 2×2 пикселей, каждый из которых преобразуется в четыре поддиапазона:

LL – низкочастотное приближение;

LH – горизонтальные различия;

HL – вертикальные различия;

HH – диагональные различия (высокочастотные детали).

Поддиапазон *LL* захватывает наиболее значимые особенности, а другие поддиапазоны – более мелкие детали, куда обычно встраивается сообщение.

Каждый блок можно представить в виде матрицы

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}, \quad (1)$$

где A, B, C и D – значения интенсивностей цвета пикселей от 0 до 255.

Формула преобразования для поддиапазона *LL*:

$$LL = \frac{A + B + C + D}{2}. \quad (2)$$

Получение *LH* описывается формулой:

$$LH = \frac{A - B + C - D}{2}. \quad (3)$$

Для получения поддиапазона *HL* используется формула:

$$HL = \frac{A + B - C - D}{2}, \quad (4)$$

а для поддиапазона *HH* соответственно:

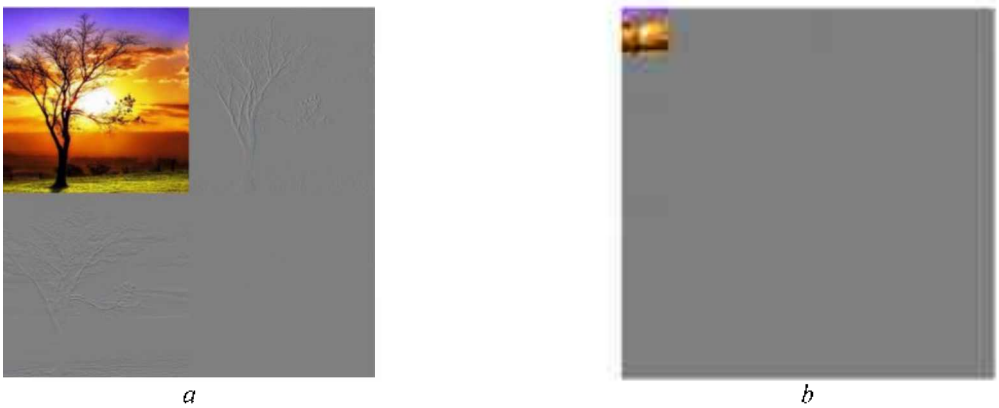
$$HH = \frac{A - B - C + D}{2}. \quad (5)$$

Преобразование необходимо повторять для всех блоков, что снижает разрешение изображения, сохраняя при этом основные детали. Встраивание секретного сообщения происходит в коэффициенты поддиапазона *HH*, при этом символы сообщения преобразуются в 8-битные значения кода ASCII. В процессе изменения значений *HH* используется специальная переменная α, равная небольшому значению (например, α = 0,001), что обеспечивает незаметность. Если бит встраиваемого сообщения равен 1, то коэффициент *HH* увеличивается на значение α, а если бит равен 0, то уменьшается на тоже значение.

При извлечении сообщения проверяются значения коэффициентов поддиапазона *HH*. Если значение *HH* было увеличено, то бит секретного сообщения равен 1, если значение было уменьшено – значение бита равно 0.

Размер изображения определяет, сколько раз его можно разложить на поддиапазоны. Каждый уровень разложения уменьшает разрешение в два раза.

Для демонстрации было разработано приложение, которое позволяет разложить изображение. На рисунке 2 представлены примеры разложения.



a *b*

Рис. 2. Разложение изображения методом ДВП: *a* – 1 уровень; *b* – 3 уровня
Fig. 2. Image decomposition using the DWT: *a* – 1 level; *b* – 3 levels

На практике не следует использовать максимальное количество уровней из-за вычислительной сложности и уменьшающейся отдачи от эффективности внедрения вследствие ухудшения качества изображения.

Разработанный метод ДВП сравнивался с пространственным методом наименее значащих битов (LSB) и частотным методом дискретного косинус-преобразования (ДКП) по параметрам MSE (среднеквадратическая ошибка) и PSNR (отношение сигнал/шум) [4]. Более низкое значение MSE указывает на более близкое соответствие между изображениями, а более высокий PSNR – на лучшее качество и большее сходство двух изображений. В одно и тоже изображение внедрялись одинаковые сообщения разной длины по 100, 1000 и 5000 байт (Б) различными методами. Результаты представлены в табл. 1.

Таблица 1. Значения параметров MSE и PSNR для различных методов
Table 1. Values of MSE and PSNR parameters for different methods

Метод и длина сообщения	MSE	PSNR
LSB 100 Б	0.56385	50.62641
ДКП 100 Б	0.33623	52.86360
ДВП 100 Б	0.11564	57.48899
LSB 1000 Б	6.43666	40.04436
ДКП 1000 Б	4.93623	41.19660
ДВП 1000 Б	0.11564	57.48899
LSB 5000 Б	12.43666	37.18336
ДКП 5000 Б	8.65038	38.76001
ДВП 5000 Б	0.11564	57.48899

Одинаковые значения MSE и PSNR для различных длин сообщений в методе ДВП возникают из-за того, что внедрение информации происходит в наименее значимой области изображения, где одни и те же коэффициенты подвергались повторным изменениям. В итоге разработанный метод ДВП не влияет на параметры анализа изображения, что позволяет встраивать достаточно большие объемы данных без ухудшения качества изображения.

Стеганографические методы также анализировались в условиях модификации изображений. Вейвлет-преобразование демонстрирует лучшую устойчивость к различным изменениям, особенно к сжатию с потерями, однако в некоторых случаях его эффективность оказывается недостаточной, поскольку при значительных изменениях изображения восстановить исходное сообщение полностью не удается. Предлагается дополнительно с ДВП использовать кодирование исходного сообщения для коррекции ошибок при его извлечении.

Сообщение объемом 5000 Б кодировалось с использованием кода Хемминга (7, 4) и внедрялось в JPEG изображение размером 1024×1024 пикселей методом ДВП [5]. Стегоизображение модифицировалось, после извлечения и декодирования сообщения рассчитывалось среднее значение параметра BER (коэффициент битовых ошибок). Сравнительный анализ представлен в табл. 2.

Таблица 2. Значения BER при декодировании извлеченного сообщения
Table 2. BER values when decoding the extracted message

Модификация изображения	BER без применения кода Хемминга	BER с применением кода Хемминга
Сжатие до 50%	5% (2000 бит с ошибкой)	0.25% (100 бит с ошибкой)
Размер уменьшен на 20%	10% (4000 бит с ошибкой)	1,12% (784 бит с ошибкой)
Контраст увеличен	15% (6000 бит с ошибкой)	2,25% (900 бит с ошибкой)

Код Хемминга (7, 4) исправляет одиночные ошибки и обнаруживает двойные, что позволяет значительно снизить BER при модификациях стегоизображения. Однако использование усовершенствованных методов для исправления ошибок на основе комбинирования кодов позволит исправлять множественные случайные и пакетные ошибки и еще больше уменьшит коэффициент BER [6].

Заключение

Преимуществом вейвлет-преобразования является возможность внедрения информации в малозаметные области изображения путем работы с различными поддиапазонами. Кроме того, данный метод демонстрирует устойчивость к сжатию с потерями и другим модификациям изображения, поскольку данные встраиваются в его частотные характеристики. Дополнительное использование кодирования информации позволяет восстановить скрытое сообщение, даже если оно было искажено в процессе передачи или изменения изображения.

Список использованных источников

1. Урбанович П.П. (2016) *Защита информации методами криптографии, стеганографии и обфускации*. Минск. Издательство «БГТУ».

2. Сейеди С.А., Садыхов Р.Х. (2013) Сравнение методов стеганографии в изображениях. *Информатика*. (37). 66–75.

3. Mallat S. (1989) A Theory for Multiresolutional Signal Decomposition: the Wavelet Representation. *IEEE Trans. Pattern Analysis and Machine Intelligence*. 11 (7). 674–693.

4. Sara U., Akter M., Uddin M. (2019) Image Quality Assessment through FSIM. SSIM. MSE and PSNR – A Comparative Study. *Journal of Computer and Communications*. 7 (3). 8–18.

5. Питерсон У., Уэлдон Э. (1976) *Коды, исправляющие ошибки*. Москва. Издательство «Мир».

6. Хартанович А.А. (2024) Комбинирование каскадной модели и стеганографического метода для размещения информации в файлах изображений. *Технические средства защиты информации*. (12). 94–95.

References

1. Urbanovich P.P. (2016) *Information Protection by Methods of Cryptography, Steganography and Obfuscation*. Minsk. BSTU Publishing House (in Russian).

2. Seyedi S.A., Sadykhov R.Kh. (2013) Comparison of Steganography Methods in Images. *Informatics*. (37). 66–75 (in Russian).

3. Mallat S. (1989) A Theory for Multiresolutional Signal Decomposition: the Wavelet Representation. *IEEE Trans. Pattern Analysis and Machine Intelligence*. 11 (7). 674–693.

4. Sara U., Akter M., Uddin M. (2019) Image Quality Assessment through FSIM, SSIM, MSE and PSNR – A Comparative Study. *Journal of Computer and Communications*. 7 (3). 8–18.

5. Peterson W., Weldon E. (1976) *Error-Correcting Codes*. Moscow. Mir Publishing House.

6. Khartanovich A.A. (2024) Combining a Cascade Model and a Steganographic Method for Placing Information in Image Files. *Technical means of information protection*. (12). 94–95 (in Russian).

Сведения об авторе

Хартанович А.А., магистрант кафедры информационных систем и технологий. Белорусский государственный технологический университет, alinakhartanovichlo@gmail.com.

Information about the author

Khartanovich A., Master`s degree student. the Department of Information Systems and Technologies, Belarusian State Technological University, alinakhartanovichlo@gmail. com.