5. Ronneberger, O., Fischer, P., Brox, T. U-Net: Convolutional Networks for Biomedical Image Segmentation. In: Navab, N., Hornegger, J., Wells, W., Frangi, A. (eds) Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015. MICCAI 2015. Lecture Notes in Computer Science. 2015, vol 9351. Springer, Cham. https://doi.org/10.1007/978-3-319-24574-4_28.

6. Goodfellow Ian J. et al. Generative adversarial nets Proceedings. In: Neural Information Processing Systems. 2014:2672–2680. – https://doi.org/10.48550/arXiv.1406.2661.

7. Zhang R., Dong, S. & Liu, J. Invisible steganography via generative adversarial networks. Multimed Tools Appl**.** 2019 (78):8559–8575. https://doi.org/ 10.1007/s11042-018-6951-z.

8. Yu C. Attention Based Data Hiding with Generative Adversarial Networks. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(01): 1120-1128. – https://doi.org/10.1609/aaai.v34i01.5463

9. Lu S.P., Wang R., Rosin P.L. Large-capacity Image Steganography Based on Invertible Neural Networks. In: 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 2021, p. 10811-10820. https://doi.org/ 10.1109/CVPR46437.2021.01067.

10. Jing J. et al. HiNet: Deep Image Hiding by Invertible Network. In: 2021 IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada, 2021, p. 4713-4722. – https://doi.org/10.1109/ICCV48922.2021.00469.

11. Guan Z. et al. DeepMIH: Deep Invertible Network for Multiple Image Hiding. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 1 Jan. 2023. 2023, 45(1):372–390. https://doi.org/10.1109/TPAMI.2022.3141725.

12. Bi X. et al. High-capacity image steganography algorithm based on image style transfer. Security and Communication Networks. 2021:1-14. – https://doi.org/10.1155/2021/4179340.

УДК 004.56+003.26

А.А. Хартанович, преп.-ст.;
П.П. Урбанович, проф. (БГТУ, г. Минск)

МЕТОД ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ В СТЕНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

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. Ее составляющими компонентами являются: контейнер, встраиваемое сообщение, ключи, контейнер со встроенным сообщением.

Стеганосистема образует стеганоканал, по которому передается (или в котором хранится) заполненный контейнер. Этот канал считается подверженным воздействиям со стороны нарушителей.

Компьютерная стеганография базируется на том, что электронные форматы могут быть до некоторой степени видоизменены без потери функциональности, а также на том, что неспособность органов чувств человека различать незначительные изменения можно использовать к объекту, несущему избыточную информацию. Во всех форматах существуют излишние биты, значения которых практически не сказываются на качестве. В эти биты можно встраивать информацию.

Стеганография изображений может быть представлена растровыми и векторными изображениями [2], где первые можно разделить на два класса: методы пространственной области и частотной.

Стеганографические методы имеют свои достоинства и недостатки, но наибольшего внимания заслуживает метод ДВП.

Дискретное вейвлет-преобразование (ДВП) – метод анализа и преобразования сигналов и изображений, использующий вейвлеты [3].

Процесс ДВП включает разложение изображения на набор коэффициентов вейвлетов различных масштабов и частот. Этот разложенный набор представляет различные детали изображения. Алгоритмы стеганографии, использующие ДВП, могут определять пороговое значение, ниже которого изменение коэффициента ДВП считается незаметным для восприятия. Затем, секретная информация может быть внедрена в коэффициенты, которые находятся выше порога.

Разложение изображения методом ДВП приводит к четырем поддиапазонам: LL (низкочастотное приближение), LH (горизонтальные детали), HL (вертикальные детали) и HH (высокочастотные диагональные детали). Поддиапазон LL захватывает наиболее значимые особенности, в то время как другие поддиапазоны – более мелкие детали. Поэтому данные обычно встраиваются в высокочастотные поддиапазоны.

Один уровень преобразования ДВП сигнала x получают применением набора фильтров. Сначала сигнал пропускается через низкочастотный фильтр g, одновременно сигнал раскладывается с помощью высокочастотного фильтра h. В результате получаются детализирующие коэффициенты и коэффициенты аппроксимации. Так как половина частотного диапазона сигналов отфильтровывается, то отсчеты сигна-

лов прореживаются в два раза. В итоге разложения каждый из получившихся сигналов представляет половину частотной полосы исходного сигнала, так что частотное разрешение удваивается. Такое разложение можно повторить несколько раз.

Данный процесс можно представить в виде двоичного дерева, где листья и узлы соответствуют пространствам с различной частотно-временной локализацией, как показано на рис. 1.

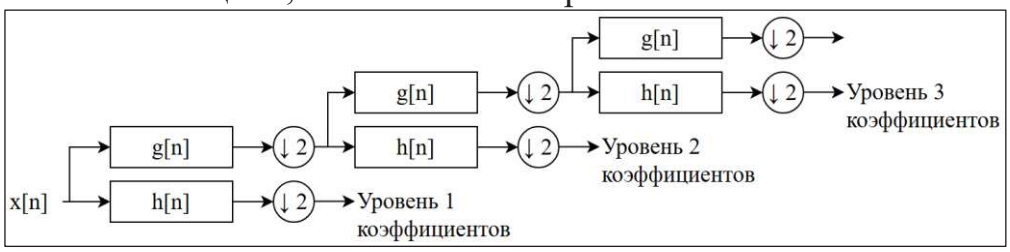

Рисунок 1 – Схема трехуровневого фильтра

На каждом уровне вышеприведенной схемы сигнал раскладывается на низкие и высокие частоты. Именно эти частоты и выбираются для встраивания в них информации.

Для демонстрации было разработано приложение, которое осуществляет процесс разложения изображения на поддиапазоны методом ДВП, что представлено на рис. 2.

В данной работе был произведен сравнительный анализ разработанного метода ДВП с известными пространственным методом LSB (метод наименее значащего бита) и частотным ДКП (дискретное косинус-преобразование). С помощью перечисленных методов было проведено внедрение сообщения в одно и тоже изображение. Исходное изображение и изображение со скрытыми в нем данными анализировались по следующим двум параметрам:

– MSE, где более низкое значение указывает на более близкое соответствие между изображениями;

– PSNR, где более высокое значение указывает на лучшее качество и большее сходство с исходным изображением [4].

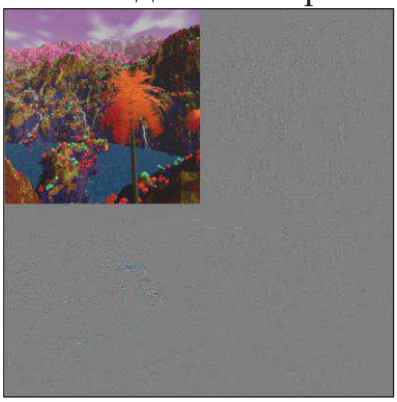

Рисунок 2 – Разложение изображения на поддиапазоны

В изображения внедрялись одинаковые сообщения разной длины по 10, 100 и 1000 байт (Б). Показатели представлены в табл. 1.

Таблица 1 – Значения параметров MSE и PSNR для различных методов

	MSE	PSNR
LSB 10 Б	0,43618	51,73412
ДКП 10 Б	0,12838	57,04563
ДВП 10 Б	0,09564	65,93899
LSB 100 Б	0,56385	48,76641
ДКП 100 Б	0,43623	51,73360
ДВП 100 Б	0,09564	65,93899
LSB 1000 Б	12,43666	37,72936
ДКП 1000 Б	4,65038	46,49001
ДВП 1000 Б	0,09564	65,93899

Идентичные MSE и PSNR для разных длин сообщений метода ДВП возникли в результате того, что в данном случае сообщение внедрялось в наименее значимую область изображения, где одни и те же коэффициенты изменялись одинаково.

Анализ показывает, что метод ДВП при разной длине встраиваемой информации не влияет на параметры анализа изображения, а значит, внедряемое сообщение может быть достаточно большим, что не скажется на качестве изображения.

В работе также произведен анализ при модификации изображений. Изображения со встроенным сообщением подвергались вращению, обрезке и сжатию. После этого проводилось извлечение, где методы оценивались по баллам, что показано в табл. 2:

– 0 – извлечение не обнаружило наличия секретной информации;

– 5 – при извлечении символы не распознаны;

– 10 – извлеченное сообщение частично совпадает с исходным;

– 15 – извлеченное сообщение полностью совпадает с исходным.

Таблица 2 – Оценка методов при модификации изображений

	LSB 10 Б	ДКП 10 Б	ДВП 10 Б	LSB 100 Б	ДКП 100 Б	ДВП 100 Б	LSB 1000 Б	ДКП 1000 Б	ДВП 1000 Б
Сжатие	5	10	10	5	5	10	0	5	10
Обрезка	15	15	15	15	15	15	10	10	10
Вращение	0	5	5	0	5	5	0	5	5
Итог	20	30	30	20	25	30	10	20	25

Итоговое количество баллов говорит о том, что использование вейвлетов является более устойчивым к различным модификациям, но не полностью соответствует ожиданиям, поэтому дополнительно предлагается совместное применение ДВП и кодирования исходного сообщения с целью исправления ошибок при извлечении информации [5].

Преимуществами использования вейвлет-преобразования является то, что информация внедряется в наименее заметные области на основе различных поддиапазонов, что обеспечивает возможность встраивания, предлагая баланс надежности и незаметности, а также данный метод более устойчив к сжатию с потерями и другим модификациям изображения, так как данные внедряются именно в частотные характеристики.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович – Минск: БГТУ, 2016. – 220 с.

2. Сейеди, С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – 2013. – № 1 (37). – С. 66–75.

3. Mallat, S. A theory for multiresolutional signal decomposition: the wavelet representation // IEEE Trans. Pattern Analysis and Machine Intelligence. – 1989. – №. 7. – P.674–693.

4. Sara, U. Image Quality Assessment through FSIM, SSIM, MSE and PSNR. A Comparative Study / U. Sara, M. Akter, M. Uddin // Journal of Computer and Communications. – 2019. – Vol 7, № 3. – P. 8–18.

5. Хартанович, А.А. Комбинирование каскадной модели и стеганографического метода для размещения информации в файлах изображений / А.А. Хартанович // Технические средства защиты информации: тезисы докладов XXII Белорусско-российской науч.-технич. конференции, Минск, 12 июня 2024 г. – Минск: БГУИР, 2024. – С. 94–95.

УДК 004.051

В.С. Кантарович, ассист.; П.П. Урбанович, проф.
(БГТУ, г. Минск)

КРИТЕРИИ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ОБФУСКАЦИИ И ДЕОБФУСКАЦИИ ПРОГРАММНОГО КОДА

В современном мире программные продукты всё чаще становятся объектом атак, важно защищать код от обратного инжиниринга и анализа злоумышленниками. Таким образом обфускация программного кода играет ключевую роль в современном мире информационной безопасности и защиты интеллектуальной собственности [1].

Обфускация программного кода – это процесс изменения и запутывания кода таким образом, чтобы его стало труднее понимать и ана-