УДК 004.056.53

АЛГОРИТМ ВСТРАИВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА, УСТОЙЧИВЫЙ К ГЕОМЕТРИЧЕСКИМ АТАКАМ И ЗАШУМЛЕНИЮ

И.В. Маутин
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье предложен неслепой алгоритм встраивания цифровых водяных знаков для защиты авторских прав на изображения. Метод базируется на дискретном вейвлет-преобразовании и алгоритме расширения спектра. Криптографическая стойкость обеспечивается использованием хаотических отображений для генерации координат, а устойчивость к геометрическим и шумовым атакам – преобразованием Арнольда и избыточным кодированием с мягким мажоритарным декодированием. Экспериментальные результаты подтверждают высокую эффективность метода.
Ключевые слова: цифровой водяной знак; стеганография; дискретное вейвлет-преобразование; метод расширения спектра; хаотические отображения; преобразование Арнольда; избыточное кодирование; мажоритарное декодирование; защита авторских прав; устойчивость к атакам.

DIGITAL WATERMARKING ALGORITHM ROBUST TO GEOMETRIC AND NOISE ATTACKS

I.V. Mautsin
Educational Institution "Belarusian State University of Informatics and Radioeletronics", Minsk, Republic of Belarus

Abstract. This paper proposes a non-blind digital watermarking algorithm for image copyright protection. The method is based on the discrete wavelet transform and the spread spectrum approach. Cryptographic security is provided by utilizing chaotic maps for coordinate generation, whereas robustness against geometric and noise attacks is achieved through the Arnold transform and repetition coding combined with soft majority decoding. Experimental results confirm the high effectiveness of the proposed method.
Keywords: digital watermark; steganography; discrete wavelet transform; spread spectrum; chaotic maps; Arnold transform; repetition coding; majority decoding; copyright protection; robustness.

Введение

Разработка алгоритмов скрытого внедрения цифровых водяных знаков (ЦВЗ) требует соблюдения баланса между незаметностью, устойчивостью к искажениям и криптографической стойкостью. Частотные методы на базе дискретного вейвлет-преобразования (DWT) демонстрируют высокую устойчивость к компрессии, однако часто остаются уязвимыми к геометрическим атакам и тривиальны для взлома при использовании стандартных генераторов последовательностей. Целью

данной работы является решение проблемы уязвимости частотных ЦВЗ к локальным разрушениям сигнала и импульсному шуму.

Основная часть

Для устранения пространственной корреляции пикселей и защиты от локальных выбросов к матрице ЦВЗ применяется дискретное двумерное преобразование Арнольда [1]. Полученная двумерная матрица линеаризуется в одномерный битовый вектор W длиной L. На втором этапе к вектору W применяется помехоустойчивое кодирование с повторением. Каждый бит w_i дублируется R раз, где R – нечетный коэффициент избыточности, например, $R = 5$ или $R = 7$). Формируется расширенная последовательность W' длиной $L \times R$.

Для обеспечения криптографической стойкости алгоритма координаты встраивания формируются псевдослучайным образом с использованием хаотических отображений [2]. Процесс инициализируется секретным ключом пользователя, который подвергается криптографическому хешированию. Полученный хеш разбивается на блоки, значения которых выступают в качестве начальных условий (x_0, y_0) и управляющих параметров для многомерной хаотической системы. Результатом работы генератора является массив уникальных пар индексов блоков (r, c). Строгая чувствительность хаотических систем к начальным условиям гарантирует, что изменение ключа даже на один бит приводит к генерации стохастически независимой карты координат, что делает несанкционированное извлечение ЦВЗ вычислительно невыполнимым.

Канал яркости исходного изображения подвергается DWT заданного уровня. Для модификации выбираются коэффициенты среднечастотных поддиапазонов, так как изменения в низких частотах приводят к видимым визуальным артефактам, а высокочастотные детали уничтожаются при компрессии.

Внедрение битов расширенной последовательности W' в выбранные хаотическим генератором координаты (r, c) выполняется по аддитивной схеме метода расширения спектра. Правило модификации вейвлет-коэффициента C математически описывается следующим образом:

$$C'_{r,c} = \begin{cases} C_{r,c} + \alpha, & \text{если } w_i = 1 \\ C_{r,c} - \alpha, & \text{если } w_i = 0 \end{cases}, \quad (1)$$

где $C_{r,c}$ – исходный вейвлет-коэффициент, α – коэффициент силы встраивания, w_i – бит последовательности W'.

Для извлечения ЦВЗ оригинальное и анализируемое изображения подвергаются DWT. С использованием ключа пользователя заново генерируется идентичная хаотическая карта координат. По заданным позициям вычисляется $\Delta C_{r,c} = C^*_{r,c} - C_{r,c}$. Массив значений ΔC разбивается

на блоки длиной R, внутри которых вычисляется медиана блока S_k: если $S_k > 0$, бит восстанавливается как 1, иначе – 0 [3]. Такой подход позволяет безошибочно извлечь информацию даже в случае уничтожения или сильного искажения части блоков. Восстановленный одномерный битовый вектор преобразуется в двумерную матрицу, к которой применяется обратное преобразование Арнольда для получения итогового визуального логотипа.

Предложенный метод был подвергнут серии испытаний на устойчивость к различным типам атак с варьируемыми алгоритмическими параметрами. В таблице ниже представлены усредненные значения данных метрик, рассчитанные для каждого отдельного класса атак.

Результаты тестирования метода
Test results of the method

Название атаки	BER	Accuracy	NC	PSNR	SSIM
Шум Гаусса	0.2190	0.7810	0.8626	55.96	0.4549
JPEG	0.0029	0.9971	0.9983	∞	0.9874
Медианный фильтр	0.0127	0.9873	0.9927	67.09	0.9464
Шум соль и перец	0.1035	0.8965	0.9381	58.96	0.6781
Закрашивание	0.0221	0.9779	0.9872	65.93	0.9118

Заключение

В ходе проведенного исследования был разработан и реализован криптостойкий неслепой алгоритм внедрения цифровых водяных знаков, объединяющий преимущества DWT, метода расширения спектра и математического аппарата теории хаоса. Экспериментальное тестирование подтвердило высокую устойчивость предложенной архитектуры.

Список использованных источников / References

1. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8(06), 1259-1284.

2. Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023). A blind and robust color image watermarking scheme based on DCT and DWT domains. Multimedia Tools and Applications, 82(21), 32855-32881.

3. Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020(1), 9597619.

Сведения об авторе

Маутин И.В., магистрант кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mautin.ivan.3@gmail.com.

Information about the author

Mautsin I., Master Student of the Informatics Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mautin.ivan.3@gmail.com.