УДК 004.056

РАЗРАБОТКА МЕТОДИКИ ИНТЕГРАЦИИ ХАОТИЧЕСКОГО ШИФРОВАНИЯ И АДАПТИВНОЙ ВЗВЕШЕННОЙ СТЕГАНОГРАФИИ В ИЗОБРАЖЕНИЯХ

Чан В. Х.[1], Нгуен Х. В.[1]
Научный руководитель – доктор технических наук, профессор Беззатеев С.В.[1]
[1]Университет ИТМО

Введение

Интеграция криптографических и стеганографических методов позволяет одновременно скрывать как содержание сообщения, так и сам факт его передачи. Хаотическое шифрование использует свойства нелинейных динамических систем (чувствительность к начальным условиям, псевдослучайность) для формирования сложных преобразований, повышающих стойкость к анализу. Стеганография в изображениях при этом предъявляет дополнительные требования: встраивание должно оставаться малозаметным визуально и устойчивым к типовым искажениям, а также учитывать неоднородность контейнера. В данной работе рассматривается методика объединения хаотического шифрования с адаптивным взвешенным встраиванием в изображениях и приводятся результаты экспериментальной оценки качества и скрытности.

Основная часть

С использованием математических моделей решаются следующие основные задачи:

1) Анализ хаотического шифрования – выбор и исследование хаотических отображений как источника псевдослучайности и механизма перемешивания, оценка чувствительности к параметрам и обеспечиваемой криптографической стойкости [1].

2) Разработка стеганографического метода на основе взвешенной метрики – адаптивное сокрытие данных по принципам WF5: разделение изображения на области различной важности (по локальным характеристикам контейнера), минимизация искажений с применением кода Хэмминга и встраивание с учётом веса (важности) области, что снижает вероятность обнаружения и визуальные артефакты [2, 3].

3) Интеграция хаотического шифрования и стеганографии – построение единого контура: шифрование полезной нагрузки хаотическим механизмом, затем встраивание полученного шифртекста в изображение взвешенным методом; на стороне приёма выполняются извлечение, проверка корректности и расшифрование.

4) Экспериментальная оценка эффективности – проверка метода на стандартных изображениях-контейнерах (Lenna, Barbara, Fruit) с расчётом метрик PSNR, SSIM и Embedding Rate (ER). При встраивании сообщения длиной 84320 бит получены: Lenna – PSNR 74.68, SSIM 1.00, ER 0.015083; Barbara – PSNR 62.61, SSIM 0.9998, ER 0.241334; Fruit – PSNR 71.74, SSIM 0.9999, ER 0.029289. При увеличении объёма внедряемых данных (повторение блока, n = 2, 4, 6) значения SSIM сохраняются на уровне 0.9991–0.9999, а PSNR остаётся не ниже 56.42 dB даже при близком к предельному встраиванию (например, при n = 6: Lenna – 66.89 dB, Barbara – 56.42 dB, Fruit – 63.98 dB), что указывает на малозаметность модификаций при росте нагрузки.

Выводы

Разработана и апробирована методика интеграции хаотического шифрования и адаптивной взвешенной стеганографии в изображениях. Комбинация подходов обеспечивает двойную защиту: хаотическое шифрование повышает стойкость полезной

нагрузки к криптоанализу, а взвешенное встраивание уменьшает искажения контейнера и снижает вероятность выявления скрытых данных. Экспериментальные результаты подтверждают высокую визуальную незаметность: для тестовых изображений значения SSIM близки к 1, а PSNR остаётся высоким даже при увеличении объёма встраивания, что делает метод пригодным для практического применения в задачах скрытой передачи данных.

Литература

1. Kocarev L., Lian S. (Eds.) Chaos-Based Cryptography: Theory, Algorithms and Applications. Springer, 2011.
2. Westfeld A. F5 – A Steganographic Algorithm: High Capacity Despite Better Steganalysis. In: Information Hiding. 2001.
3. Беззатеев С.В., Волошина Н.В. Маскирующее сжатие на основе модели взвешенной структуры изображения. Информационно-управляющие системы, 2017, №6, с. 88–95.
4. Voloshina N., Bezzateev S., Zhidanov K. Weighted Digital Watermarking Approaches Comparison. Redundancy 2016, Saint Petersburg, pp. 172–174.
5. Steganographic WF5 Method for Weighted Embedding: An Overview and Comparison. Springer, 2019. URL: https://link.springer.com/chapter/10.1007/978-3-030-30859-9_37 (дата обращения: 08.01.2025).

Обучающийся _____ Чан Ван Хоанг
(Фамилия И.О.)

Научный руководитель _____ Беззатеев Сергей Валентинович
(Фамилия И.О.)