Лабораторная работа №1

ФИО

Гусакова В. А., Зимовец В. А.

Topic

Data Hiding; Steganography; Reversible Watermarking

Описание предметной области

Данный топик охватывает исследования в области сокрытия данных с помощью визуальной информации, изображений. Стеганография — это практика представления информации в другом объекте таким образом, чтобы присутствие информации не было очевидно для человеческого наблюдения. Одним из способов сокрытия информации являются обратимые водяные знаки (watermarks). Это идентифицирующее изображение, узор или сообщение, которое выглядит как различные оттенки светлоты/темноты при просмотре с подходящими настройками искажённого изображения.

Недостатки

Некоторые методы создания водяного знака могут приводить к искажению заложенных данных, что является критическим при передачи информации.

Идея

Решение проблемы искажения начальных данных с использованием методов глубокого обучения.

Краткий текст обзора

В условиях современных вызовов защита интересов человека и гражданина является основополагающей в вопросе безопасности. В этом контексте очень важна возможность беспрепятственной передачи конфиденциальной информации. Одним из возможных решений является сокрытие данных. Оно позволяет хранить секретную информацию в различном виде без явного факта существования скрытых данных. Подобный способ хранения информации называется стеганографией. Существует множество методов сокрытия данных с помощью текста [5, 9] или аудио [3, 5], однако наиболее распространенным способом обеспечения безопасности является стеганография путем встраивания данных в изображение и создания стего-изображения или обратимого водяного знака. Данные (информационные биты) скрыты в пиксельных значениях изображения, что делает невозможным для злоумышленника обнаружить, где хранятся данные [5, 8].

Для создания обратимых водяных знаков существует множество методов. [4, 6, 7, 1, 2]. Так был найден метод Reversible Data Hiding (RDH) для встраивания данных в сложные области изображения с помощью многократной модификации гистограммы для оптимизированного встраивания данных с более высокой сложностью, при этом сокрытие данных становится более защищённым от современного стег-анализа [4].

Ещё одним методом, связанным с гистограммами, является Prediction-error Expansion (PEE). Он состоит из генерации ошибки предсказания и её модификации. Сначала вычисляется предварительно предсказанное значение для целевого пикселя из его контекста, чтобы сгенерировать ошибку предсказания (т. е. разницу между интенсивностью пикселя и его предсказанным значением). Из полученных ошибок метод модификации определяет расширяемые для переноса данных и смещаемые для создания пространства встраивания [6].

Помимо этого, существует метод, основанный на предсказании и адаптивном классификационном шифровании, который также рассчитывает изображение с ошибкой предсказания. Затем значения пикселей изображения делятся на две категории с помощью порогового диапазона, который выбирается адаптивно в зависимости от содержания изображения [7].

Немногие предыдущие схемы обратимых видимых водяных знаков имеют как хорошую прозрачность, так и видимость водяных знаков. Поэтому была предложена адаптивная схема, объединяющая общую вариативность и визуальное восприятие в сжатой области Block Truncation Coding (BTC). Она заключается в расчете фактора визуального восприятия путем слияния характеристик текстуры и яркости [1].

Основной проблемой RDH является искажение передаваемой информации. И чтобы преодолеть этот недостаток, происходит внедрение глубокого обучения. Основное преимущество методологий глубокого обучения для сокрытия данных заключается в том, что они работают с водяными знаками изображений более адаптивным образом с помощью динамически обучающихся алгоритмов, что помогает извлечению как высокоуровневых, так и низкоуровневых признаков для водяных знаков из нескольких экземпляров больших данных.

References

1. Hengfu Yang ZG Mingfang Jiang. Adaptive Reversible Visible Watermarking Based on Total Variation for BTC-Compressed Images. *Computers, Materials & Continua*. 2023;74(3):5173-5189. doi:[10.32604/cmc.2023.034819](https://doi.org/10.32604/cmc.2023.034819)
2. Zhong X, Huang PC, Mastorakis S, Shih FY. An Automated and Robust Image Watermarking Scheme Based on Deep Neural Networks. *CoRR*. 2020;abs/2007.02460. <https://arxiv.org/abs/2007.02460>
3. Alieksieiev A, Svatovskiy I. ANALYSIS OF COMMON AUDIO STEGANOGRAPHY METHODS. *Grail of Science*. Published online December 16, 2023:117-118. doi:[10.36074/grail-of-science.08.12.2023.24](https://doi.org/10.36074/grail-of-science.08.12.2023.24)
4. Chen H, Wang J, Zhou Y, Chang T, Shi K, Yuan J. Improving the Security of Reversible Data Hiding Using Multiple Histogram Modification. *Mathematical Problems in Engineering*. 2022;2022:1-12. doi:[10.1155/2022/7192697](https://doi.org/10.1155/2022/7192697)
5. Satish EG, Sreenivasa N, Naresh E, Naidu P, Ac R. Multimedia Multilevel Security by Integrating Steganography and Cryptography Techniques. *ITM Web of Conferences*. 2023;57. doi:[10.1051/itmconf/20235701012](https://doi.org/10.1051/itmconf/20235701012)
6. He W, Xiong G, Wang Y. Reversible data hiding based on multi‐predictor and adaptive expansion. *IET Image Processing*. 2021;16. doi:[10.1049/ipr2.12395](https://doi.org/10.1049/ipr2.12395)
7. Qu L, He H, Zhang S, Chen F. Reversible Data Hiding in Encrypted Images Based on Prediction and Adaptive Classification Scrambling. *Computers, Materials & Continua*. 2020;65:2623-2638. doi:[10.32604/cmc.2020.09723](https://doi.org/10.32604/cmc.2020.09723)
8. Kumar R, Yadav A. Steganography: The Art of Data Hiding. In: Shashikala Channalli et al /International Journal on Computer Science and Engineering Vol.1. ; 2023:291-300. doi:[10.1007/978-981-99-3485-0\_22](https://doi.org/10.1007/978-981-99-3485-0_22)
9. Tyagi L, Gupta A, Mohamed A. *Unveiling the Invisible an In-Depth Analysis of Text Steganography Techniques, Challenges, and Advancement*.; 2023:183. doi:[10.1109/ICTACS59847.2023.10390024](https://doi.org/10.1109/ICTACS59847.2023.10390024)
10. Frattolillo F. Watermarking Protocols: Problems, Challenges and a Possible Solution. *The Computer Journal*. 2014;58. doi:[10.1093/comjnl/bxu015](https://doi.org/10.1093/comjnl/bxu015)