В результате этапа обучения на основе эталонных наборов данных вход-выход ИНС настраивается таким образом, чтобы в дальнейшем для произвольного входного сигнала выдать достаточно точный результат. Перед началом обучения весовые коэффициенты устанавливаются равными некоторым случайным значениям. В процессе обучения сеть должна корректировать весовые коэффициенты так, чтобы максимально уменьшить значение общей ошибки. По завершении успешного обучения сети можно переходить к работе с тестовыми объектами [3].

Интеллектуальный анализ и обработка данных представляют собой мощный инструмент, способствующий преобразованию больших объемов данных в ценные знания и информацию. Применение этого подхода позволяет раскрывать скрытые закономерности и тенденции, что важно для принятия стратегических решений. В целом, развитие методов и технологий интеллектуального обработки данных обещает значительное усиление аналитических возможностей и эффективность принимаемых на их основе решений.

ЛИТЕРАТУРА

1. Гифт Н. Прагматичный ИИ. Машинное обучение и облачные технологии : науч. изд./ Н. Гифт ; пер. с англ. И. Пальти. – СПб : Питер, 2019. – 300 с.

2. Серебряная Л.В., Третьяков Ф.И. Методы и алгоритмы принятия решений: учеб.-метод. пособие для студ. спец. «Программное обеспечение информационных технологий» всех форм обуч. / Л. В. Серебряная, Ф. И. Тртетьяков. – Минск: БГУИР, 2014. – 50 с.

3. Серебряная, Л.В. Методы построения искусственных нейронных сетей для классификации данных / Л.В. Серебряная // Цифровая трансформация. – 2022. – Т. 28, № 1. – С. 20–26.

УДК 004.03.26+004.56

Д.В. Сазонова, асп.,
П.П. Урбанович, проф. (БГТУ, г. Минск)

АНАЛИЗ МОДЕЛЕЙ И СРЕДСТВ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Стеганография – наука о способах передачи или хранения информации при сохранении в тайне самого факта такой передачи (хранения) [1]. С развитием искусственного интеллекта (ИИ) интеграция сте-

ганографии и нейронных сетей (НС) [2] привела к появлению технологий сокрытия информации, основанных на глубоком обучении.

В докладе проанализированы особенности основных стеганографических методов на основе ИНС.

Стеганографические системы на основе архитектуры «кодер-декодер». Классический вариант данной архитектуры рассмотрен в [3]. Здесь реализуется сокрытие цветного изображения в другом цветном изображении того же размера. В процессе обучения НС декодера гарантируется сходство между изображением-контейнером и секретным изображением, обеспечивая заданную точность извлечения сообщения из контейнера. Модель уязвима для стеганоанализа.

В [4] предложена модель StegNet, в которой модифицирова функцию потерь для контроля шума и обеспечения большего сходства между носителем и секретным изображением. Архитектуру U-Net, в свою очередь, претерпела дальнейшую модификацию в [5] с целью для сохранения особенностей разных уровней (плоскости пикселей) изображения, что еще больше улучшило качество извлеченного изображения.

Все три упомянутых метода используют архитектуру кодер-декодер для сокрытия/извлечения сообщения, обеспечивая при этом достаточно высокий уровень скрытности стего-изображений. Однако, они различаются в механизмах сокрытия и устойчивости к атакам. Метод, описанный в [3] позволяет встраивать секретное изображение равномерно по всему изображению-контейнеру. В сравнении с StegNet и U-Net этот метод обеспечивает среднюю устойчивость к атакам и требует значительных вычислительных ресурсов. StegNet использует дополнительные механизмы для повышения устойчивости к атакам. U-Net, изначально разработанный для сегментации изображений, обеспечивает высокую эффективность в сокрытии и извлечении информации.

Можно отметить, что названия основных структурных компонентов НС «кодер» (encoder) и «декодер» (decoder) встречаются во многих моделях, где основу составляют иные механизмы стеганопреобразований в сравнении с описанными.

Стеганографические системы на основе генеративно-состязательных сетей (GAN). GAN (Generative Adversarial Network) [6] – это архитектура нейронных сетей, которая состоит из двух частей: генератора (Generator) и дискриминатора (Discriminator), которые обучаются в состязательной манере. Генератор создает новые данные (например, изображения) на основе входного шума. Дискриминатор оценивает, являются ли данные, представленные ему, настоящими (из обучающего набора данных) или созданными генератором.

В процессе обучения генератор «старается» обмануть дискриминатор, создавая все более реалистичные данные, а дискриминатор, в свою очередь, «старается» лучше отличать настоящие данные от сгенерированных.

К данному классу систем относятся ISGAN (Invisible Steganography via Generative Adversarial Networks – невидимая стеганография на основе генеративно-состязательных сетей) [7] и ABDH (Attention-Based Dual Hiding – двойное сокрытие, основанное на внимании) [8]. ISGAN использует стандартную архитектуру GAN, встраивая сообщение равномерно по всему изображению. В сравнении с ABDH ISGAN обеспечивает среднюю устойчивость к атакам. Обе модели требуют значительных вычислительных ресурсов и отличаются высокой сложностью обучения НС, но обеспечивают высокое качество стего-изображений и устойчивость к шумам.

Стеганографические системы на основе обратимых сетей. Обратимые НС позволяют не только получить выходные данные из входных, но и восстановить входные данные, используя выходные. Обратимые сети используют специальные слои, которые сохраняют всю информацию, позволяя восстановить исходные данные.

В стеганографических приложениях обратимые сети позволяют скрыть информацию в изображении таким образом, что её можно извлечь без потерь. При этом создаются стегоизображения, которые трудно отличимы от оригинальных, и обеспечивается точное восстановление скрытых данных. Среди стеганоалгоритмов на основе обратимых сетей выделим следующие: ISN (Invertible Steganography Network – сеть для обратимой стеганографии) [9], HiNet (Reversible Image Hiding Network – сеть для обратимого сокрытия изображений) [10], DeepMIH (Deep Multi-Image Hiding – сокрытие нескольких изображений на основе глубокого обучения сети) [11].

Все модели на основе обратимых сетей обеспечивают точное восстановление скрытой информации. Они требуют значительных вычислительных ресурсов. Сети сложны в обучении, но обеспечивают устойчивость к шумам.

Считается, что архитектуры сетей ISGAN, HiNet и DeepMIH реализуют передовыме методы стеганографии на основе НС, обеспечивая высокую скрытность и качество стего-изображений.

Стеганографические системы на основе переноса стилей. Перенос стилей – это задача компьютерного зрения, которая заключается в изменении стиля изображения, сохраняя его содержимое. Стиль одного изображения применяется к другому, сохраняя исходные контуры и объекты.

Модели сетей на основе переноса стилей [12] основаны на том, что скрываемое изображение применяется как стилевое оформление по отношению к изображению-контейнеру. Эта особенность используется при извлечении сообщения из стеганоконтейнера.

Сеть ISTNet (Image Style Transfer Network основана на преобразовании стиля изображение-контейнера в другое стегоизображение с совершенно другим стилем, учитывающим оформление осаждаемого сообщения. Эта сеть использует VGG-подобную архитектуру для извлечения признаков стиля и содержания.

Все модели на основе переноса стилей используют нейронные сети для переноса стиля из одного изображения на другое, что позволяет скрывать информацию в "стиле" изображения-контейнера. Эти методы обеспечивают высокую скрытность и устойчивость к стеганоанализу, так как изменения в "стиле" менее заметны для человеческого глаза и традиционных методов стеганоанализа. Модели требуют значительных вычислительных ресурсов. Сети требуют достаточно трудоемкого обучения, но обеспечивают высокое качество стего-изображений и устойчивость к шумам.

Схема стеганосистемы на основе стилизации применяет секретное изображение как стиль к изображению-контейнеру и использует дестилизацию для извлечения информации. Она обеспечивает среднюю устойчивость к атакам и среднюю пропускную способность. Размер скрываемого сообщения имеет ограничение, зависящее от сложности используемого стиля.

ЛИТЕРАТУРА

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

2. Урбанович П.П. Нейросетевые технологии в криптографических приложениях: [монография] / П.П. Урбанович, М.Д. Плонковски, М. Долецки. – Минск: БГТУ, 2024. – 221 с.

3. Baluja S. Hiding Images in Plain Sight: Deep steganography Advances in Neural Information Processing Systems. In: NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems, Long Beach California, USA, December 4 - 9, 2017. – NY: Red Hook, 2017. – P. 2069–2079.

4. Wu P., Yang Y., and Li X. Stegnet: Mega image steganography capacity with deep convolutional network. Future Internet. 2018, 10.6:54. – https://doi.org/10.3390/fi10060054.

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].