адаптивно визначає, чи просторові, чи частотні ознаки є більш інформативними для конкретного зразка. Навчання реалізовано зі стратегією transfer learning (заморожування backbone з наступним fine-tuning), LR warmup, cosine annealing та early stopping. Експериментальна оцінка на датасеті GenImage (зображення від 10+ генераторів: Stable Diffusion, GLIDE, BigGAN, StyleGAN3, VQ-Diffusion та ін.) показала accuracy 94.3%, F1-score 0.929, precision 0.907, recall 0.951 та ROC-AUC 0.976, що підтверджує високу ефективність гібридного підходу та його здатність надійно виявляти зображення від різноманітних генеративних моделей.

1. Verdoliva L. Media Forensics and DeepFakes: an overview. arXiv, 2020. URL: https://arxiv.org/pdf/2001.06564
2. Rafique R., Gantassi R., Amin R. та ін. Deep fake detection and classification using error-level analysis and deep learning. Scientific Reports (Nature), 2023. URL: https://www.nature.com/articles/s41598-023-34629-3
3. Epstein D.C., Jain I., Wang O., Zhang R. Online Detection of AI-Generated Images. ICCV Workshop, 2023. URL:https://openaccess.thecvf.com/content/ICCV2023W/DFAD/papers/Epstein_Online_Detection_of_AI-Generated_Images__ICCVW_2023_paper.pdf
4. Cozzolino D., Poggi G., Corvi R., Nießner M., Verdoliva L. Raising the Bar of AI-generated Image Detection with CLIP. CVPR Workshop, 2024. URL:https://openaccess.thecvf.com/content/CVPR2024W/WMF/papers/Cozzolino_Raising_the_Bar_of_AI-generated_Image_Detection_with_CLIP_CVPRW_2024_paper.pdf

Modern data hiding techniques: adaptivity, artificial intelligence and content synthesis

UDC 004.056:004.8 (043.2)

Artem Frolov[1], Vasyl Rizak[2]

Uzhhorod National University,
[1]artem.frolov@uzhnu.edu.ua, [2]vrizak@uzhnu.edu.ua

Modern steganography has evolved from simple data hiding in least significant bits (LSB) to complex methods that exploit machine learning and adaptive algorithms. The aim of this work is to analyze contemporary data hiding techniques that combine adaptive algorithms, neural network architectures and generative models, and to outline promising directions for further research.

1. Adaptive embedding based on distortion minimization. This is the “gold standard” of modern steganography: instead of embedding data uniformly, the algorithm analyses the content and identifies regions where modifications will be least detectable by steganalyzers. The mechanism relies on additive cost functions: each pixel is assigned a modification cost — pixels on object edges and in textured areas have low cost, while smooth surfaces (e.g. clear sky) have high cost. The key algorithms are: 1) S-UNIWARD, which operates in the spatial and frequency

domains; 2) HILL, which uses high-efficiency filters for cost estimation [1]. These methods remain the most difficult to detect with classical statistical analysis tools (SRM).

2. Generative adversarial networks (GAN-Steganography). This is a next-generation approach in which neural networks compete with one another: one tries to hide data, the other tries to detect it. The system consists of three parts: 1) an encoder that hides the data; 2) a decoder that extracts it; 3) a critic (discriminator) that tries to tell the "stego" apart from the original. During training the encoder learns to deceive the critic, producing visually flawless containers [2]. Unlike classical schemes, the message can be distributed across complex image features that are not described by simple mathematical formulas [3].

3. Coverless (generative) steganography. This method completely abandons modification of an existing file, which resolves the main problem of steganography — the presence of editing artefacts. The secret message is used as a seed for a generative model: the network synthesizes a realistic human face or a landscape, with the generation parameters (eye color, cloud shapes, etc.) themselves representing the encoded bits. Since no original container image ever existed, the analyzer has nothing to compare the result with.

4. Robust steganography for real-world channels (Robust Deep Stego). Most methods break down when the image is uploaded to social platforms (Facebook, Telegram, etc.), since these services compress the files (JPEG compression). During training of the neural network a "noise" layer is added that simulates JPEG compression, resizing or the addition of Gaussian noise. As a result, the network learns to hide data in those image components that are preserved even after aggressive processing by social network algorithms [4].

5. Linguistic steganography. This consists in using large language models (LLMs) to hide data in textual messages. While generating text (for instance, a chatbot response) the algorithm chooses between synonyms or alternative sentence constructions based on a secret key: choosing the word "automobile" instead of "car" may denote bit "0", and vice versa — bit "1" [5]. The resulting text appears entirely natural to a human reader, as it is produced by a modern language model that respects grammatical and stylistic norms [6].

Conclusions. The analysis of current trends in steganography allows us to highlight the following main directions: 1) a shift to intelligent embedding; 2) the dominance of neural network architectures; 3) a conceptual change of approach (coverless steganography); 4) adaptation to real-world transmission conditions; 5) multimodality of hiding. Modern steganography is becoming increasingly adaptive and context-aware: the main vector of development has shifted from the question "how to hide" to the question "how to make the intervention a natural part of a complex environment", where machine learning algorithms play the key role.

1. Holub V., Fridrich J., Denemark T. Universal distortion design for steganography in an arbitrary domain. EURASIP Journal on Information Security. 2014. Vol. 2014:1.
2. Volkhonskiy D., Nazarov I., Borisenko B., Burnaev E. Steganographic generative adversarial networks. Workshop on Adversarial Training,

Neural Information Processing Systems. 2016.
3. Tan S., Li B. Stacked convolutional auto-encoders for steganalysis of digital images. Asia-Pacific Signal and Information Processing Association, 2014 Annual Summit and Conference (APSIPA). IEEE, 2014. P. 1–4.
4. Zhu J., Kaplan R., Johnson J., Fei-Fei L. HiDDeN: Hiding Data with Deep Networks. Computer Vision – ECCV 2018. Springer, 2018.
5. Yang Z.-L., Guo X.-Q., Chen Z.-M., Huang Y.-F., Zhang Y.-J. RNN-Stega: Linguistic steganography based on recurrent neural networks. IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, No. 5. P. 1280–1295.
6. Ma Y., Liu X., Bai S., Wang L.-Y., Liu A., Tao D., Hancock E. Region-wise generative adversarial image inpainting for large missing areas. arXiv preprint arXiv:1909.12507. 2019.

Enhancing facial verification in surveillance systems through super-resolution preprocessing and multi-model embedding concatenation

UDK 004.93 (004.8)

Denys Khanin[1], Viktor Otenko[2]

Lviv Polytechnic National University, [1]denys.o.khanin@lpnu.ua, [1]viktor.i.otenko@lpnu.ua

Facial verification is a critical component of modern security infrastructure, yet its effectiveness in surveillance deployments is limited by two challenges: low-resolution (LR) imagery from cameras [1] and the vulnerability of single-model verification architectures [2]. This paper proposes an integrated pipeline combining super-resolution (SR) preprocessing with multi-model concatenated embedding verification. The approach builds on the experimental work on concatenated embeddings [3, 4] and comparative analysis of SR methods [5].

Experiments on the CFP dataset [6] evaluated verification using embeddings from VGG-Face, Facenet, Facenet512, OpenFace, ArcFace, and SFace in concatenated configurations [3]. The best concatenated configurations consistently outperformed individual models across accuracy and EER. A normalization study [4] revealed that sequential Z-Score followed by L2 normalization is optimal for multi-model concatenation.

Table 1

Verification performance: single models vs. concatenated embeddings on CFP dataset

Configuration	Accuracy, %	EER, %
Facenet512 (best single)	97.45	3.40
Facenet + Facenet512	**97.68**	**2.87**
All 6 models	96.67	3.92

The best pair (Facenet + Facenet512) achieved 97.68% accuracy with EER of 2.87%, outperforming the best single model by 0.23 percentage points, while the all-model concatenation showed lower performance (96.67%) due to noise from weaker