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

models. A comparative SR study [5] showed Real-ESRGAN [7] excels at real-world degraded images, while FSRNet [8] offers optimal speed-accuracy balance for face-specific tasks.

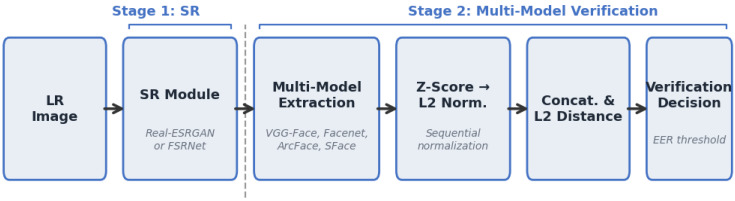

Fig.1. Architecture of the proposed SR-enhanced multi-model concatenated verification pipeline

The pipeline (Fig. 1) has two stages. Stage 1 enhances the LR image via SR (Real-ESRGAN or FSRNet). Stage 2 passes the enhanced image through multiple face recognition models; each embedding undergoes sequential normalization and concatenation before L2 distance verification against an EER-optimized threshold.

$$\hat{e}_i = \frac{(e_i - \mu_i)}{\sigma_i}, \quad then \quad \hat{e} = \frac{\hat{e}}{\|\hat{e}\|_2} \#(1)$$

where e_i is the raw embedding from model i, μ_i and σ_i are its mean and standard deviation, and $\|\cdot\|_2$ denotes the L2 norm. This ensures embeddings from heterogeneous models are harmonized before concatenation.

The pipeline is modular and each component can be updated independently. Multi-model architecture also provides security resilience, as compromising verification requires exploiting vulnerabilities across multiple models simultaneously. The primary trade-off is computational cost, acceptable for security-critical applications. Future work will focus on experimental validation on surveillance-specific datasets and real-time optimization.

1. Zou W.W., Yuen P.C. Very low resolution face recognition problem. IEEE Transactions on Image Processing. 2012. Vol. 21, No. 1. P. 327–340.
2. Goel R., Mehmood I., Ugail H. A Study of Deep Learning-Based Face Recognition Models for Sibling Identification. Sensors. 2021. Vol. 21. 5068.
3. Khanin D., Otenko V., Khoma V. Research on the effectiveness of concatenated embeddings in facial verification. CSDP-2024, Lviv Polytechnic National University, Lviv, Ukraine.
4. Khanin D. Comparative analysis of embedding normalization methods in face recognition systems. SCIFiC-2024, National Aerospace University "Kharkiv Aviation Institute".
5. Khanin D., Otenko V. Comparative analysis of super-resolution methods for improving face recognition accuracy. Computer Systems and Networks. 2025. Vol. 7, No. 1.
6. Sengupta S., Cheng J.C., Castillo C.D. et al. Frontal to Profile Face

Verification in the Wild. IEEE WACV. 2016.
7. Wang X., Xie L., Dong C., Shan Y. Real-ESRGAN: Training Real-World Blind Super-Resolution with Pure Synthetic Data. ICCV Workshops. 2021. P. 1905–1914.
8. Chen Y., Tai Y., Liu X. et al. FSRNet: End-to-End Learning Face Super-Resolution with Facial Priors. CVPR. 2018. P. 2492–2501.

Моделювання мережевих атак на основі аналізу графу мережевих взаємодій

УДК 004.056.55

Дмитро Хіжняк[1], Геннадій Шаповалов[2]

Національний університет «Одеська політехніка»,
[1]9480560@stud.op.edu.ua, [2]shapovalov@op.edu.ua

Сучасні комп'ютерні мережі функціонують в умовах постійного зростання кількості кіберзагроз. Особливо поширеними є атаки типу port scan, DoS/DDoS та brute force, які спрямовані на порушення доступності сервісів або отримання несанкціонованого доступу до систем [1]. Традиційні методи виявлення атак, засновані на сигнатурах, мають обмежену ефективність, особливо щодо нових або модифікованих типів атак [2].

Одним із перспективних підходів є використання графового аналізу, який дозволяє представити мережевий трафік у вигляді орієнтованого графа, де вузли відповідають IP-адресам або хостам, а ребра — мережевим взаємодіям між ними [3]. Такий підхід дає можливість враховувати структуру взаємозв'язків у мережі та виявляти аномальні патерни поведінки.

Метою роботи є моделювання мережевих атак **з** використанням графового аналізу та розробка застосунку для виявляти у мережі аномальних патернів поведінки.

Для оцінки поведінки вузлів використовується інтегральний показник аномальності, що формується на основі нормалізованих графових метрик, зокрема ступеня вершини, інтенсивності трафіку та кількості унікальних з'єднань:

$$z(x_t) = \frac{x - \mu_t}{\sigma_t},$$

де x_t - значення метрики в момент часу t (або у вікні Δt), μ_t та σ_t - середнє і стандартне відхилення метрики у базовому періоді (наприклад, у попередніх k вікнах).

За підходом, що використано в роботі, аналіз структури графа дозволяє виділити характерні ознаки можливих атак. Для port scan типовим є сценарій «один до багатьох», для DDoS — «багато до одного», тоді як brute force характеризується інтенсивними повторюваними з'єднаннями між обмеженою кількістю досліджуваних мережевих вузлів.

Реалізація запропонованого підходу виконана у вигляді програмного застосунку, що здійснює обробку flow-даних, побудову графа мережевих