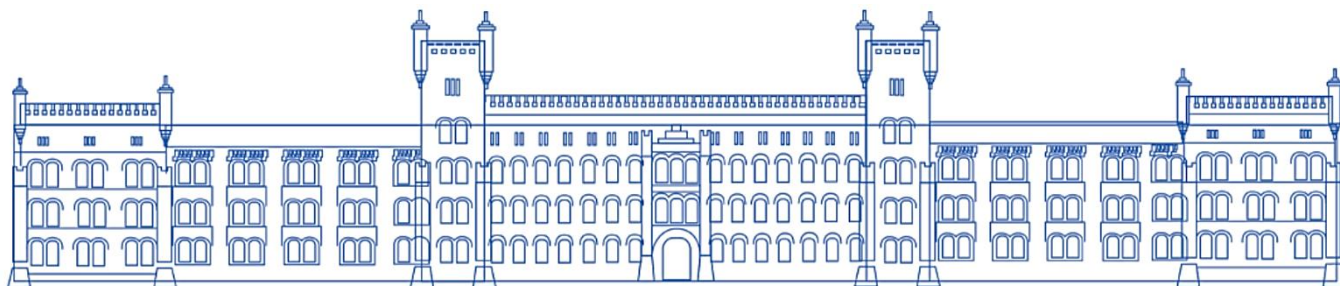




ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ



ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ

*Збірник тез доповідей
I Міжнародної науково-практичної конференції*

17-18 квітня 2025 року

Цивільний захист в умовах війни : збірник тез доповідей I Міжнародної науково-практичної конференції, м. Львів, 17-18 квітня 2025 року. Львів: ЛДУ БЖД, 2025. 296 с.

РЕДКОЛЕГІЯ:

Василь ЛОЇК	кандидат технічних наук, доцент, начальник кафедри цивільного захисту, ЛДУБЖД
Роман ЯКОВЧУК	доктор технічних наук, доцент, начальник факультету цивільного захисту ЛДУБЖД
Ольга МЕНЬШИКОВА	кандидат фізико-математичних наук, доцент, заступник начальника факультету цивільного захисту, ЛДУБЖД
Андрій ГАВРИСЬ	кандидат технічних наук, доцент, заступник начальника кафедри цивільного захисту, ЛДУБЖД
Олександр СИНЕЛЬНИКОВ	кандидат технічних наук, доцент, доцент кафедри цивільного захисту, ЛДУБЖД
Андрій ГАВРИЛЮК	кандидат технічних наук, доцент, доцент кафедри цивільного захисту, ЛДУБЖД
Павло БОСАК	кандидат технічних наук, доцент, доцент кафедри цивільного захисту, ЛДУБЖД
Андрій ТАРНАВСЬКИЙ	кандидат технічних наук, доцент, доцент кафедри цивільного захисту, ЛДУБЖД
Мар'ян ЛАВРІВСЬКИЙ	старший викладач кафедри цивільного захисту, ЛДУБЖД
Олександр ЛЮБОВЕЦЬКИЙ	старший викладач кафедри цивільного захисту, ЛДУБЖД
Володимир РИХВА	викладач кафедри цивільного захисту, ЛДУБЖД
Олександра ПЕКАРСЬКА	викладач кафедри цивільного захисту, ЛДУБЖД
Максим ДОВГАНОВСЬКИЙ	викладач кафедри цивільного захисту, ЛДУБЖД
Вікторія ФІЛІПОВА	викладач кафедри цивільного захисту, ЛДУБЖД

У збірнику тез I Міжнародної науково-практичної конференції «Цивільний захист в умовах війни» висвітлено досвід сучасних тенденцій й викликів в організації цивільного захисту в умовах війни, а також формування основних напрямків вдосконалення та розвитку системи цивільного захисту.

Для наукових, науково-педагогічних та педагогічних працівників закладів освіти, працівників наукових, виробничих установ, підрозділів ДСНС України, представників державних та місцевих органів влади, громадських і професійних організацій та здобувачів освіти.

Автори несуть особисту відповідальність за зміст представлених публікацій, достовірність результатів і дотримання вимог академічної доброчесності. Оргкомітет не несе відповідальності за порушення правил написання в друкованих авторських матеріалах.

REFERENCES

1. Hordiichuk-Bublivska, O. V. (2024). *Methods and means of big data processing in distributed information systems* (Ph.D. dissertation, Lviv). 150 pages.
2. Klymash, M. M., Mrak, V. B., & Hordiichuk-Bublivska, O. V. (2021). Research on methods for extracting dynamic objects in video sequences. *Infocommunication Technologies and Electronic Engineering*, (1), 63–75.
3. Ostian, Y. Z. (2024). Artificial intelligence and personal data: Privacy protection in the digital environment. *Scientific Bulletin of Uzhhorod National University*, (1), 47.
4. Dibrova, I. S., & Sichko, T. V. (2023). Security and privacy in databases. *Bulletin of the Student Scientific Society of Donetsk National University named after Vasyl Stus*, (1), 187.
5. Artificial intelligence and its impact on the ethical aspects of scientific research. (2023). *Academic Visions*, (22), 445–469.

УДК 004.415.24

DEEP LEARNING-DRIVEN AUDIO STEGANOGRAPHY FOR SECURE STATE-LEVEL COMMUNICATION: CHALLENGES AND STRATEGIC POTENTIAL

O.-S. I. Malets, O. O. Smotr
Lviv State University of Life Safety, Lviv

The integration of deep learning into audio steganography presents transformative possibilities for secure state-level communication, particularly in domains such as military operations and critical infrastructure systems. Audio steganography refers to the technique of concealing information within an audio carrier in such a way that the presence of the hidden message is undetectable to the human auditory system. Unlike encryption, which protects the content of a message but reveals its existence, steganography provides a complementary form of security by ensuring that sensitive data transmission remains covert. Traditional audio steganographic methods, such as Least Significant Bit (LSB) embedding, have been widely used due to their simplicity and minimal computational requirements. These approaches typically allow embedding of approximately 176 kB of hidden data per minute in a 44.1 kHz, 16-bit stereo audio file, depending on the compression ratio and embedding density. However, they suffer from significant vulnerabilities, including low robustness to signal manipulation (e.g., filtering, compression), limited payload capacity, and an inability to adapt dynamically to changes in the communication environment [1,2].

Deep learning offers a paradigm shift in this space by enabling intelligent, context-aware audio embedding and extraction mechanisms. Neural network architectures—such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformers—allow the model to analyze both local and global signal characteristics to identify optimal regions for data insertion. For instance, CNNs are particularly effective at learning spectral features of audio signals in the frequency domain, making them suitable for embedding data in perceptually insignificant regions. RNNs and LSTMs (Long Short-Term Memory networks) can exploit temporal dependencies to maintain consistency and coherence in the steganographic signal across time. More recently, transformer-based models, originally developed for natural language processing, have been adapted to audio due to their ability to capture long-range dependencies and dynamically reweight feature importance using attention mechanisms [3,4]. These advancements not only increase embedding efficiency and reduce signal degradation but also facilitate training of highly generalizable models capable of operating across a variety of audio formats and signal types.

An emerging trend in this field is the use of generative adversarial networks (GANs) to create more robust steganographic systems. In such setups, a generator network encodes data into an audio file while a discriminator attempts to detect the presence of hidden information. By training both

networks simultaneously in an adversarial manner, the system becomes increasingly capable of producing stego-audio that closely mimics the distribution of natural audio, thereby improving undetectability and resilience against steganalysis [5,6]. Additionally, autoencoders and variational autoencoders (VAEs) are employed for end-to-end encoding-decoding workflows, enabling joint optimization of the steganographic payload, audio quality, and noise resilience. These systems often incorporate error-correction schemes and signal quality monitoring during both encoding and decoding, allowing them to operate effectively in real-world transmission conditions that include packet loss, dynamic bitrates, and variable environmental noise.

From a performance perspective, deep learning-based methods can increase data payloads by up to 20–25%—achieving 210–220 kB per minute—without significantly compromising audio quality. More importantly, these models are able to preserve perceptual transparency even under lossy compression schemes such as MP3 or AAC, where traditional LSB methods often fail. Furthermore, these systems exhibit strong adaptability: by monitoring signal distortions during transmission, some models can dynamically adjust embedding strategies using online learning or reinforcement learning techniques. For example, in a battlefield communication scenario, an AI-driven steganographic model could automatically reduce embedding density in high-noise conditions to maintain signal intelligibility while preserving the covert channel.

The strategic applications of such techniques are broad and critically important. In military communications, deep learning-based audio steganography allows encrypted messages or mission-critical metadata to be embedded into ordinary-sounding voice transmissions or music files, evading detection by adversarial surveillance systems. Similarly, in critical infrastructure domains—such as energy grids, transportation systems, and water treatment facilities—SCADA commands can be covertly transmitted over secured but publicly observable networks, thus protecting command integrity while reducing exposure to cyber-attacks. These methods provide a covert security layer that can operate in tandem with traditional cryptographic systems, offering both deniability and resilience. For example, in a scenario involving cross-border field communications, soldiers could transmit encoded situational updates embedded within standard operational radio chatter, ensuring that even intercepted signals do not reveal sensitive intent or structure.

Despite their potential, deep learning-based steganographic systems are not without limitations. One key concern is the computational overhead involved in training and deploying high-capacity models, particularly in constrained environments such as embedded systems or mobile devices. Moreover, model interpretability remains a challenge; many of these systems operate as black boxes, making it difficult to guarantee consistent behavior across unseen inputs. Finally, adversarial attacks targeting the stego-system—such as adversarial perturbations or model inversion—pose ongoing risks and require continuous research to develop robust countermeasures.

In conclusion, the synergy between deep learning and audio steganography represents a significant advancement in the secure transmission of state-sensitive data. By leveraging neural networks' ability to learn complex representations of audio and adapt to environmental noise and variability, these systems offer a scalable, covert, and resilient platform for communication under high-risk or adversarial conditions. As the geopolitical and cyber threat landscape continues to evolve, the importance of such techniques will only grow—positioning deep learning-based steganography as a cornerstone of next-generation information security infrastructures.

REFERENCES

1. K. M. M. Tantawi, A. S. Tolba, and A. M. Badr, “High capacity audio steganography based on LSB and genetic algorithm,” *Multimedia Tools and Applications*, vol. 80, pp. 2575–2595, 2021.
2. J. Song, C. Zhang, X. Liu, and Y. Zhang, “StegaStamp++: Invisible and Robust Message Embedding via Joint Optimization,” *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 2381–2390, 2022.
3. H. Kim, Y. Choi, and H. Lee, “Transformer-Based Audio Steganography Using Attention Mechanism,” *IEEE Access*, vol. 9, pp. 118765–118774, 2021.

СЕКЦІЯ 5 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЇ

АВТОМАТИЗОВАНА ПЛАТФОРМА ФОРМУВАННЯ ПЛАНІВ ВИКЛАДАЧІВ ЯК ІНСТРУМЕНТ ЦИФРОВІЗАЦІЇ ОСВІТИ У СФЕРІ БЕЗПЕКИ

Д. Цветков, Д. Райта185

АНАЛІЗ ВПЛИВУ ЛІСОВИХ ПОЖЕЖ НА ІНТЕНСИФІКАЦІЮ ЗСУВНИХ ПРОЦЕСІВ

О.О. Карабин, В.В. Карабин, І.М. Кордіяка186

ВАЖЛИВІСТЬ МАТЕМАТИКИ У ЦИВІЛЬНОМУ ЗАХИСТІ

О.М. Трусевич188

ВИКОРИСТАННЯ 3D-МОДЕЛЮВАННЯ ТА ТЕХНОЛОГІЇ UNREAL ENGINE У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ РЯТУВАЛЬНИКІВ В УМОВАХ ВІЙНИ

С.С. Мезенцев, В.М. Пилипенко190

ДИНАМІЧНА СТІЙКІСТЬ РОБОТІВ З КІНЦІВКАМИ: НОВІТНІ ДОСЯГНЕННЯ ТА АКТУАЛЬНІ ПРОБЛЕМИ.

Д. Котелевич, Ю. Борзов192

ЗАСТОСУВАННЯ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ ОЦІНКИ ТЕХНІЧНОГО СТАНУ ЗРУЙНОВАНИХ БУДІВЕЛЬ ТА ІНФРАСТРУКТУРИ В УМОВАХ ВІЙСЬКОВИХ КОНФЛІКТІВ

А. Титаренко, І. Несен193

ЗАСТОСУВАННЯ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ПІДВИЩЕННЯ ПРОГНОЗУВАННЯ ЗАТОПЛЕНЬ З УРАХУВАННЯМ ІСТОРИЧНИХ ДАНИХ ТА ПОТЕНЦІЙНИХ ЕКОЛОГІЧНИХ ЗАГРОЗ

А.П. Гавриць, О.О. Пекарська.....195

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ЗДОБУВАЧІВ ОСВІТИ ДО ЗАХИСТУ В УМОВАХ ЗАГРОЗИ ТА ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

В.С. Петренко, О.М. Саух197

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОПЕРАТИВНОМУ РЕАГУВАННІ: АНАЛІЗ І ОПТИМІЗАЦІЯ РІШЕНЬ ДЛЯ ПІДРОЗДІЛІВ ДСНС УКРАЇНИ

Г.С. Босак, Р.М. Головатий199

КАТЕГОРИЗАЦІЯ ВИДІВ ПОЖЕЖ ЗА ОПИСОМ ОБ'ЄКТУ ПОЖЕЖІ

О.М. Шопський, І.О. Малець, Р.О. Гриник201

КІБЕРЗАГРОЗИ В УМОВАХ ВІЙНИ: ШЛЯХИ ЗМІЦНЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ ТА БОРОТЬБА З ЦИФРОВИМИ АТАКАМИ

О.Г. Мельник, Р.П. Мельник.....202

КІБЕРГІГІЄНА: ОСНОВИ БЕЗПЕЧНОЇ ПОВЕДІНКИ В ЦИФРОВОМУ ПРОСТОРІ	
С.В. Гончар, І.С. Крапивний	205
ОНЛАЙН-ПЛАТФОРМА ДЛЯ НАВЧАННЯ ТА ПЕРЕКВАЛІФІКАЦІЇ ВЕТЕРАНІВ У СФЕРІ БЕЗПЕКИ ТА ЦИВІЛЬНОГО ЗАХИСТУ НА БАЗІ JAVA SPRING	
В. Білецький, Д. Райта	206
ПРО ЗНАХОДЖЕННЯ СХЕМИ ЕЛЕКТРОПОСТАЧАННЯ ЗАСОБАМИ ПАКЕТУ MAPLE	
О.Ю. Чмир	207
ПРОАНАЛІЗОВАНО СИСТЕМУ МОНІТОРИНГУ АТМОСФЕРНОГО ПОВІТРЯ. ЗАПРОПОНОВАНІ ШЛЯХИ ЗМЕНШЕННЯ ЗАБРУДНЕННЯ АТМОСФЕРНОГО ПОВІТРЯ	
О.М. Мамайкін, Р.В. Данильченко, Ю.І. Чеберячко	209
РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ КООРДИНАЦІЇ ВОЛОНТЕРСЬКИХ ІНІЦІАТИВ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ	
Д. Федорук, Р. Головатий.....	211
РОЗПІЗНАВАННЯ ФРАГМЕНТІВ ЗОБРАЖЕННЯ, ОТРИМАНОГО З ЛІДАРА, ПІД ЧАС ПОШУКОВИХ РОБІТ	
О.А. Кузик, Н.Є. Бурак, О.В. Придатко	212
СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ ЗДОРОВ'Я В УМОВАХ ВІЙНИ	
В.Ю. Миронюк, Ю.С. Назар	214
ЦИФРОВА МОДЕРНІЗАЦІЯ ВЕБ-СИСТЕМИ ЗМАГАНЬ РЯТУВАЛЬНИКІВ У КОНТЕКСТІ ЦИВІЛЬНОГО ЗАХИСТУ	
М. Мусянович, Д. Райта	216
APPLICATION OF MACHINE LEARNING FOR ASSESSING THE IMPACT OF LOWER LIMB PROSTHETICS ON EVACUATION DURATION	
O.V. Khlevnoi, N.V. Zhezlo-Khlevna	218
MODERN DATA PROCESSING METHODS IN AUTOMATED SYSTEMS	
D.D. Smyk , N.Ye. Burak	220
DEEP LEARNING-DRIVEN AUDIO STEGANOGRAPHY FOR SECURE STATE-LEVEL COMMUNICATION: CHALLENGES AND STRATEGIC POTENTIAL	
O.-S.I. Malets1, O.O. Smotr	222
INFORMATION AND ANALYTICAL TECHNOLOGIES FOR SUPPORTING MANAGEMENT DECISIONS IN EMERGENCY SITUATIONS	
O.R. Staso, N.Ye. Burak	224
ВИКОРИСТАННЯ ІННОВАЦІЙНИХ МЕТОДІВ ФІЗИЧНОГО ТРЕНУВАННЯ	
С. Антошук, І. Шутяк	226