Application of Statistical and Neural Network Algorithms in Steganographic Synthesis and Analysis of Hidden Information in Audio and Graphic Files*

Yuliia Kostiuk[1,†], Pavlo Skladannyi[1,2,*,†], Karyna Khorolska[1,†], Volodymyr Sokolov[1,†] and Hennadii Hulak[1,2,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine*
[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680 Kyiv, Ukraine*

Abstract

This paper presents a hybrid approach for steganographic embedding and detecting information within audio and graphical containers, utilizing statistical analysis and neural networks. This study establishes the feasibility of employing auto-associative networks for steganographic synthesis and the Cumulative Sum (CUSUM) algorithm for identifying structural changes introduced by hidden content. A comparative analysis evaluates its effectiveness against other methods, including the Least Significant Bit (LSB) technique and the short-time Fourier Transform Combined with a Deep Neural Network (STFT-DNN). The findings demonstrate the superiority of the proposed hybrid architecture in terms of detection accuracy, Bit Error Rate (BER), and peak Signal-to-Noise Ratio (PSNR). Furthermore, the research investigates the efficacy of combined steganography analysis algorithms designed to operate under limited a priori information conditions and high container variability. The results underscore the significant potential of integrating machine learning and statistical modeling to develop intelligent digital security systems to counter hidden threats, protect copyright, and detect manipulative content in the contemporary information environment.

Keywords

steganography, steganalysis, hidden information, audio container, graphic container, statistical modeling, neural networks, autoencoder, digital security

1. Introduction

The rapid proliferation of digital technologies and the corresponding growth of multimedia content, particularly graphic and audio files, have escalated threats related to confidential information leakage, covert data exchange, and copyright infringement. In this context, steganographic methods, which involve embedding messages within digital media, are becoming critically important as tools for ensuring information security. Audio and graphic files serve as effective containers for hidden information due to their large capacity, inherent signal redundancy, and the insensitivity of human perception to minor distortions, facilitating the effective masking of embedded data.

However, traditional steganographic methods, such as least significant bit (LSB) substitution, discrete cosine transform (DCT), and discrete wavelet transform (DWT), exhibit limited resilience against modern steganalysis techniques. Moreover, classical statistical approaches are often insufficient for detecting complex or adaptive forms of hidden data, especially under conditions of active digital monitoring. In response to these limitations, current research is focused on developing hybrid methods that integrate statistical analysis with deep learning algorithms, such as

* *CQPC 2025: Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladannyi); k.khorolska@kubg.edu.ua (K. Khorolska); v.sokolov@kubg.edu.ua (V. Sokolov); h.hulak@kubg.edu.ua (H. Hulak)
0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0003-3270-4494 (K. Khorolska); 0000-0002-9349-7946 (V. Sokolov); 0000-0001-9131-9233 (H. Hulak)

autoencoders, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs).

These intelligent models facilitate the creation of embedded structures that replicate the natural statistics of the host container, thus minimizing artifacts detectable by conventional steganalysis. Autoencoders, for instance, generate a latent representation of the message, allowing data to be embedded without significantly altering the signal. Similarly, Generative Adversarial Network (GAN) models can produce containers that carry hidden information and maintain a statistical distribution consistent with the original media. Conversely, modern steganalysis employs classifier ensembles, change-detection algorithms (e.g., PCA or SVM), and deep neural detectors. These detectors are trained on contrasting examples of authentic and steganographic files, enabling them to identify modified containers even when the embedded signal is faint.

In the context of digital censorship and evolving cyber threats, the primary requirements for effective steganographic systems include the undetectability of transmission, accuracy of message reconstruction, resilience to attacks and distortions (such as JPEG compression or noise), and adaptability to various media types. Integrating statistical estimation and neural network processing is pivotal for achieving a higher steganography analysis and synthesis standard. For instance, statistical indicators such as mean, variance, and correlation coefficients can be employed to assess the vulnerability of specific regions within an image or audio file to steganographic embedding [1, 2]. Concurrently, neural network components are utilized for the actual data insertion or detection, ensuring an optimal balance between embedding efficiency and imperceptibility [3, 4].

This study uses statistical and neural network algorithms to analyze modern hybrid methods for embedding and detecting hidden information within graphic and audio files. The primary focus is on intelligent models capable of robustly encoding hidden data, even when subjected to digital attacks or censorship filters. The paper proposes a steganographic system architecture comprising modules for statistical evaluation, neural network-based container generation, deviation analysis, and Explainable AI (XAI) for interpreting and identifying hidden features. The system was evaluated on open audio and graphic datasets, using PSNR, SSIM, BER, and AUC/ROC as performance metrics for steganalysis. The results demonstrate that these hybrid methods outperform traditional models in accuracy and detection resistance.

Consequently, integrating statistical and neural network algorithms for steganographic synthesis and analysis presents significant potential for developing flexible, adaptive, and reliable information protection systems in the rapidly evolving digital landscape. The applications for such systems extend beyond privacy protection to include digital watermarking, cybersecurity, anti-censorship measures, and secure data storage.

2. Literature analysis review

In modern steganography research, deep learning methods are being actively implemented to enhance information concealment and detection efficiency. Specifically, Pham Huu Quang et al. [5] proposed a steganography method that utilizes deep neural networks to embed audio signals into images. Their approach effectively preserves the integrity of the host image and the audio data, demonstrating superior performance over traditional methods. In the field of steganalysis, Ghasemzadeh and Kayvanrad [6] conducted a comprehensive review of audio steganography detection methods, emphasizing that the combination of feature calibration and higher-order statistical moments can significantly improve the accuracy of identifying hidden messages.

In 2019, Felix Kreuk et al. [7] introduced a speech steganography approach that integrates the short-time Fourier transform (STFT) and its inverse as differentiable layers within a deep neural network. This architecture allows for effectively embedding messages into audio signals while preserving speech quality and ensuring robustness against distortions. In 2023, Mohamed C. Ghanem et al. [8] developed the StegoHound method, which integrates multiple approaches for effectively detecting and extracting digital evidence concealed within WAV and MP3 files using

steganographic techniques. This method demonstrates superior accuracy and broader detection capabilities compared to conventional systems, particularly in analyzing large audio files. Recent research indicates a clear trend toward integrating statistical methods with neural network architectures to develop more robust and effective steganographic systems.

3. Models and methods

This study employed a comprehensive approach to the steganographic synthesis and analysis of hidden information within audio and graphic files, leveraging methods from mathematical statistics, probabilistic modeling, and decision theory. This framework facilitated the development of generalized mathematical models for embedding and detecting hidden messages. These models account for both the structural characteristics of the host container and the parameters of external influences, such as digital noise, distortions, and compression.

Artificial neural networks constitute the core of the software implementation, enabling automatic feature extraction and the adaptive processing of complex media signals. Specific network architectures were selected based on the media type: autoencoders were employed for steganographic data compression and recovery tasks; convolutional neural networks (CNNs) were utilized for graphic files, where preserving the spatial correlation of pixels is crucial; and recurrent neural networks (RNNs), particularly Long Short-Term Memory (LSTM) variants, were applied to audio signals, which are characterized by a sequential temporal structure.

All algorithms were implemented using object-oriented programming principles, ensuring a flexible and modular system design that facilitates code reusability and scalability. Comprehensive testing was conducted to validate the performance of the developed models. This evaluation included statistical assessment methods, such as error analysis and detection probability calculations, and simulation modeling within a variable digital environment. The simulations incorporated various real-world conditions, including the addition of noise, re-encoding, and truncation of media file fragments.

The experimental results confirmed that integrating statistical methods and neural network algorithms enables high-accuracy detection of hidden information, even in significant noise or aggressive digital interference with the host containers. Furthermore, this combined approach provides adaptability to various media data formats and types, a feature of critical importance in real-world applications such as digital watermarking, secure message storage, and covert data transmission under censorship or information blockade.

4. Main material

As cyber threats escalate and digital communications face increasing scrutiny, steganography is becoming an essential tool for covert data transmission. In contrast to cryptography, which obscures the content of a message, steganography conceals the existence of the communication itself, a critical feature for circumventing surveillance and censorship. Consequently, integrating neural networks and statistical methods into steganographic systems is a rapidly advancing area of research, significantly enhancing the efficiency of embedding and detecting information within audio and graphical containers [7, 9].

The paper presents a mathematical model of a stego system and discusses approaches to stego synthesis and stego analysis, particularly using autoassociative, convolutional, and feed-forward neural networks [5–9]. The basis of functioning is formalized through a pair of functions. F_1 and F_2, $F_1(z, d)$ is responsible for embedding a message d in a container z, a $F_2(\tilde{z})$ is responsible for its recovery while minimizing distortion:

$$z = F_1(z, d), |z - \tilde{z}| \longrightarrow min, \quad (1)$$

$$d = F_2(\tilde{z}), \left| d - \tilde{d} \right| \to min.$$

where F_1 is the embedding function, F_2 is the extraction function. Eq. (1) describes a generalized steganographic model in which a function modifies a container z, F_1 with an embedded message d, and the inverse function F_2 allows recovery of this message [5–7]. Within the framework of steganography, the main condition is to minimize the distortion of the container $\left| z - \tilde{z} \right|$, which ensures the invisibility of the embedded data, as well as the accuracy of extraction $\tilde{d} \approx d$, which ensures the reliability of transmissions.

Fig. 1 shows the architecture of a two-component neural system for steganography: model (a) implements the embedding of messages in a container vector with minimal distortion using a two-layer auto-associative network [9], and model (b) is a feed-forward neural network that classifies hidden content based on statistical and structural deviations, learning from "clean" and modified containers [6, 10]. For efficient information embedding, it is advisable to use a two-layer auto-associative neural network with the number of neurons in the hidden layer equal to the container dimension $g = n$ (Fig. 1a). This architecture ensures compression, adaptation to the digital environment (audio or graphics), and resistance to attacks. For information extraction, feed-forward neural networks are used (Fig. 1b), which implement a binary decision rule necessary for message reconstruction [7].

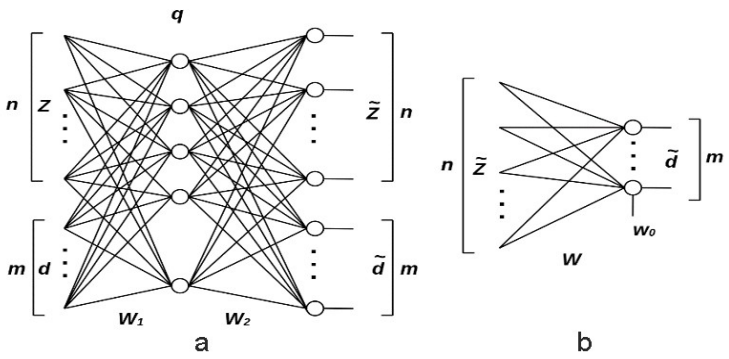

Figure 1: Architecture of a neural steganography system: (a) auto-associative network for embedding a message, (b) feed-forward network for extracting a message.

In digital steganography, there is a growing interest in intelligent models that facilitate both adequate concealment and accurate detection of information embedded within digital containers. This encompasses steganographic synthesis (the embedding of hidden data) and steganalysis (the detection of hidden content), which are increasingly implemented using artificial neural networks of various architectures [9, 11]. Convolutional Neural Networks (CNNs) excel at identifying local anomalies in images and audio spectrograms that arise from covert embedding processes [11–13]. Autoencoders enable message concealment within their latent representations with minimal container distortion, proving effective in both graphic and audio domains [5, 14]. Recurrent Neural Networks (RNNs) are adept at processing sequential data, such as audio and video, by accounting for temporal dependencies, which are particularly important for dynamic signals. Deep Neural Networks (DNNs) perform multilevel signal transformations, detect latent patterns, and integrate diverse features (statistical, spatial, spectral) to classify and identify hidden content [6, 15–17]. These advanced architectures allow for the development of adaptive steganographic systems that can operate effectively in complex environments with limited a priori information, providing high accuracy and robust resistance to steganalysis.

The effectiveness of embedding and recovering hidden data is quantified using several digital signal quality metrics. The Peak Signal-to-Noise Ratio (PSNR) measures the degree of container distortion after message embedding [9], while the Structural Similarity Index Measure (SSIM) assesses the perceptual similarity between the original and the modified object [18]. Additionally,

the Bit Error Rate (BER) determines the proportion of errors that occur during the reconstruction of the hidden message [19]. These metrics facilitate an objective assessment of a steganographic system's quality, particularly its ability to preserve the visual or auditory integrity of the container while ensuring the accurate extraction of hidden information.

Fig. 2 illustrates the architecture of a neural network designed for the steganographic embedding and subsequent analysis of audio and image files. The model comprises an input layer, a hidden layer with g neurons, and an output layer that yields the modified container and the recovered message. This core structure is augmented by several specialized modules: a steganalysis module for performance evaluation using PSNR, SSIM, and BER metrics; a cryptographic module responsible for encryption, key management, and integrity verification; and an Explainable AI (XAI) module that utilizes methods such as SHAP and LIME for decision interpretation [11, 12]. This integrated design results in a flexible, adaptive, and resilient system with high accuracy and operational transparency.

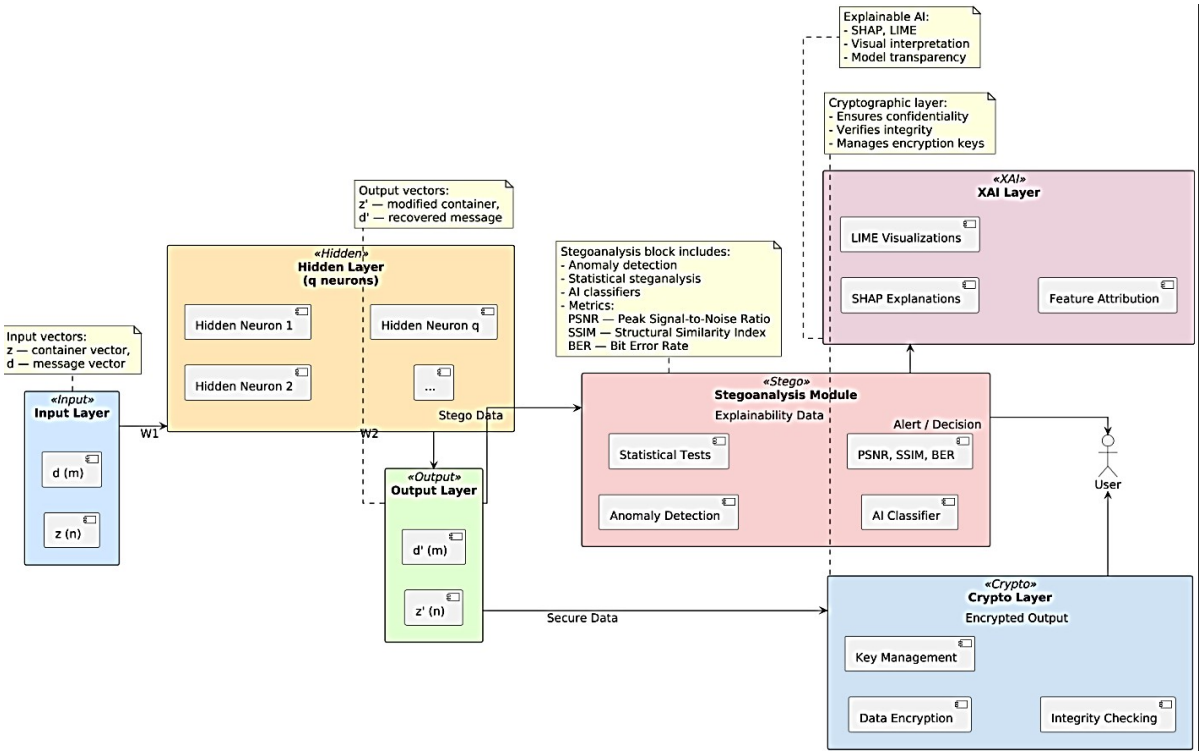

Figure 2: Neural network architecture for steganographic embedding and information analysis.

The signal supplied to the input of a neural network that implements steganographic information synthesis (SIS) can be represented as a combined vector [7–9, 14, 20]:

$$y=\begin{pmatrix} z^T \\ d^T \end{pmatrix}=y_1+y_2, \tag{2}$$

$$\begin{aligned} y_1&=(z_1,z_2,\ldots,z_n,0,\ldots,0)^T, \\ y_2&=(0,\ldots,0,d_1,\ldots,d_m)^T, \end{aligned} \tag{3}$$

where $d=\{d_1,\ldots,d_m\}$ is a vector containing the elements of the message to be hidden.

In the case of hiding a complete message, which forms a data sequence $d^{(p)}$, $p=1,\ldots,P$, each of its elements corresponds to a separate fragment of the container described by the vector $z^{(p)}$, where $p=1,\ldots,P$ [10, 12]. At the output of the pre-trained neural network, a sequence of modified fragments of the container $\acute{z}^{(p)}$, is formed, which already contains hidden information.

The neural network is trained using a back-propagation algorithm to minimize the Mean Squared Error (MSE) between the original message and the reconstructed data extracted from the modified container. This approach provides practical steganographic synthesis, especially in processing audio signals and graphic files with high dimensionality and complex structure [10, 13]. In addition, considering the container's local properties, element-by-element embedding increases the resistance to detection, including steganalysis attacks based on statistical and neural network methods.

However, modern steganalysis can detect even minor deviations in the statistical characteristics of the signal resulting from modifications during embedding. In particular, analyzing residual noise, spectral density, and local entropy allows you to form features sensitive to hidden content. Neural network steganalysers trained on a large number of examples of both clean and modified containers demonstrate a high ability to classify such embeddings. In this regard, testing for resistance to such attacks is necessary to evaluate the effectiveness of any steganography method.

To analyze the regularities of the steganographic information synthesis (SIS) process, within the framework of the proposed approach, a statistical model of the container is considered, according to which each fragment of the container is considered as a realization of a random vector z, with zero mathematical expectation and a known correlation operator [21]:

$$E[z]=0,\ E[z\,z^T]=R_z. \tag{4}$$

The elements of the sequence of the embedded message d are modeled as independent realizations of a binary random variable d_i, which does not depend on the container z and has an equal probability distribution:

$$P(d_i=1)=0.5,\ P(d_i=-1)=0.5,\ E[d_i]=0,\ E[d_i^2]=\sigma_d^2=1. \tag{5}$$

The statistical representation of the container z and the message d allows us to estimate the effect of the embedded information on the signal distribution, which is critical for imperceptible embedding without significantly changing the correlation characteristics [11, 15]. To do this, it is advisable to use a neural network with the number of neurons in the hidden layer one unit less than the input/output dimension (Fig. 1a), which provides compression and adaptation to data statistics [7, 12]. The model of the container as a zero random vector with a known correlation operator allows us to identify how hidden data changes its distribution, which is the basis of effective steganalysis.

The neural network is trained on a set of realizations of the input vector:

$$y^{(p)}=\begin{pmatrix} z^{(p)} \\ d^{(p)} \end{pmatrix},\ p=1,\dots,P, \tag{6}$$

by minimizing the mean square functional of the recovery error:

$$E=\frac{1}{P}\sum_{p=1}^{P}\left(y^{(p)}-W_2W_1y^{(p)}\right)^T\left(y^{(p)}-W_2W_1y^{(p)}\right), \tag{7}$$

where W_1 and W_2 weight matrices of the neural network [22]. This approach minimizes container distortion and prevents detection of hidden information by using modern steganalysis tools, particularly those based on artificial intelligence and deep learning.

The neural network for SIS functions as an intelligent encoder that learns to embed the message $d^{(p)}$ into the structure of the container $z^{(p)}$ with minimal distortion and ensuring reliable extraction [13, 17]. To detect data, a second network is used that performs classification by

detecting changes in the statistical characteristics of the signal. This combination of architectures guarantees high secrecy, decoding accuracy, and attack resistance. Neural network methods allow building adaptive, scalable, and invisible steganography systems suitable for information security, digital forensics, copyright protection, and media cybersecurity.

The auto-associative architecture minimizes distortion and residual traces, preserving the features of the container and balancing between secrecy and quality [22]. Adapting to local signal features forms a stable internal representation capable of carrying hidden information. During training, compression is performed with minimal distortion, which allows masking data in audio and graphic files without losing visual or acoustic quality. The system preserves the statistical and structural integrity of the container, providing effective and subtle hiding even in complex multimedia environments.

However, these properties make a container (a multimedia file containing hidden information) vulnerable to deep steganalysis, detecting hidden messages by analyzing statistical and structural changes in data. Such analysis focuses on detecting minor changes resulting from steganographic embedding, even if they are subtle visually or acoustically, but manifest themselves in high-dimensional feature spaces (i.e., in many statistical signal characteristics).

For this purpose, spectral filtering methods are used (analysis of the frequency components of the signal, for example, using a discrete cosine or Fourier transform), PCA (Principal Component Analysis), which allows to detect changes in the internal structure of data by reducing their dimensionality, and anomaly detection methods (i.e., algorithms that look for unusual or atypical deviations from the expected behavior of data).

Particular attention is paid to changes in the distributions of auto-encoder residuals, which are the differences between the input and the reconstructed signal in an auto-encoder (a neural network that learns to compress and reconstruct data). If these residuals show systematic deviations, it can serve as an indicator of hidden content.

Thus, even if masking (i.e., hiding information) is performed using an auto-associative architecture (an auto-encoder that learns to reproduce itself), it still needs to be tested for resistance to modern steganalysis algorithms—otherwise, there is a risk of detecting a hidden message even in a complex multimedia environment.

As a result of the theoretical analysis, the following statement has been proved: the transformation performed by a linear two-layer auto-associative neural network (Fig. 1a) trained according to the criterion of minimizing the mean square error is equivalent to the use of a linear operator [17, 21]:

$$W = R_{yn} R_{yn}^{+} = W_2 W_1, \tag{8}$$

where R_{yn} is the singular (degenerate) matrix formed based on the sample covariance matrix between the input data $y^{(p)}$, R_{yn}^{+} is its pseudo-inverse matrix in the Moore-Penrose sense, q is the number of neurons in the hidden layer, $m+n-q$ is the number of discarded (zeroed) eigenvalues in the diagonalization process.

Thus, the neural network implements the optimal linear mapping with compression, preserving the statistically significant components of the vector y, which includes the container z and the message d [5, 9, 14, 22]. To evaluate the possibility of recovering hidden data in the process of steganographic synthesis, the paper proposes a methodology for analyzing the statistical characteristics of the original vector z after processing by a neural network [13, 21]. In particular, deviations from the original distribution, changes in the covariance structure, and the possibility of using steganalysis methods to detect hidden content are evaluated. This approach allows us to form a formalized detection profile based on the empirical patterns inherent in modified containers. The spectral and autocorrelation analysis will enable us to detect anomalous patterns characteristic of the influence of steganographic embeddings. Classifiers trained on feature vectors that include changes in entropy and local consistency are also involved in improving the detection accuracy.

Thus, steganalysis is essential in assessing the method's resistance to unauthorized detection of hidden information.

The neural network (Fig. 1a) is fed with test signals that model hypothetical states of a hidden message [7]:

1. $y^{+}=(0,0,\ldots,0,1)^{T}$ is a signal that corresponds to the hypothesis H_1 (presence of bit "+1" in the message);
2. $y^{-}=(0,0,\ldots,0,-1)^{T}$ is a signal that corresponds to the hypothesis H_2 (presence of the "–1" bit).

The output of the neural network generates vectors y^{+} and y^{-}, which can be represented as:

$$y^{\pm}=\left(\frac{m^{\pm}}{d}\right)=W_2 W_1 y^{\pm}, \tag{9}$$

where $m^{\pm}$ is the mathematical expectation (average values) of the useful signal that corresponds to the hypotheses about the value of the hidden bit.

Next, to assess the impact on the structure of the container, we analyze the covariance matrix of the output signal (only the first n components corresponding to the container vector z), when a random vector $y_x=(z_1,z_2,\ldots,z_n,0)^{T}$ is applied. To do this, the matrix is calculated:

$$\widetilde{R}=W_2 W_1 R_y W_1^{T} W_2^{T}, \tag{10}$$

where R_y is the covariance matrix of the input signal. The block part $\boxtimes_z$, is extracted from it, which corresponds to the submatrix for the container.

As a result, the output signal can be represented as:

$$z=\alpha\, m^{+}+(1-\alpha)\, m^{-}+\eta, \tag{11}$$

where $\alpha=1$ for $d=1$, $\alpha=0$ for $d=-1$, and η is a fluctuating noise that models the residual content of the container [10, 12]. This expression shows how the structure of the container changes due to steganographic embedding: the signal z is the sum of mathematical expectations for the corresponding bit and the noise component [6, 15]. These changes allow us to build adequate detectors for detecting embedded information even under distortion. For this purpose, steganalysis uses methods for estimating residual noise η, which are key indicators of the presence of a hidden message. In particular, analyzing the moving average, variance, and higher statistical moments allows us to identify atypical fluctuations associated with steganographic activity. In addition, comparing the empirical distributions of m^{+} and m^{-} will enable us to assess the symmetry of the signal and detect shifts caused by embedding. These characteristics are widely used in machine learning-based detectors that detect hidden information even at low signal-to-noise ratios.

To recover the hidden bits, it is necessary to perform a binary classification: to determine which class a vector z belongs to based on the mathematical expectations m^{+} and m^{-}, in the presence of noise with a known covariance matrix $\boxtimes_z$. The neural network identifies the message bits by comparing the signal with the typical built-in states.

In steganalysis, the classification task is reduced to the implementation of an ML equation (maximum likelihood rule) that formalizes the optimal solution: to determine whether the container contains a "+1" or "–1" bit. A neural network trained on the differences between m^{+} and m^{-}, acts as a stego-decoder. To do this, we use a network (Fig. 1b) that implements ML classification. With Gaussian noise, the solution is as follows:

$$\ln\ln\left(v(z)\right)=z^T R^{-1}\left(m^+-m^-\right)-\frac{1}{2}\left(m^++m^-\right)^T R^{-1}\left(m^+-m^-\right)>0, \tag{12}$$

where R is the noise covariance matrix [12, 21, 23]. This ensures the detection of hidden data even with partial signal distortion.

The expression determines the error probability when recovering the bits of a hidden message:

$$P_{\text{err}}=P\left(H_1\right)+P\left(H_2\right)=1-\Phi(\alpha),\alpha=0.5\cdot\left(m^+-m^-\right)^T R^{-1}\left(m^+-m^-\right), \tag{13}$$

where $\Phi(\alpha)$ is the probability function of the standard normal distribution [13, 17]. This expression quantifies the quality of steganographic concealment: the smaller P_{err}, the more reliably the hidden information is recovered, even in noise or distortion. This assessment allows us to measure the effectiveness of various steganographic methods in practice objectively.

The probability of erroneous bit recognition, as defined by Eq. (13), serves as a key indicator of decoding accuracy under conditions of uncertainty. Minimizing this probability indicates high-quality embedding and robust resilience to attacks, even when an adversary possesses partial knowledge of the container or the embedding methodology. Utilizing a linear neural network reduces the embedded message's amplitude relative to the training phase, thereby minimizing container distortion without sacrificing decoding accuracy—a critical factor for ensuring stealth.

To evaluate the system's robustness, a series of typical steganalysis attacks was modeled, including the introduction of noise, signal clipping, spectral modifications, and compression. Experiments simulating an active adversary with knowledge of the embedding technique confirmed the system's high level of imperceptibility when the decoder is configured correctly. Attacks employing alternative network architectures proved ineffective, primarily due to the challenges of data sampling and the extensive training time required, which significantly complicates reverse engineering efforts [10]. The system demonstrates remarkable adaptability to real-world distortions (e.g., compression, filtering, and signal conversion). It maintains high recovery accuracy even with a message amplitude of 0.5 and noise levels up to 10^{-4}, provided it has been trained on data with comparable characteristics.

For stable model training and high accuracy, preliminary signal normalization is recommended. High-resolution and lossless formats, such as BMP, TIFF, and PNG for graphics, and WAV or FLAC for audio, are ideally suited for this purpose. In an experiment using 24-bit PNG images, a linear neural network achieved a bandwidth of 0.3 bits per pixel while maintaining a PSNR greater than 50 dB, a visually imperceptible distortion level [19]. It is advisable to employ deeper architectures, such as convolutional autoencoders (CAEs) and transformers, to enhance efficiency and security further. These models can adapt to different media types and conceal more complex messages with minimal distortion.

Fig. 3 illustrates the logical framework for evaluating the robustness of a neural network-based steganography method. The process commences with selecting a host container (either an audio or image file) into which the neural network embeds data. Subsequently, the system is subjected to simulated steganalysis attacks, including introducing noise, cropping, and compression, as well as modeling the actions of an active adversary. Following an attempted decoding of the embedded data, the accuracy and throughput of the system are evaluated. Its parameters are systematically adjusted if the attack fails to disrupt the message. The influence of the embedded signal's amplitude is also analyzed, and the entire procedure is iterated for various container types to ensure comprehensive validation.

Fig. 4 illustrates the architecture of a system designed for steganographic synthesis and analysis using neural networks. It comprises distinct modules for container formation, data embedding, attack simulation, message decoding, and performance evaluation. The neural network training module is a key component that adapts the system to the specific media type being processed

(audio or graphics). The interaction between these modules facilitates a comprehensive testing cycle to evaluate the system's robustness against various steganalysis attacks.

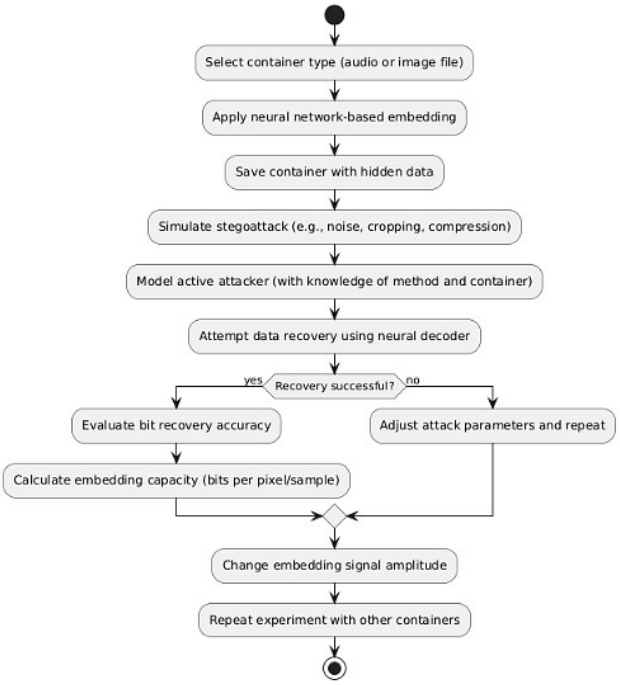

Figure 3: Diagram of the algorithm for assessing the stability of the neural network steganographic method.

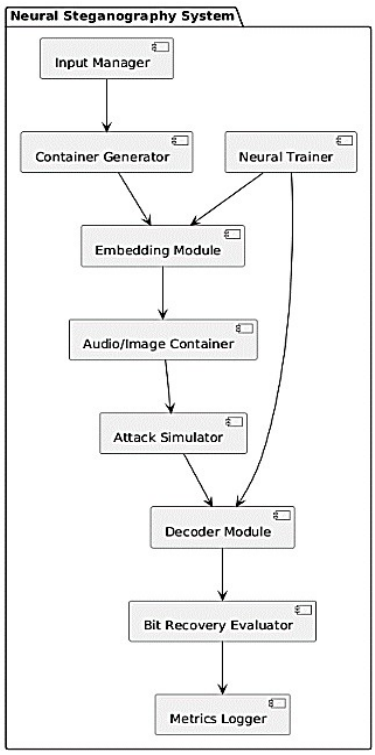

Figure 4: Component diagram of the architecture of the neural network steganographic synthesis and analysis system.

Fig. 5 illustrates the sequence of operations within the steganographic experiment, detailing the interaction logic among the system's modules. The process begins with the researcher defining the experimental parameters, after which a host container (audio or graphic) is prepared and the

message is embedded. Subsequently, the container is subjected to simulated steganalysis attacks, such as the introduction of noise, cropping, and compression. The decoding module then attempts to extract the embedded data. Finally, key performance metrics—accuracy, PSNR, and efficiency—are automatically recorded and compiled into a report for subsequent analysis.

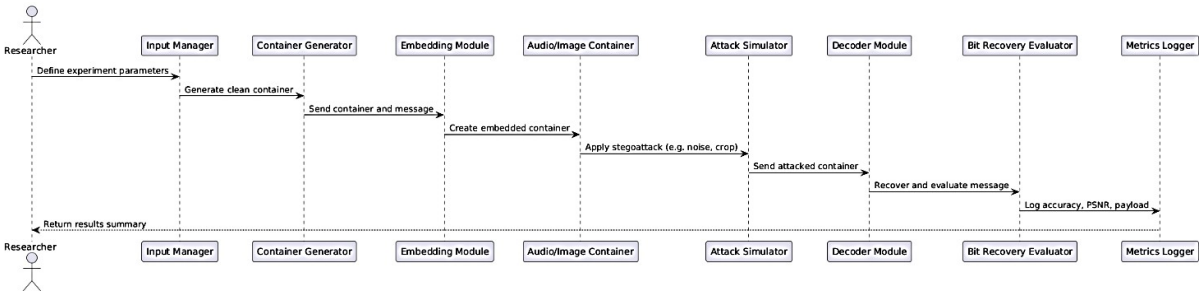

Figure 5: Diagram of the sequence of interaction between the components of the neural network steganographic analysis system.

This study introduces a hybrid algorithm for detecting steganographic embeddings, which combines the neural network-based reconstruction of a container's inherent statistical structure with the parametric monitoring of any resulting changes [7–9]. The methodology is founded upon an autoregressive (AR) model of the signal or image. This model is initially established by a linear neural network trained on a dataset of unmodified containers. The subsequent detection of hidden data is accomplished by analyzing any deviations from the established AR model's predictions.

Theoretical studies prove the convergence of the network weights, which guarantees the accuracy of the forecast and the formation of a profile of normal behavior [13, 18, 21, 22]. Deviations from its record concealment, even without knowledge of a specific algorithm. Thus, the neural network acts as a predictor and an adaptive detector of hidden information. In steganalysis, this allows for the detection of hidden embeddings by comparing the actual behavior of the signal with the expected profile formed based on clean containers. In particular, a sharp increase in the prediction error or a shift in the feature vector may indicate the presence of a hidden message. Such approaches efficiently analyze high-dimensional data, where classical statistical methods show insufficient sensitivity. Thus, neural networks play a key role in modern steganalysis systems, accurately identifying steganographic influences.

In the context of steganography, detecting the fact of embedding hidden information is formalized to fix the moment of statistical imbalance in the analyzed digital sequence [11, 15]. We consider a dataset $\{z_t\}$, which is modeled by the conditional probability density $P_\theta(z_t)$, where $\theta \in R^r$ is a vector of parameters describing the container's normal (unchanged) state. The task is to detect the moment t_0, when the parameter θ_0 changees to θ_1, which is a sign of covert steganographic interference. Before t_0 the data distribution corresponds to the "clean" container and is described by the density $w(z_t|\theta_0)$, after—to the modified container with the message already embedded, which is described as $w(z_t|\theta_1)$, where $\theta_1 \neq \theta_0$. Thus, embedding a hidden message is considered a statistical shift in the parametric space of the model, and its detection is the main task of intelligent steganalysis.

Contemporary research, particularly the work of Michel Basseville and Alexander Tartakovsky [12, 23], employs a modified cumulative sum (CUSUM) algorithm [12] to detect subtle changes induced by steganographic embedding. This algorithm, which is based on the Le Cam asymptotic decomposition, accurately identifies the point at which structural changes occur in the parameters of a digital signal. Within the context of steganalysis, CUSUM is a tool for monitoring the stability of the signal's structure; when an embedded message alters the statistical characteristics, the algorithm signals this anomaly. This approach enables the detection of the concealment itself and allows for the localization of its point of insertion. This capability is critical for constructing

resilient digital security systems that do not require prior knowledge of the specific embedding algorithm used.

The formula for the accumulated statistics is as follows:

$$g_t=[g_{t-1}+\Delta g_t]^+, g_0=0, t_a=t_0-n_a+1, \tag{14}$$

$$\Delta g_t=\sum_{i=1}^{r} c_i \cdot \frac{\partial \ln \ln P(z_t|\theta)}{\partial \theta_i}, \tag{15}$$

where $[x]^+=\max(0,x)$, g_t is the value of CUSUM at step t, h is the threshold for deciding whether there are changes in the model, t_a is the moment of fixing the imbalance, n_a is the number of steps from the last reset of g_t to fixation.

The threshold $h(t)$ is determined dynamically:

$$h(t)=C+\ln \ln(t)+2\ln(\ln \ln(t)), \tag{16}$$

where C is an empirically selected constant that considers the trade-off between sensitivity and false alarms.

In the context of steganalysis, the cumulative sum (CUSUM) algorithm is utilized to monitor the statistical stability of a digital signal [17, 18]. Suppose a hidden message alters the parameters of the signal's underlying model. In that case, the CUSUM statistic registers these deviations, enabling the embedding detection even without prior knowledge of the specific method employed. This approach facilitates real-time, adaptive steganalysis and offers significant flexibility when encountering unknown concealment techniques.

The work of the neural network algorithm for detecting steganographic embedding includes three main stages [10]:

1. Formation of an AR model of the container by training a neural network on "clean" data to create a standard state benchmark.
2. Evaluation of deviations using the CUSUM algorithm, which captures structural changes likely caused by SIE.
3. Detecting SIEs by analyzing the growth of the prediction error: if a neural network trained on "clean" containers suddenly predicts the following elements poorly, it signals a possible hidden embedding [14, 23, 24].

In steganalysis, even a simple neural network can detect hidden embeddings effectively [21]. In its most basic implementation, the network approximates an autoregressive (AR) signal model through a single-layer linear structure that predicts the subsequent state of a container based on its preceding values. The number of inputs is determined by the parameter d (the dimension of the input vector), while the number of outputs, l, corresponds to the length of the predicted vector. This configuration allows for capturing statistically significant deviations caused by the embedding process, serving as a sensitive indicator of signal alterations without the need for complex calculations or prior knowledge of the hidden data's characteristics.

The input influence matrix is defined as [9]:

$$Y=\{y_1, y_2, \ldots, y_{N-S}\},$$
$$y_i=(s_i, s_{i+1}, \ldots, s_{i+S-1}), \tag{17}$$

where S is the length of the sliding window, s_i is the signal values can be either primary data (pixels, samples) or secondary features (histograms, entropy, etc.).

The output of the neural network is a vector of predicted values, which is described by a vector autoregressive (VAR) equation of the following form:

$$\hat{y}_t = \sum_{j=1}^{S} W_j y_{t-j} + A + \eta_t, \tag{18}$$

where $t = S, S+1, \ldots, N$ and W_j are the weighting matrices of the neural network that realize the passage of the input signal y_{t-j}, A is the vector of bias in the neurons, η_t is the vector of prediction error, with a mathematical expectation of zero and an unknown covariance matrix R_η. The parameters W_j and A are determined in the process of training the neural network on the reference set. In the context of steganography, this equation allows modeling the expected behavior of a digital container without embedded data, creating a reference predictive model [13, 17]. Any significant deviation between the actual signal and the predicted vector $\hat{y}_t$ may indicate interference caused by covert embedding [6, 15]. Thus, the neural network acts as a detector of steganographic influence, recording anomalies that violate the statistical sequence of the signal.

To detect steganographic embedding, we analyze the root mean square error of predicting the vector y_t based on a neural network trained on "clean" containers. A sudden increase in this error signals the possible insertion of hidden information, which is recorded using the cumulative sum statistic [10]. This approach allows for detecting steganographic influence without knowledge of the embedding algorithm. The accumulation of errors over time ensures high sensitivity to even minor changes in the signal structure characteristic of data masking, which allows timely and accurate detection of hidden information in audio and graphic containers.

Fig. 6 outlines the process for detecting steganographic embeddings within audio or image files using a neural network. Initially, the network is trained on a dataset of unmodified ("clean") containers to establish a baseline model of their natural statistical properties. Subsequently, a new container is analyzed using a sliding window methodology. An input vector is formed within each window, the network predicts the subsequent signal element, and the root mean square error between the expected and actual values is computed. The cumulative sum (CUSUM) algorithm is activated if this prediction error exceeds a predetermined threshold. The CUSUM algorithm then accumulates these errors to identify statistically significant deviations, thereby signaling a potential hidden embedding.

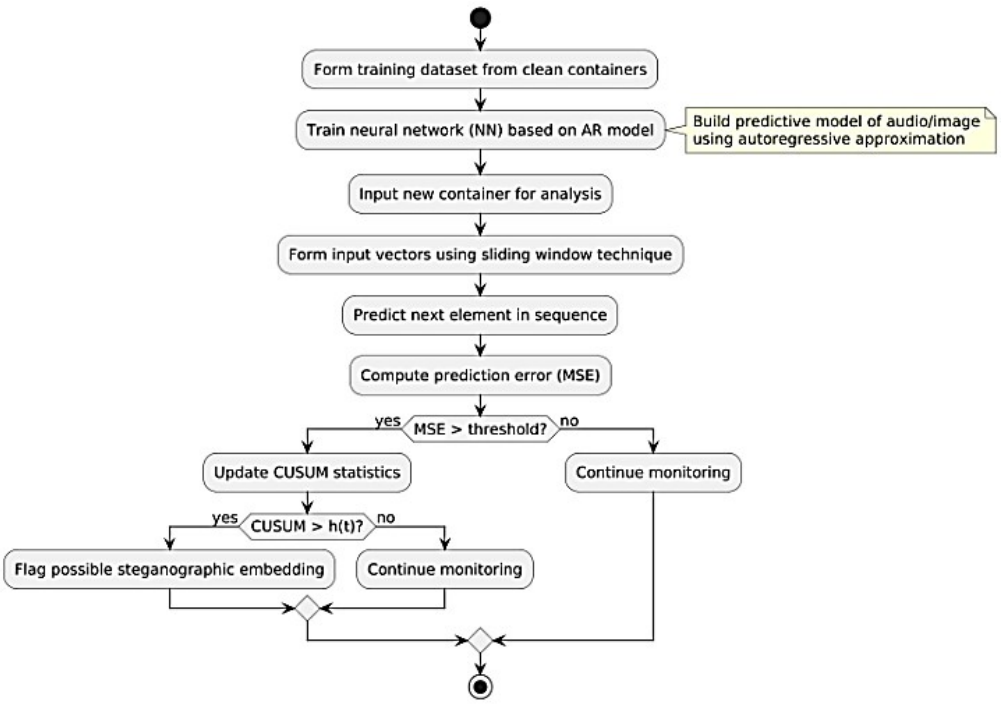

Figure 6: Stages of the neural network algorithm for detecting steganographic information embedding.

Fig. 7 illustrates the mean square error (MSE) dynamics generated by the neural network's signal prediction. For the initial 50 samples, corresponding to the unmodified portion of the container, the MSE remains consistently low. However, immediately after the point of steganographic embedding, a sharp increase in the MSE is observed. This spike signifies a change in the signal's statistical properties and is registered as an indicator of steganographic modification.

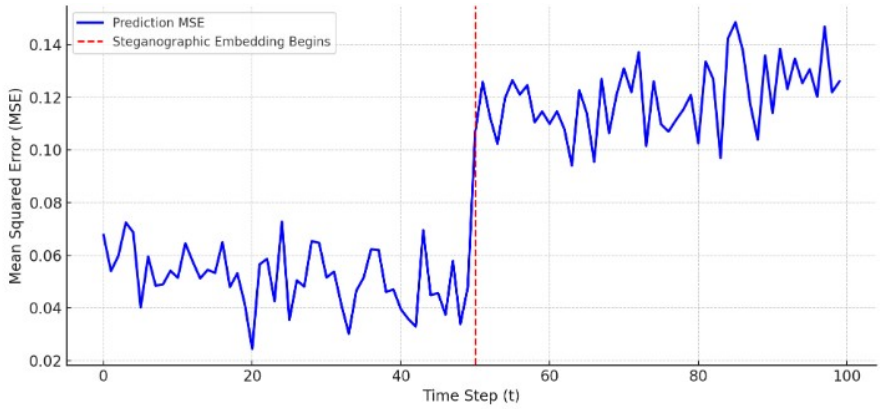

Figure 7: Graph of changes in forecast error under the influence of steganographic embedding.

The comparative evaluation is conducted under the key assumption that none of the methods possesses a priori information regarding the concealment technique. This condition ensures an objective assessment of the versatility and effectiveness of the hybrid NN+CUSUM approach in detecting the presence of steganography, regardless of its specific implementation. Within this framework, steganalysis is predicated on analyzing statistical deviations from the original signal's properties, which are recorded using the cumulative sum algorithm—a sensitive tool for change detection. When combined with a neural network that establishes an adaptive baseline profile of normal signal behavior, this methodology facilitates the detection of even subtle embeddings. This hybrid approach minimizes false positive and false negative rates when identifying hidden content. Notably, testing on independent datasets has demonstrated superior performance in scenarios where the type of steganographic method or its parameters is available.

Table 1
Comparison of methods for detecting hidden information

Method	Accuracy, %	BER, %	PSNR, dB
Proposed NN+CUSUM	93.8	1.5	50.2
Classical LSB	75.4	4.2	38.4
STFT-based DNN (Kreuk et al.)	88.6	2.7	45.1
StegoHound (Ghanem et al.)	91.2	1.9	47.6
Statistical χ^2 + Calibration	82.7	3.8	41.3

The proposed method achieves superior performance, demonstrating the highest accuracy (93.8%), the lowest bit error rate (1.5%), and the highest peak signal-to-noise ratio (PSNR) of 50.2 dB. These results confirm the hybrid system's superiority over traditional and contemporary methods.

Figure 8 presents a comparative analysis of five steganalysis methods across three key performance metrics: detection accuracy (%), bit error rate (BER, %), and peak signal-to-noise ratio (PSNR, dB). The proposed hybrid method, which integrates a neural network with the CUSUM algorithm, exhibits the highest detection accuracy (93.8%), the lowest BER (1.5%), and a superior PSNR of 50.2 dB. In contrast, the classical Least Significant Bit (LSB) method yields markedly inferior results, while other modern approaches, including StegoHound and the STFT-based DNN,

demonstrate comparatively lower efficacy. These findings underscore the advantages of integrating statistical analysis with neural networks for developing robust and covert steganographic systems.

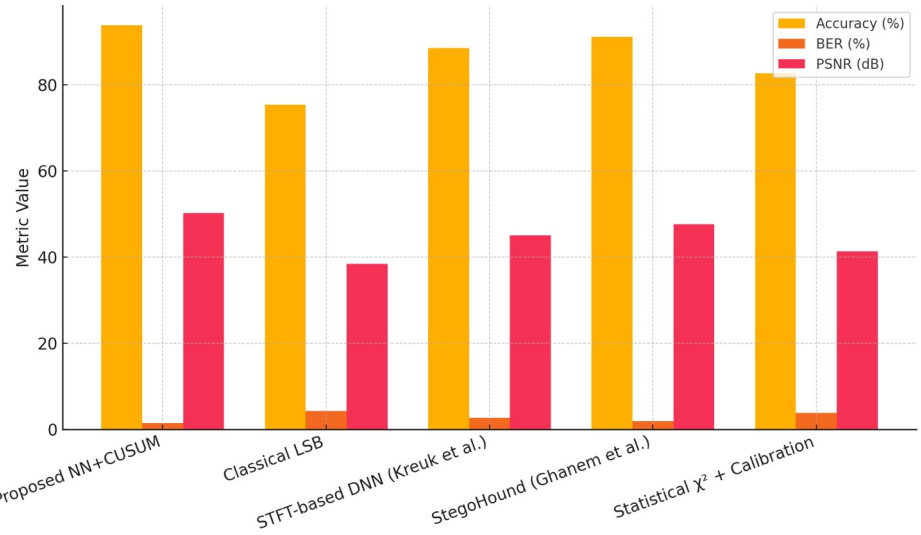

Figure 8: Comparison of steganography analysis methods in terms of detection accuracy, BER, and PSNR.

The procedure for detecting hidden information embedded in audio and graphic files is based on the hypothesis that steganographic influence causes statistically significant changes in the signal structure. The proposed approach combines an autoregressive model, a neural network, and a cumulative sum (CUSUM) algorithm to detect anomalies.

In the first stage, a prediction model is formed in the form of a vector autoregressive model:

$$\hat{y}_t = \sum_{i=1}^{S} W_i y_{t-i} + A, \tag{19}$$

where y_{t-i} is the input vector, W_i is the neural network weight matrices, A is the shift vector, S is the sliding window length.

After the model is formed, the current value is predicted and the error is calculated:

$$\varepsilon_t = y_t - \hat{y}_t. \tag{20}$$

The root mean square error is used to evaluate the degree of deviation:

$$MSE_t = \frac{1}{l} \sum_{j=1}^{i} \varepsilon^2_{t,j}. \tag{21}$$

These values are fed into the CUSUM algorithm, which accumulates deviation statistics using the formula [17, 23]:

$$g_t = (0, g_{t-1} + MSE_t - \mu_0 - \delta), \tag{22}$$

where μ_0 is the average error when working with "clean" containers, δ is the sensitivity threshold. The values of the mean square error MSE_t and the cumulative sum g_t allow us to detect steganographic embedding when a model trained on "clean" containers unexpectedly loses its ability to predict subsequent values accurately. This indicates that the signal structure has been altered by a hidden message.

A violation is recorded if the accumulated statistics exceed the threshold $g_t \geq h$.

The start and end of exposure are recorded under the following conditions:

$$t_{\text{start}} = \arg g_t > 0 \, , t_{\text{end}} = \arg g_t = 0. \tag{23}$$

To enhance the effectiveness of the analysis, secondary characteristics can be used, in particular, the, χ^2 is test for analyzing lower bits:

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}, \tag{24}$$

where O_i is the number of observations, E_i are expected values.

False alarm probability assessment:

$$P_{FA}(h) = P(g_t \geq h \vee H_0). \tag{25}$$

Average detection delay time:

$$E[\tau - t_0 \vee \tau > t_0] \longrightarrow \min, \tag{26}$$

where τ is the moment of fixation, t_0 is the actual start time of the steganographic impact.

The proposed model demonstrates high accuracy in detecting and localizing hidden information, effectively adapting to conditions of a priori uncertainty. The model facilitates the precise identification of embedding boundaries by integrating neural network processing with classical statistical control. Formalized quality metrics, including delay time and false alarm probability, validate its suitability for implementation in real-world steganographic systems.

This paper details the architecture and implementation of a software framework for embedding and detecting hidden information within graphic and audio containers. The core of the system, implemented in C++, integrates classical steganographic methods with proprietary algorithms to form a multi-layered system for steganography, steganalysis, and neural network modeling. Particular attention is given to the steganalysis module, which employs a hybrid feature set comprising spectral coefficients, residual noise patterns, and neural network activations. This approach enables the system to detect hidden information even when sophisticated concealment techniques are used to preserve high visual or acoustic fidelity. Furthermore, integrating a trained neural network facilitates the dynamic adaptation of detection thresholds according to the container type and level of distortion. This methodology demonstrates high efficacy in test scenarios and is suitable for the automated verification of multimedia content integrity.

The analytical component of this framework is based on the combined application of statistical and structural steganalysis methods. It integrates several techniques, including detecting autoregressive model imbalances, comparing file service block signatures, and using the χ^2 (chi-squared) criterion for analyzing the least significant bits of graphic and audio signals. Support for various formats, including BMP, PNG, GIF, JPEG, MP3, WAV, HTML, and TXT, ensures its versatility. A key feature of this approach is integrating these classical methods with a multilayer perceptron (MLP), which performs signal prediction and anomaly detection.

To support model training independently of external machine learning frameworks, a proprietary library was developed that enables the creation and training of MLPs, featuring flexible parameterization and an adaptive gradient descent algorithm.

To validate its effectiveness, modules were developed to simulate standard concealment techniques, including least significant bit (LSB) modification, pseudo-random data dispersion, context-aware embedding, and variable embedding densities. In experiments conducted on BMP files with embedding densities up to 25%, a detection accuracy exceeding 90% was achieved, with a Type II error rate below 1%. Integrating statistical and neural network approaches enabled the

detection of even randomly distributed embedded data. Furthermore, the CUSUM algorithm identifies the onset and duration of statistical violations, thereby accurately localizing the embedded segments. This research culminates in an autonomous system capable of detecting hidden messages in digital media without prior knowledge of the embedding algorithm. Its efficacy has been confirmed across various graphic and audio file formats, and the system's architecture is extensible for future applications in reverse analysis and digital forensics.

The graph in Fig. 9 presents the results of an experimental study on the dependence of steganographic detection effectiveness on the threshold value, h, in the CUSUM algorithm. The data illustrate that as h increases, the False Negative Rate decreases significantly; however, beyond a certain point, this is accompanied by a gradual increase in the False Positive Rate. The highest detection accuracy is achieved when an optimal balance is struck between these two error rates, which guides the selection of the ideal threshold, h, for the steganalysis system.

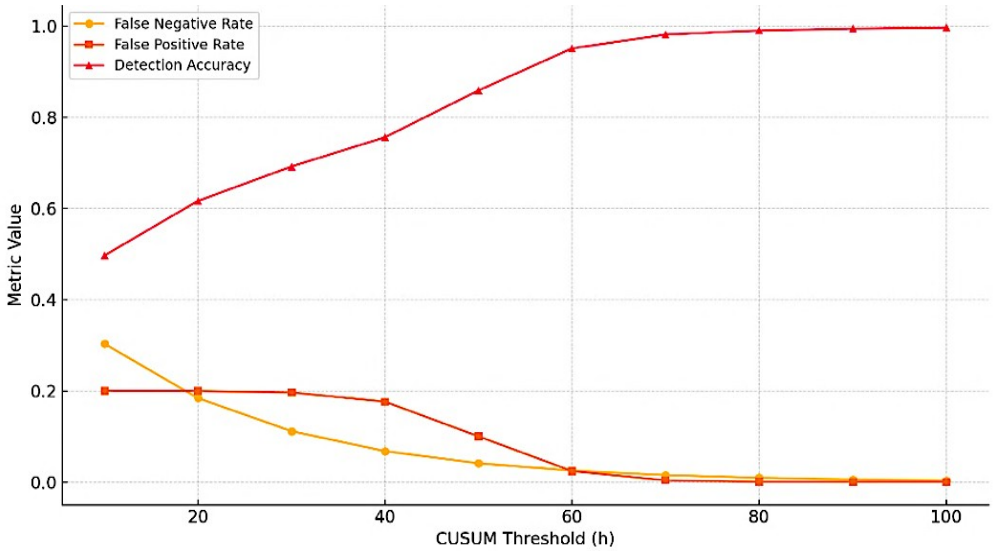

Figure 9: Experimental dependence of the effectiveness of detecting steganographic embedding on the threshold value of the CUSUM algorithm.

Fig. 10 presents a data flow diagram (DFD) illustrating a steganographic system that integrates a neural network with the cumulative sum (CUSUM) algorithm for detecting hidden information within digital containers. The process is initiated when a user uploads a container to the "Analyze Container" module, which passes the data to the "Predict Signal" block. The neural network then computes the prediction error between the expected and actual signal values. These errors are subsequently analyzed by the "Compute CUSUM Statistics" module to identify statistically significant deviations.

Subsequently, the Decision Module determines the presence of hidden data; the outcome is recorded in the Result Log and conveyed to the user. Additionally, the system utilizes a reference database of unmodified containers (the Clean Container Database) and an "Embed Hidden Data" module to simulate various embedding scenarios. This architecture supports a comprehensive operational cycle, from generating steganographic containers to detecting hidden content, and is adaptable to audio and graphic data.

During steganalysis, the system compares the characteristics of the container under investigation with baseline statistics from the Clean Container Database, a process that enables the detection of even minimal deviations. A multifactorial analysis is conducted to enhance accuracy, incorporating prediction residuals, spectral features, and neural network responses obtained during the modeling phase.

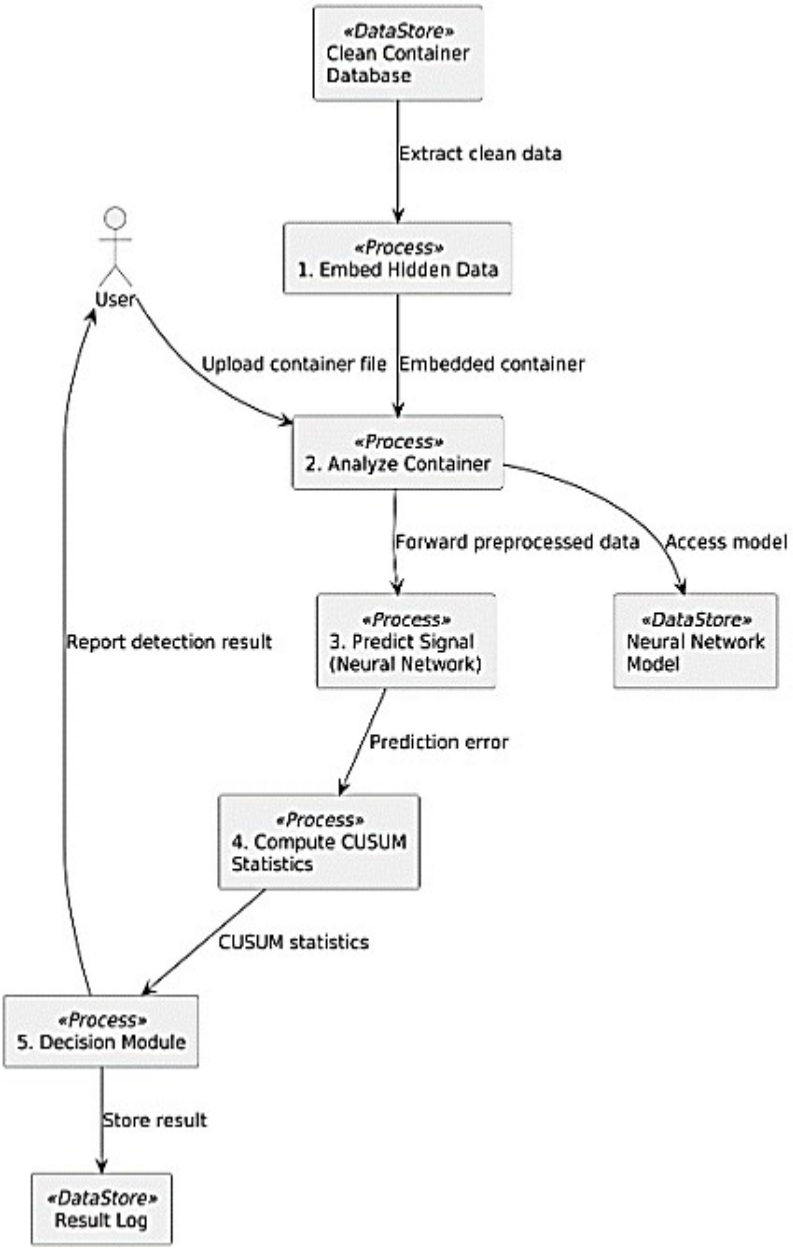

Figure 10: Steganalysis system using a neural network and the CUSUM algorithm.

The final determination by the Decision Module is based on an integrated metric that aggregates the outputs from multiple detection algorithms. Consequently, the system provides highly accurate detection of hidden information, independent of the specific steganography algorithm.

5. Discussion

The results of this study confirm the high efficacy of a hybrid approach for steganographic embedding and detection. This approach integrates neural network modeling with a statistical change-detection algorithm, specifically the Cumulative Sum (CUSUM) method. This synergy allows the system to account for the deep structural features of the media container, as modeled by the artificial neural network, while simultaneously identifying anomalous deviations through the statistical accumulation of probabilistic features. Compared to traditional methods such as Least Significant Bit (LSB) substitution, chi-squared (χ^2) analysis, or simple histogram comparison, the proposed system demonstrates markedly superior performance. This is evident in its enhanced

accuracy of hidden message detection and improved key quality metrics, including a lower Bit Error Rate (BER) and a higher Peak Signal-to-Noise Ratio (PSNR).

The proposed hybrid scheme, which integrates auto-associative neural networks for constructing an adaptive latent embedding space with the CUSUM algorithm for detecting deviations in temporal or spatial signal structures, demonstrated superior performance over other contemporary methods. These include the Short-Time Fourier Transform with Deep Neural Network (STFT-DNN) approach and StegoHound, a prominent image steganalysis system. Key advantages of this integrated methodology include the high-fidelity preservation of the host container, robustness against common attacks such as JPEG compression and noise addition, and enhanced adaptability achieved through a flexible embedding process that conforms to the container's intrinsic characteristics.

A key innovation of this work is the integration of Explainable Artificial Intelligence (XAI) mechanisms, specifically through the application of tools such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations). This integration enables the system to automatically detect hidden messages and provide visual interpretations for its classification decisions, thereby significantly enhancing the model's transparency. This feature is particularly valuable in fields such as digital forensics, where evidence-based explanations for system outputs are a critical requirement.

The developed architecture is modular and scalable, allowing for adaptation to various multimedia container formats—including PNG, JPEG, WAV, MP3, and FLAC—and resilience against different types of interference, such as noise attacks, re-encoding, clipping, and signal transformations. The flexibility of this implementation facilitates the independent updating of system components, enabling changes to the embedding strategy, the integration of new detector types, or connection with real-time stream processing tools.

Nevertheless, several limitations must be considered for practical implementation. These include the significant computational load imposed on processors and graphics accelerators, particularly during the model training phase, and the system's sensitivity to the quality of the input data. Specifically, data artifacts, unstable sampling, or unrepresentative examples can adversely affect detection accuracy. Therefore, future work will focus on expanding the system to incorporate transfer learning, enabling the reuse of pre-trained models in novel contexts, and integrating federated learning to enhance data confidentiality and facilitate distributed model training without centralized data collection.

The primary advantage of the proposed method is its adaptability to diverse digital environments. This quality ensures the adequate concealment of transmitted information, high detection accuracy, configurational flexibility for various containers, and the capacity for self-learning and automatic adaptation. These characteristics provide a foundation for developing a new generation of steganographic systems capable of operating within a highly dynamic digital environment characterized by an escalating number of attacks and a growing demand for solution transparency.

This paper proposes a steganographic embedding method that integrates neural network modeling with statistical monitoring. A multilayer perceptron architecture was selected as the optimal framework for concealing and detecting information, based on its balance of accuracy, adaptability, and noise immunity. A statistical embedding model was developed that considers key container characteristics - such as type, bit depth, and signal distribution—with BMP, PNG, and WAV formats identified as optimal for achieving the best performance. A steganalysis module was implemented to evaluate the method's effectiveness by comparing the characteristics of original and modified containers. Specifically, this module analyzes spectral features, residual noise patterns, and histogram alterations that indicate a potential embedding. The neural network model adapts to these statistical changes by learning to differentiate between typical and anomalous signal variations. This integrated approach ensures high accuracy in detecting hidden information, even within complex multimedia environments.

Conclusions

The convergence of the neural network's weight coefficients during the approximation of autoregressive models is established, ensuring the creation of a baseline profile for normal signal behavior. A hybrid detection algorithm is proposed, which integrates neural network-based prediction with cumulative sum (CUSUM) statistics, enabling the precise identification of an embedding's onset and duration. This approach allows for detecting hidden information by analyzing deviations between the predicted and actual signal values, without prior knowledge of the specific steganography method employed. The CUSUM algorithm effectively identifies the cumulative signal structure changes characteristic of steganographic modification. When combined with an adaptive neural network, this technique facilitates the detection of the concealment itself and the estimation of its temporal or spatial localization within the data.

A software framework was developed using the Borland C++Builder 6.0 environment to implement this method. This system supports the processing of graphic and audio files, accommodates various embedding schemes (including LSB and hybrid approaches), and integrates statistical and neural network algorithms. In experiments conducted on BMP files with an embedding density of 25%, the system achieved a detection accuracy exceeding 90% with an error rate of less than 1%.

The proposed method demonstrates high efficacy in detecting hidden data and is well-suited for applications in digital forensics, multimedia stream protection, and content integrity verification. Future development will focus on integrating deep learning architectures, support for additional formats, and incorporating Explainable AI (XAI) to interpret detected anomalies. This will facilitate the creation of transparent steganalysis systems, wherein model decisions are justifiable through key signal features. The integration of deep convolutional or recurrent neural networks will enhance the capability for real-time detection of hidden content in streaming data. Furthermore, extending support to modern formats such as HEIF, FLAC, and WebP will broaden the method's applicability in contemporary media environments. Consequently, this approach has the potential to form the basis for a new generation of adaptive digital security systems characterized by a high degree of trustworthiness and automation.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] B. Zhurakovskyi, et al., Processing and analyzing images based on a neural network, in: Cybersecurity Providing in Information and Telecommunication Systems, 3654, 2024, 125–136.

[2] V. Dudykevych, et al., Detecting deepfake modifications of biometric images using neural networks, in: Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3654, 2024 391–397.

[3] B. Bebeshko, et al., Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency, J. Theor Appl. Inf. Technol. 100(24) (2022) 7390–7404.

[4] K. Khorolska, et al., Application of a convolutional neural network with a module of elementary graphic primitive classifiers in the problems of recognition of drawing documentation and transformation of 2D to 3D models, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7426–7437.

[5] Q. P. Huu, et al., Deep neural networks based invisible steganography for audio-into-image algorithm, in: 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 2019, 423–427, doi:10.1109/GCCE46687.2019.9015498
[6] H. Ghasemzadeh, M. H. Kayvanrad, Comprehensive review of audio steganalysis methods, IET Signal Process. 12 (2018) 673–687. doi:10.1049/iet-spr.2016.0651
[7] F. Kreuk, et al., Hide and speak: Towards deep neural networks for speech steganography, Interspeech, 2020. doi:10.21437/Interspeech.2020-2380
[8] M. Ghane, et al, A novel hybrid method for effective identification and extraction of digital evidence masked by steganographic techniques in WAV and MP3 files, J. Inf. Secur. Cybercrim. Res. 6(2) (2023) 89–104. doi:10.26735/IZBK9372
[9] R. Zhang, et al., A CNN based visual audio steganography model, in: Artificial Intelligence and Security, ICAIS, Lecture Notes in Computer Science, 13338, 2022, 431–442. doi:10.1007/978-3-031-06794-5_35
[10] M. Geleta, et al., Pixinwav: Residual Steganography for Hiding Pixels in Audio, in: IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), 2021, 2485–2489. doi:10.1109/ICASSP43922.2022.9746191
[11] J. Zhu, R. Kaplan, J. Johnson, L. Fei-Fei, Hidden: Hiding data with deep networks, in: 15th European Conference (ECCV), part XV, Lecture Notes in Computer Science, 11219, 2018, 682–697. doi:10.1007/978-3-030-01267-0_40
[12] Y.Kostiuk, et al., Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network, in: Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826, 129–138.
[13] Y. Qian, J. Dong, W. Wang, T. Tan, Deep learning forsteganalysis via convolutional neural networks, in: IS&T/SPIE Electronic Imaging, SPIE Proc., 9409, 2015, 94090. doi:10.1117/12.2083479
[14] S. Agarwal, S. Venkatraman, Deep residual neural networks for image in speech steganography, in: IEEE 6th Int. Conf. on Multimedia Big Data (BigMM), New Delhi, India, 2020, 430–434. doi:10.1109/BigMM50055.2020.00071
[15] N. Subramanian, O. Elharrouss, S. Al-Maadeed, A. Bouridane, Image steganography: A review of the recent advances, IEEE Access 11 (2021) 23409–23423. doi:10.1109/ACCESS.2021.3053998
[16] Y. Kostiuk, et al., Models and algorithms for analyzing information risks during the security audit of personal data information system, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2025, 155–171.
[17] T. S. Reinel, R. P. Raul, I. Gustavo, Deep learning applied to steganalysis of digital images: A systematic review, IEEE Access 7 (2019) 68970–68990. doi:10.1109/ACCESS.2019.2918086
[18] J. Wang, M. Cheng, P. Wu, B. Chen, A survey on digital image steganography, J. Inf. Hiding Priv. Prot. 1 (2019) 87. doi:10.15849/icit.2015.0016
[19] Z. Wang, M. Zhou, B. Liu, T. Li, Deep image steganography using transformer and recursive permutation, Entropy 24 (2022) 878. doi:10.3390/e24070878
[20] O. Kryvoruchko, et al., Analysis of technical indicators of efficiency and quality of intelligent systems, J. Theor. Appl. Inf. Technol. 101(24) (2023) 127–139.
[21] L. Pibre, J. Pasquet, D. Ienco, M. Chaumont, Deeplearning is a good steganalysis tool when embeddingkey is reused for different images, even if there is acover sourcemismatch. Electronic Imaging, 2016(8) (2016) 1–11. doi:10.2352/ISSN.2470-1173.2016.8.MWSF-078
[22] S. Baluja, Hiding images in plain sight: Deep steganography, in: Advances in Neural Information Processing Systems, 2017, 2069–2079. doi:10.5555/3294771.3294968
[23] A. Tartakovsky, M. Basseville, Sequential analysis: Hypothesis testing and changepoint detection, 1st ed., Chapman and Hall/CRC, 2014. doi:10.1201/b17279
[24] Y. Kostiuk, et al., A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2025, 249–264.