

Development and Research of a Method for Detecting Steganographic Embedding of a Secret Message in a Digital Image

Alla Kobozieva^{1,†}, Kateryna Tryfonova^{1,†} and Oleksandr Laptiev^{2,†}

¹ Odesa National Maritime University, Mechnikova str. 34, Odesa, 65029, Ukraine

² Taras Shevchenko National University of Kyiv, Volodymyrska str. 60, Kyiv, 01033, Ukraine

Abstract

The paper presents the development and experimental evaluation of a novel steganalysis method for detecting hidden information in digital containers without requiring access to the original container. In this study, the term container refers to digital images, including both grayscale and color formats. The proposed approach is based on the statistical analysis of singular values obtained through singular value decomposition of image matrix blocks. The detection method involves analyzing the distribution of the largest singular values and applying the Kolmogorov-Smirnov test to identify deviations from uniformity, which may indicate the presence of steganographic embedding. Experimental results demonstrate the high accuracy of the method in detecting hidden messages embedded using principal component domain modification, particularly at medium and high payload levels. The proposed method ensures a high level of specificity and is characterized by high computational efficiency due to the optimization of the method, making it suitable for real-time applications and large-scale data processing. The findings contribute to enhancing information security and counteracting covert communication channels in cyberspace.

Keywords

information security, steganography, steganography analysis, digital images, singular value decomposition

1. Introduction


In the modern digital society, where information is among the most valuable assets, ensuring its protection has become a matter of strategic importance. The rapid growth of data volumes, the expansion of global networks, and the increasing number of cyber threats underscore the ongoing need to improve methods for guaranteeing the confidentiality, integrity, and availability of information. Among the most commonly used means of information protection are cryptographic methods, which convert plaintext data into an encrypted form that is unintelligible to unauthorized individuals. At the same time, steganography, the science of concealing the very fact of information transmission, is increasingly viewed as an alternative or complementary approach to ensuring information security [1, 2]. Although cryptography is a powerful tool for ensuring security, it has certain vulnerabilities, most notably, the fact that the presence of encrypted data itself may attract the attention of a potential adversary. In contrast, steganography enables the concealment of secret messages by embedding them into multimedia objects without leaving visible signs of modification, thereby making detection significantly more difficult. As a result, steganography is considered particularly valuable in scenarios where it is necessary to ensure not only the confidentiality but also the imperceptibility of information transmission. Owing to these advantages, steganography has gained widespread application across various fields. It is effectively employed in military operations,

ICST-2025: Information Control Systems & Technologies, September 24-26, 2025, Odesa, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ alla_kobozieva@ukr.net (A. Kobozieva); trifonova@op.edu.ua (K. Tryfonova); olaptiev@knu.ua (O. Laptiev)

 <https://orcid.org/0000-0001-7888-0499> (A. Kobozieva); <https://orcid.org/0009-0004-4468-1618> (K. Tryfonova);

<https://orcid.org/0000-0002-4194-402X> (O. Laptiev)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

copyright protection, secure corporate and diplomatic communications, as well as in digital watermarking and content authentication systems. However, the very properties that make steganography appealing for legitimate use have also led to its active exploitation in cybercriminal activities.

In 2002, international law enforcement agencies uncovered the activities of the cybercriminal group known as Shadowz Brotherhood, which was involved in the distribution of child sexual abuse materials. The perpetrators employed steganographic techniques to conceal illicit content within image files, particularly in the PNG format, which did not arouse suspicion at first glance. Specialized software tools were used to embed illegal data into visual objects, making detection significantly more difficult [3].

In 2010, the activities of a group of Russian agents, commonly referred to as sleeper spies, were uncovered in the United States, where they had been conducting long-term intelligence operations. According to official reports from the Federal Bureau of Investigation, these agents utilized steganography to transmit classified information to Moscow covertly. Specifically, secret messages were embedded into ordinary digital images in JPEG format and transmitted via the Internet. As a result of the Federal Bureau of Investigation's analysis, this method was identified, leading to the arrest of multiple individuals and the exposure of a large-scale espionage network [4].

In 2012, a case involving the use of steganography by the terrorist organization Al-Qaeda for covert transmission of classified information was documented. Specifically, German law enforcement authorities discovered a pornographic video file into which encrypted text documents had been embedded using specialized software. These documents contained instructions related to the planning of terrorist attacks, including methods for constructing improvised explosive devices, guidelines for evading surveillance, and general operational strategies. The steganographic embedding enabled the concealment of this content within the video file in a manner undetectable by standard analytical tools. This incident became one of the first publicly confirmed examples of steganography being used in the context of terrorism, highlighting its potential as a means of covert communication and a significant challenge for national security agencies [5].

In 2021, the use of steganography was documented in the context of cybercrime, particularly during Magecart-type attacks. Cybercriminals injected malicious JavaScript code into the websites of online retailers to harvest users' payment information. The stolen credit card data was concealed within JPEG files using steganographic techniques, allowing it to appear as ordinary images. These files were stored on the same servers as legitimate website content, which significantly hindered the detection of unauthorized activity by traditional cybersecurity tools [6].

In 2024, researchers documented a targeted cyberattack, provisionally named SteganoAmor, orchestrated by the hacker group TA558. This attack represents a sophisticated multivector threat that combines social engineering, exploitation of known software vulnerabilities, and steganography. As a result, over 320 organizations operating in the fields of tourism, education, healthcare, and related sectors were affected. The attack begins with the distribution of phishing emails containing document attachments. These documents exploit a software vulnerability to execute malicious code on the victim's device. Upon opening, a script is triggered that downloads a JPEG image, which serves as a carrier of embedded malicious code. This steganographic concealment allows the image to appear benign, thus evading suspicion from both the user and conventional security software. Once the image is retrieved and the hidden payload decoded, the malicious code is executed. A distinguishing feature of this attack is the use of steganography as the primary mechanism for concealing harmful components. Since the visual characteristics of the carrier images remain unchanged, traditional antivirus solutions are largely ineffective in detecting the threat [7].

2. Problem statement

The increasing misuse of steganographic techniques, particularly in recent years, is reflected in the growing number of cyberattacks in which hidden messages are embedded in digital content to transmit commands, exfiltrate confidential data, or distribute malicious software. This trend poses a

tangible threat to information security at both governmental and corporate levels. In this context, there is a growing relevance and scientific necessity for the development of advanced steganalysis methods capable of detecting signs of hidden information in the absence of access to the original cover image. Effective steganalytic tools should not only reveal the presence of covert data transmission but also facilitate the identification of the specific steganographic techniques employed.

The object of this study is the process of detecting hidden secret information embedded in digital graphical content. The subject of the study comprises the methods used for detecting hidden secret information within digital graphical content. The aim of this study is to improve the effectiveness of detecting hidden secret information embedded in digital graphical content in cases where the original cover image is unavailable. To achieve this objective, the research proposes the development of a steganalysis method based on statistical analysis in the principal component domain.

3. Literature review

The continuous advancement and growing complexity of digital steganography methods have led to increased development and a rising number of steganalytic approaches, resulting in a surge of scientific research focused on the detection and analysis of hidden information in digital media. To ensure the further advancement of steganographic analysis, it is essential to conduct an in-depth examination of the advantages, limitations, and specific features of existing methods. Such analysis enables a well-founded selection of directions for their improvement and adaptation to emerging challenges. In this context, an appropriate and effective approach is the application of classification to existing methods, which enables the systematization of knowledge, facilitates analytical comparison of different solutions, and contributes to the identification of patterns and trends in the field's development.

The classification of steganalytic methods is carried out based on selected criteria [8].

Depending on the amount of available information, steganalysis methods are classified as targeted or universal. Targeted methods utilize prior knowledge about the embedding technique, while not requiring access to the steganographic key. Universal methods are based on detecting distinguishing features between modified and unmodified digital content.

Depending on the objective of the attack, steganalysis methods can be classified as static, dynamic, and auxiliary. Static methods are aimed at detecting the presence of hidden content and identifying the steganographic method used. Dynamic methods involve analyzing the size and location of the hidden message, as well as the potential extraction of the concealed information. Auxiliary methods are intended to trigger the retransmission of the steganographic message in order to facilitate its subsequent analysis.

Based on the target of detection, steganalysis methods can be categorized as visual, signature-based, and statistical. Visual methods rely on the analysis of visual patterns perceived by the human visual system. Signature-based methods aim to detect anomalies, such as structural irregularities within a file. Statistical methods are based on comparing the statistical characteristics of modified and unmodified content to identify deviations indicative of steganographic embedding.

One of the earliest and most widely used statistical methods is the pairwise value analysis based on Pearson's chi-squared criterion [9]. This method examines pairs of values that differ only in their least significant bit. After the embedding of random bits, the frequencies of such pairs tend to equalize, while their total sum remains unchanged. The expected values are compared with the observed ones, and a significant deviation may indicate the presence of a hidden message. One of the main limitations of this method is its low effectiveness when the embedded message is short or has a non-uniform value distribution, as well as its applicability being restricted to uncompressed images.

Research on the embedding of secret messages using the least significant bit method led to the development of regular-singular analysis [10]. This method is based on analyzing regular and singular groups of pixels, which exhibit different responses to a specific bit-flipping operation. The authors of [10] proposed a technique for constructing a diagram that enables estimation of the length

of the hidden message, even when its location within the pixels is randomized. The primary drawback of the method is its high sensitivity to noise and its inefficiency when applied to compressed images.

The advancement of steganalytic research for compressed digital images has led to the development of numerous methods that exploit format-specific characteristics and are based on analyzing changes in the statistical distributions of frequency coefficients. In [11], the authors proposed a method grounded in the observation that image compression leaves a distinctive trace in the distribution of discrete cosine transform coefficients, and even minor alterations to pixel values disrupt this consistency.

One of the earliest methods to apply machine learning to steganalysis is the approach proposed by the authors in [12]. The method involves detecting hidden messages in images by analyzing higher-order statistical features extracted after a wavelet transform. The image is decomposed into subbands based on scale and orientation, and statistical characteristics are computed for each subband. The resulting feature vector is then fed into a support vector machine, which classifies the image as either containing or not containing hidden information.

The automation, development, and growing popularity of artificial neural networks have enabled their application in steganographic analysis. In [13], a method for blind steganalysis of digital images is presented, utilizing an artificial neural network trained on wavelet-based features and image quality metrics. The developed system classifies images as either containing or not containing hidden information, without prior knowledge of the embedding method. The designed neural network requires large volumes of training data and substantial computational resources.

A convolutional neural network architecture for steganalysis of digital images based on a joint normalization method was proposed in [14]. The authors demonstrate that traditional normalization degrades the generalization capabilities of the model when using paired training, which is typical in hidden message detection tasks. The proposed normalization approach employs a unified set of statistics across all training batches, ensuring more stable learning and improved accuracy during testing.

The effectiveness of detecting hidden secret information in digital images using a deep convolutional neural network was investigated in [15]. The study analyzed three network implementations based on well-known steganographic datasets. The results confirm the feasibility of applying the proposed network architecture in steganalysis. Optimization of the network architecture and its parameters plays a crucial role in the overall performance of steganalysis.

4. Materials and methods

The advancement of steganalysis methods for digital images is impossible without the parallel study of modern steganographic approaches, as the effectiveness of hidden information detection directly depends on a deep understanding of the principles underlying its embedding. The strategy for developing steganalysis should be grounded in accumulated knowledge in the field of steganography, aiming to create detection techniques that outpace contemporary hiding methods and remain effective even in the presence of new or modified steganographic techniques.

Despite demonstrating a certain level of effectiveness, neural network-based steganalysis methods cannot be regarded as a universal solution for steganographic analysis tasks. Their performance largely depends on the volume and quality of training datasets. Moreover, the inherently low interpretability of such models complicates their application in critical information security systems. An additional limitation is their high computational complexity, which restricts their efficiency in resource-constrained environments. Therefore, to ensure reliable steganographic analysis, it is advisable to investigate modifications of steganographic methods across different domains, as well as to analyze their interrelationships. An effective approach in this context involves the development of hybrid models that integrate modern artificial intelligence techniques with classical statistical and heuristic methods.

Many steganographic methods employ the principal component domain for embedding secret information, as it enables an optimal balance between imperceptibility, robustness to distortions, and controllability of the embedding process. Owing to these properties, the principal component domain is considered a promising domain for covert data embedding in digital images.

Singular value decomposition is commonly used to transform data into the principal component domain, as it enables the efficient extraction of an orthogonal basis representing the main directions of data variation.

Let $F=(f_{y,x})$ be an $R \times C$ matrix of a digital image [16], whose elements $f_{y,x}$, $y=1,R$, $x=1,C$. The singular value decomposition of the matrix F is given by [17,18]:

$$F = U \Sigma V^T, \quad (1)$$

where U – is a matrix of dimensions $R \times R$, that satisfies the relation $U^T U = I$, it is an orthogonal matrix;

V – is a matrix of dimensions $C \times C$, that satisfies the relation $V^T V = I$, it is an orthogonal matrix;

Σ – is a diagonal matrix with elements $\sigma_1, \dots, \sigma_{C-1}, \sigma_C$, such that $0 \leq \sigma_C \leq \sigma_{C-1} \leq \dots \leq \sigma_1$.

The columns u_1, \dots, u_C of matrix U – are the left singular vectors, the columns v_1, \dots, v_C of matrix V – are the right singular vectors, and the values $\sigma_1, \dots, \sigma_C$ – are the singular values of matrix F .

The singular value decomposition of matrix F is not unique in the general case. According to [19], a vector is called lexicographically positive if its first nonzero component is positive. The singular value decomposition $F=U \Sigma V^T$ is called normal if the columns of the matrix U are lexicographically positive. According to [19], a matrix has a unique normal singular value decomposition if its singular values are pairwise distinct and nonzero.

Let us consider a steganographic embedding method for a secret message based on singular value decomposition, as presented in [20]. The authors note that the proposed approach ensures a high embedding capacity, demonstrates robustness against typical and some targeted distortions, and that the results of experimental testing confirmed its resilience to JPEG image compression down to 40%. To implement the method, the secret message is first converted into a sequence of decimal numbers according to ASCII codes, which are then transformed into a binary representation, forming a binary sequence. For a color image selected as the cover, a matrix from one of the color channels is chosen.

The embedding method of the secret message involves a step-by-step processing of the image matrix F , which includes dividing it into blocks f of size $N \times N$, each of which is used to embed a single bit of the message. Singular value decomposition is performed for each block, after which the largest singular value is quantized using a step size d . Depending on the bit to be embedded, the quantized value is modified to match the desired parity. Then, an updated value of the largest singular value is formed, and the inverse reconstruction of the block is carried out. After all blocks have been processed, the updated image matrix is constructed.

In [20], experimental results demonstrate that the effectiveness of the method depends on the quantization step and block size, which can be used as components of the secret key. The influence of these parameters on the robustness and imperceptibility of the embedded data was investigated. In particular, increasing the quantization step improves robustness against distortions but reduces imperceptibility. Optimal values of the parameter d are recommended for the red, green, and blue channels, along with acceptable ranges of variation for each.

The extraction method of the secret message involves dividing the image matrix F into blocks f of size $N \times N$, each used to recover a single bit. Singular value decomposition is performed for each block, and the largest singular value is quantized using a step size corresponding to the respective color channel. The embedded bit is determined based on the parity of the quantized value. The recovered bits are then combined to reconstruct the original message.

To demonstrate the functionality of the proposed steganographic method, a software implementation was developed, and an experiment was conducted. A color image of size 872×576 pixels was used as the cover. The embedding was performed in the blue channel, which was segmented into 8×8 blocks. The generated secret message corresponded to the number of blocks, with each bit embedded into the largest singular value of the respective block using a quantization

step of $d=52$. Only the blue channel was modified, while the red and green channels remained unchanged. The results are presented in Figure 1.



Figure 1: Digital images: (left) before applying the steganographic method; (right) after applying the method.

An expert visual analysis of the images before and after steganographic embedding into the blue channel revealed no noticeable changes. This is consistent with the well-known fact that the human eye is least sensitive to the blue channel, which ensures high visual imperceptibility.

The steganographic method investigated and implemented for experimental purposes is considered one of the most effective in ensuring robustness against one of the most common types of attacks on hidden information, compression attacks, particularly in the JPEG format. The method's high resilience stems from the fact that modifications are applied not in the pixel domain, but in the principal component domain, where certain components are less sensitive to global structural changes caused by compression. Moreover, due to its solid mathematical foundation and the use of well-formalized block-based parameters, specifically, the largest singular values of each block, the method exhibit high predictability and controllability. These characteristics ensure its universality and suitability for further enhancement. The effectiveness of using singular values as information carriers has been repeatedly emphasized in contemporary scientific literature, further confirming the relevance of the chosen approach [21, 22]. Thus, the method serves as a conceptual foundation for the development of modified information hiding schemes with enhanced robustness and stealth.

A distinguishing feature of the proposed approach is the use of quantization, whereby the values of components are modified according to a predefined quantization step of the color channel. This technique enables efficient embedding of information bits while preserving the visual quality of the image.

At the same time, the principle that underlies the effectiveness of the embedding process can also be applied in reverse, for the purpose of detecting potential steganographic activity, specifically the presence of hidden secret messages. This is achievable even in the absence of access to the original image or the steganographic key.

Since the embedding method is characterized by a well-defined mathematical structure, specifically, the modification of block singular value sets according to a fixed-multiplicity rule, it becomes possible to develop a specialized steganalysis approach capable of detecting statistical deviations within the distribution of singular values.

Consider a digital image in which the matrices of each color channel are preliminarily divided into blocks of fixed size. For each block, singular value decomposition is performed, resulting in a set of the largest singular values for each color channel. Taking into account the specified quantization steps for the respective color channels, the following value is computed for the largest singular value of each block according to the expression:

$$\delta = \sigma_1 - \left\lceil \frac{\sigma_1}{d} \right\rceil \cdot d \quad (2)$$

where d – is the quantization step of the color channel;

σ_1 – is the largest singular value of the block from the color channel matrix.

For each resulting set of δ values corresponding to the three color channels, histograms can be constructed.

Figure 2 presents a set of such histograms for the digital image shown in Figure 1, which was used as the original image prior to applying the secret message embedding method.

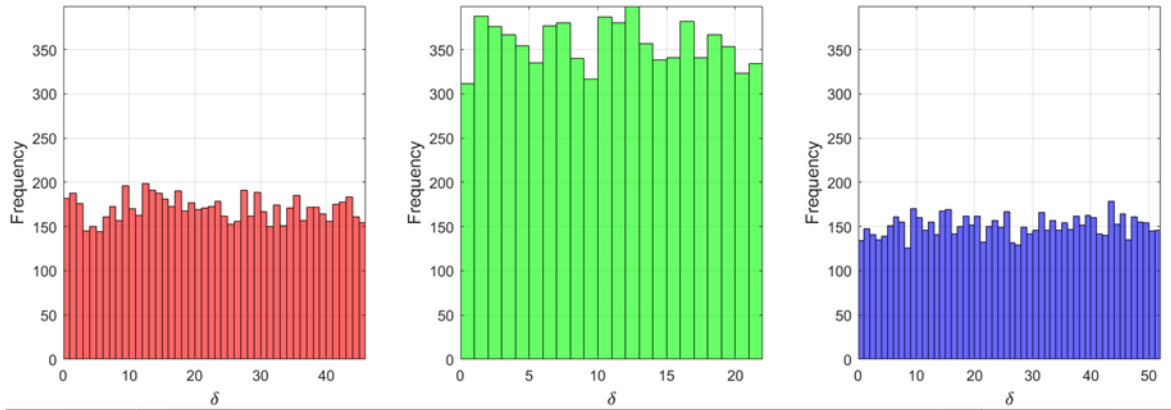


Figure 2: Histograms of δ for the three color channels of the digital image prior to the application of the secret message embedding method.

Figure 3 presents a set of histograms corresponding to the digital image shown in Figure 1, after applying the method of secret message embedding into the blue color channel.

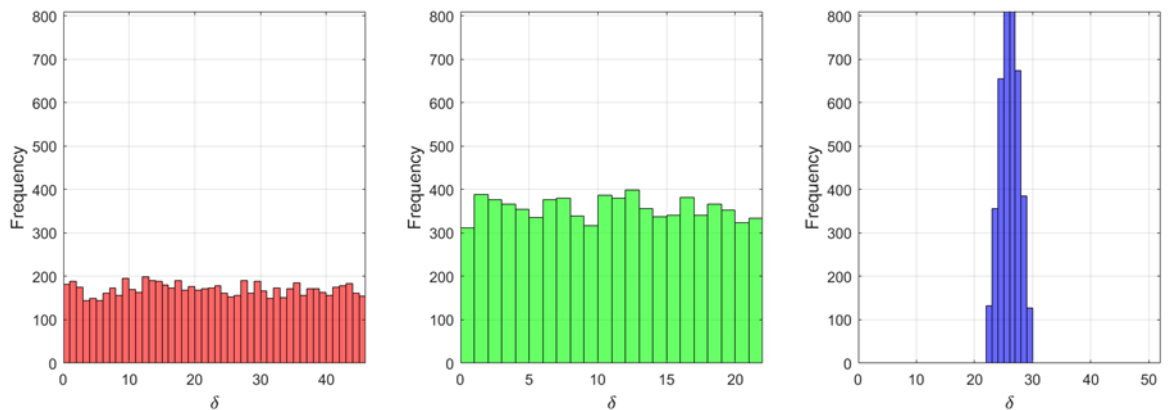


Figure 3: Histograms of δ for the three color channels of the digital image after applying the secret message embedding method to the blue channel.

The histograms of the color channels constructed for the images before and after applying the steganographic method are representative of the majority of images used in the conducted statistical study.

Based on the available statistical data set, a hypothesis can be formulated regarding their conformity to a uniform distribution. To verify this hypothesis, an appropriate statistical procedure must be applied. Such an analysis enables the assessment of how well the empirical data distribution aligns with the theoretical uniform distribution, which constitutes an important step in further investigation and justification of the conclusions.

To confirm or refute the hypothesis regarding the conformity of the statistical data distribution to the uniform distribution, the Kolmogorov-Smirnov test will be applied [23–25]. The choice of this test is justified by its non-parametric nature, which does not require prior knowledge of the parameters of the theoretical distribution. This ensures its versatility and convenience for analyzing

a wide range of empirical data. Furthermore, the Kolmogorov-Smirnov test demonstrates high effectiveness when working with small and medium-sized samples, which is a significant advantage over the Pearson test, which is less suitable under such conditions.

The main steps for applying the Kolmogorov-Smirnov test to assess the hypothesis of uniform distribution of empirical data are as follows:

1. formulate the hypotheses: null hypothesis H_0 the sample comes from a uniform distribution over the interval $[a,b]$; alternative hypothesis H_1 the sample does not come from a uniform distribution over $[a,b]$;
2. normalize the data;
3. sort the sample data in ascending order: $x_1 \leq x_2 \leq \dots \leq x_n$;
4. compute the empirical distribution function: for each x_i calculate $F_n(x_i) = \frac{i}{n}$;
5. compute the theoretical distribution function for the uniform distribution: $F(x_i) = x_i$;
6. calculate the maximum absolute deviation between the empirical and theoretical distribution functions: $D_n = \max_x |F_n(x) - F(x)|$;
7. determine the critical value D_k for the chosen significance level α from the Kolmogorov-Smirnov critical value table;
8. accept or reject the hypothesis: if $D_n > D_k$, the null hypothesis H_0 is rejected; if $D_n \leq D_k$, the null hypothesis H_0 is accepted.

Taking into account the conducted research, the steganalysis method for digital images based on the analysis of the singular values of image matrix blocks consists of the following steps:

1. select the matrix F corresponding to a chosen color channel of the image;
2. select the quantization step d appropriate for the chosen color channel;
3. select the block size N of matrix;
4. partition the matrix F into non-overlapping blocks f of size $N \times N$;
5. for each block f , perform the following:
 - a. compute the set of singular values via singular value decomposition $f = U \Sigma V^T$ (1);
 - b. calculate the statistic δ in accordance with formula (2);
6. apply the Kolmogorov-Smirnov test to the set of δ values: if the null hypothesis is accepted, the container is considered empty; if the hypothesis is rejected, the container is assumed to contain hidden data.

5. Discussions

The proposed steps of the method are applied to the matrices of each color channel using a corresponding quantization step selected from the set of permissible values established by the authors through empirical studies in [20], and for each block partitioning with sizes proposed in [20], namely 4, 8, 16, 32, and 64.

During the implementation of the method, a set of parameter combinations is formed, including F – the selected color channel matrix, d – the quantization step, and N – the block size. For each of these combinations, statistical verification is performed using the Kolmogorov-Smirnov test. If the null hypothesis of distribution conformity is rejected, the corresponding parameter combination is interpreted as an indicator of the presence of steganographic embedding. The collection of such combinations may serve as a steganographic key, enabling the detection of hidden information transmission within a digital image.

Figure 4 presents the empirical and theoretical distribution function plots obtained as a result of applying the Kolmogorov-Smirnov test to the values of the three color channels of the digital image shown in Figure 1, which was used as the original image prior to secret message embedding.

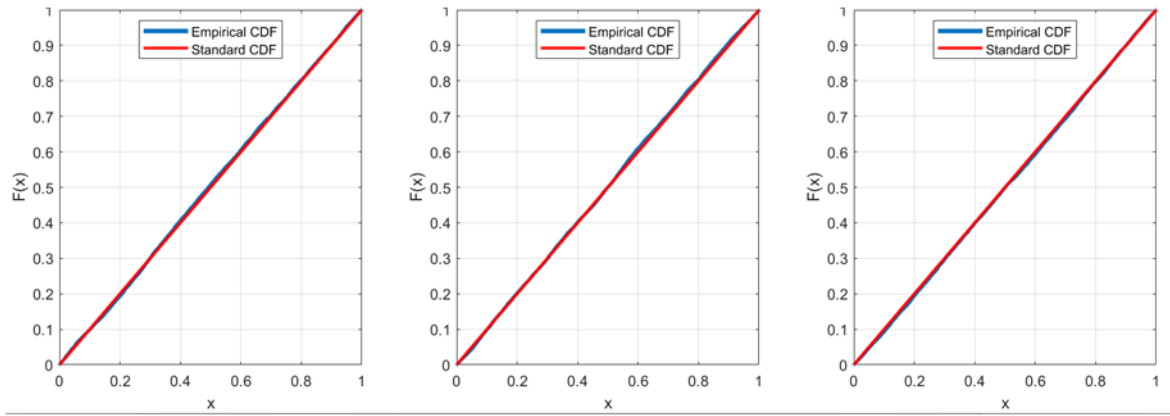


Figure 4: A study of the Kolmogorov-Smirnov test for the three color channels of the digital image prior to applying the secret message embedding method.

Figure 5 presents the empirical and theoretical distribution function plots obtained as a result of applying the Kolmogorov-Smirnov test to the values of the three color channels of the digital image shown in Figure 1, after the secret message embedding procedure was performed.

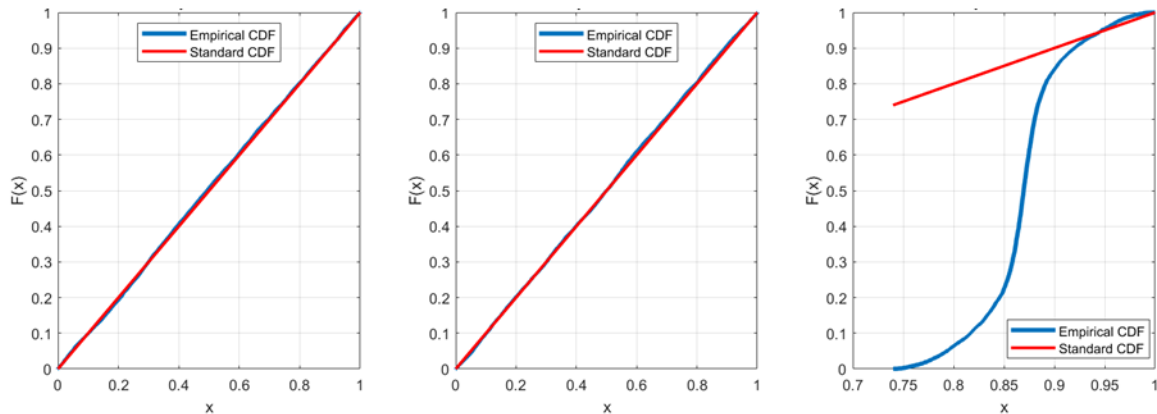


Figure 5: A study of the Kolmogorov-Smirnov test for the three color channels of the digital image after applying the secret message embedding method to the blue channel.

As a result of the study, the null hypothesis regarding distribution conformity was rejected under the following conditions: F – blue color channel, $d = 52$ – quantization step, and $N=8$ – block size, which together define the steganographic key.

6. Performance Assessment

The evaluation of the effectiveness of a steganalysis method is based, in particular, on its ability to perform reliable binary classification of images with respect to the presence or absence of hidden secret information. To quantitatively assess the quality of such detection, statistical indicators are employed that reflect the probability of two types of classification errors. A false positive (type I error) occurs when the method incorrectly detects hidden data in an image that, in reality, contains none. A false negative (type II error) arises when the presence of steganographic content goes undetected. Since reducing the likelihood of one type of error typically increases the other, it is appropriate to apply metrics that assess the overall balance between the method's sensitivity and specificity. This approach enables the reasoned selection of the method's operational point within an acceptable trade-off between detection accuracy and the probability of false alarms.

The experimental setup comprised both hardware and software components essential for the implementation, execution, and evaluation of the steganography and steganalytic processes. All experiments were carried out on a personal computer equipped with an Intel Core i7 processor, 16

GB of RAM, and operating under the Windows 10 environment. The steganalysis method was implemented in the C# programming language, utilizing the OpenCV library for image processing tasks.

As part of the experimental study, a dataset of digital images in both uncompressed and compressed formats was created to simulate the process of hidden data embedding with varying container payload levels. The embedding was carried out using the previously described method, based on the modification of the largest singular value. Five embedding levels were considered: 5%, 25%, 50%, 75%, and 100% of the maximum number of blocks available for embedding. The secret messages were generated randomly as binary sequences of the required length, and the embedding was performed across different color channels. The overall dataset was balanced: half of the images served as empty containers, while the other half contained embedded data at varying payload levels. The developed steganalysis method was applied to each image in the dataset to evaluate its detection performance.

The analysis of the experimental results revealed a clear pattern. At embedding levels of 100%, 75%, and 50%, the steganographic content was detected with 100% accuracy, without any occurrence of false negatives (type II errors). Beginning at the 25% embedding level, a decline in the method's sensitivity was observed, as some instances of hidden data remained undetected, indicating the presence of type II errors. When the embedding rate was reduced to 5%, the proportion of undetected steganographic images increased to approximately 30%, demonstrating a significant decrease in detection effectiveness. It is important to note, however, that throughout the entire series of experiments, the false positive rate (type I error) remained below 1%, indicating a high level of specificity for the proposed method.

In addition to detection accuracy, an equally important characteristic of a steganalysis method is its computational efficiency, particularly in scenarios requiring large-scale image processing or real-time performance. A comparative performance analysis of the method was conducted in two implementation modes: a standard mode involving pixel-by-pixel access to image data, and an optimized mode that enables direct byte-level access through the use of pointers. This comparison allows for the assessment of the method's suitability for time-sensitive or high-throughput applications.

The analysis of the obtained results indicates that the use of the optimized mode for accessing pixel data significantly reduces the execution time of the steganalysis method, on average by a factor of 4 to 5 compared to the standard implementation. The most notable improvement in processing speed is observed at higher embedding levels, where a larger number of blocks must be analyzed.

Such a result can be explained by the significant overhead inherent in classical image processing methods, particularly due to the need to create auxiliary objects and to perform data structure copying or transformation operations. In contrast, the optimized approach provides direct access to the byte-level representation of the image, which eliminates these overheads and significantly enhances performance, especially when processing high-resolution or large-volume images.

7. Conclusions

This study proposes a novel approach to steganographic analysis of digital images, based on the detection of anomalies in the distributions of modified components of the largest singular values within image matrix blocks. The method employs quantization of singular values followed by statistical evaluation of the resulting data using the Kolmogorov–Smirnov test. This enables the identification of hidden information embedding without requiring access to the original image and allows for the potential extraction of the steganographic key.

The results of the experimental study demonstrated the high effectiveness of the proposed method at medium and high levels of container payload. Specifically, for embedding rates of 50% and above, the method achieved 100% detection accuracy with no occurrence of false negatives. At the same time, the false positive rate remained below 1% across the entire dataset, indicating a high degree of specificity.

Particular attention was given to the analysis of the computational efficiency of the method's implementation. A comparison between the standard approach and an optimized version, based on direct access to the image's byte-level representation, revealed an average processing speed-up of 4 to 5 times. This performance gain makes the method suitable for real-time applications and for processing large volumes of image data.

A promising direction for future research includes the adaptation of the method for video stream analysis, as well as integration with machine learning techniques to enhance adaptability and resilience against emerging steganographic attacks.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

- [1] H.F. Konakhovych, D.O. Prohonov, O.Yu. Puzyrenko, *Computer Steganographic Processing and Analysis of Multimedia Data*. Kyiv: Center of Educational Literature, 2018.
- [2] V.O. Khoroshko, Yu.Ye. Yaremchuk, V.V. Karpinets, *Computer Steganography: A Textbook*. Vinnytsia: VNTU, 2017.
- [3] BBC News, "Accessing the secrets of the brotherhood". URL: <http://news.bbc.co.uk/2/hi/science/nature/2082657.stm>
- [4] The Guardian, "FBI breaks up alleged Russian spy ring in deep cover". URL: <https://www.theguardian.com/world/2010/jun/29/fbi-breaks-up-alleged-russian-spy-ring-deep-cover>
- [5] Ars Technica, "Steganography: how al-Qaeda hid secret documents in a porn video". URL: <https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video>
- [6] BleepingComputer, "Hackers hide credit card data from compromised stores in JPG file". URL: <https://www.bleepingcomputer.com/news/security/hackers-hide-credit-card-data-from-compromised-stores-in-jpg-file>
- [7] BleepingComputer, "New SteganoAmor attacks use steganography to target 320 orgs globally". URL: <https://www.bleepingcomputer.com/news/security/new-steganoamor-attacks-use-steganography-to-target-320-orgs-globally>
- [8] N.V. Koshkina, *Spectral methods of computer steganography and steganoanalysis methods with training and classification*, Doctor of Technical Sciences thesis, The National Academy of Sciences of Ukraine, V.M. Glushkov Institute of Cybernetics, Kyiv, Ukraine, 2016.
- [9] A. Westfeld, A. Pfitzmann, Attacks on Steganographic Systems, in *Lecture Notes in Computer Science*, vol. 1768, 2000, pp. 61–75.
- [10] J. Fridrich, M. Goljan, R. Du, Reliable detection of LSB steganography in color and grayscale images, in *MM&Sec '01: Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges*, 2001, pp. 27–30. <https://doi.org/10.1145/1232454.1232466>
- [11] J. Fridrich, M. Goljan, R. Du, Steganalysis based on JPEG compatibility, in *International Symposium on the Convergence of IT and Communications*, Denver, CO, USA, 2001. <https://doi.org/10.1117/12.448213>
- [12] S. Lyu, H. Farid, Detecting hidden messages using higher order statistics and support vector machines, in *Proceedings of Lecture Notes in Computer Science*, 5th International Workshop on Information Hiding, vol. 2578, 2002, pp. 340–354.
- [13] J. Davidson, C. Bergman, E. Bartlett, An artificial neural network for wavelet steganalysis, in *Proceedings of SPIE: The International Society for Optical Engineering, Mathematical Methods in Pattern and Image Analysis*, vol. 5916, 2005, pp. 1–10. <https://doi.org/10.1117/12.615280>

- [14] S. Wu, S. Zhong, Y. Liu, A Novel Convolutional Neural Network for Image Steganalysis With Shared Normalization, *IEEE Transactions on Multimedia*, vol. 22, no. 1, 2020, pp. 256–270. <https://doi.org/10.1109/TMM.2019.2920605>
- [15] A. Kuznetsov, N. Luhanko, E. Frontoni, Image steganalysis using deep learning models, *Multimedia Tools and Applications*, vol. 83, 2024, pp. 48607–48630. <https://doi.org/10.1007/s11042-023-17591-0>
- [16] R.C. Gonzalez, R.E. Woods, *Digital Image Processing*, 4th ed., Pearson, New York, NY, 2018.
- [17] J.W. Demmel, *Applied Numerical Linear Algebra*, SIAM, Philadelphia, PA, 1997.
- [18] G.H. Golub, C.F. Van Loan, *Matrix Computations*, 4th ed., Johns Hopkins University Press, Baltimore, MD, 2013.
- [19] C. Bergman, J. Davidson, Unitary Embedding for Data Hiding with the SVD, in *Security, Steganography, and Watermarking of Multimedia Contents VII*, SPIE, vol. 5681, 2005, pp. 619–630. <https://doi.org/10.1117/12.587796>
- [20] L. Popyack, M. Sieffert, R. Forbes, C. Green, T. Blake. Assured Information Security: A Stego Intrusion Detection System, presented at the *Digital Forensic Research Workshop (DFRWS) USA*, 2004.
- [21] I.I. Bobok, A.A. Kobozeva, O.A. Laptiev, V.A. Savchenko, T.L. Kurtseitov. Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel. *Problems of the Regional Energetics*, vol. 2 (66), 2025, pp. 90–104.
- [22] I.I. Bobok, A.A. Kobozeva, Localization of the Disturbance Region of Formal Parameters of a Steganographic Container to Ensure the Robustness of a Stegosystem, *Radioelectronics and Communications Systems*, 67(8), 2024.
- [23] F.J. Massey. The Kolmogorov-Smirnov Test for Goodness of Fit. *Journal of the American Statistical Association*, vol. 46, no. 253, 1951, pp. 68–78.
- [24] G. Marsaglia, W. Tsang, J. Wang. Evaluating Kolmogorov's Distribution. *Journal of Statistical Software*, vol. 8, issue 18, 2003, pp. 1–4. <https://doi.org/10.18637/jss.v008.i18>
- [25] MathWorks. One-sample Kolmogorov–Smirnov test. URL: <https://www.mathworks.com/help/stats/kstest.html>