REPUBLIC OF AZERBAIJAN

On the right of the manuscript

ABSTRACT

of the dissertation for the degree of Doctor of Philosophy

RESEARCH AND DEVELOPMENT OF EFFECTIVE ALGORITHMS FOR HIDING CONFIDENTIAL INFORMATION

Specialty: 3339.01– Information protection methods and systems, information security

Field of science: Technical sciences

Applicant: **Ababil Faxraddin gizi Naghiyeva**

Ganja – 2025

The work was performed at Azerbaijan Technological University.

Scientific consultant: doctor of technical sciences, professor
Sakit Gambay oglu Verdiyev

Official opponents: ----------

Dissertation Council No ED 1.35 operating under the Institute of Information Technologies of the Ministry of Scienc and Education of the Supreme Attestation Commission under the President of the Republic of Azerbaijan

Chairman of the Dissertation council:

_____

Scientific secretary of the Dissertation council:

_____

Chairman of the scientific seminar:

_____

GENERAL CHARACTERISTICS OF THE WORK

Relevance of the Study. The widespread use of the Internet and modern wireless communication tools has created new opportunities for the large-scale exchange of multimedia information. In this regard, new challenges have emerged concerning the security of both stored information and data transmitted via global and local networks. Recently developed and globally used networks, software, and various digital devices have significantly expanded users' access to multimedia resources at a global scale. As a result, the interest of malicious actors in detecting confidential information transmitted through open communication channels has increased.

Protecting confidential information from unauthorized interference in the digital environment has become a matter of utmost importance. Various approaches are applied in the field of information security, including cryptography, steganography, watermarking, and others. In cryptographic methods, the content of information is protected by encryption. Although a malicious attacker may observe the transmission of confidential information, they cannot utilize it, as the encrypted content cannot be deciphered without the appropriate key.

Steganography, which enables the concealment of information, plays a significant role in confidential communication. It is a scientific field dedicated to the embedding and transmission of secret information within various multimedia files such as images, audio, video, and text documents. The fundamental principle of steganography is that the transmitted information remains imperceptible, making it impossible for an attacker to detect the existence of hidden content.

Thus, the primary objective of steganography is to conceal not the content itself, but the very fact of information transmission. The advantage of steganography lies precisely in this feature, as the hidden confidential data remains invisible to malicious adversaries. On the recipient's side, the concealed information can be successfully extracted from the carrier file i.e., the stego-file without any distortion or loss, and subsequently used as intended.

In the design and development of steganographic systems, particular attention is usually given to the following issues:

- undetectability;
- robustness (resistance to various types of attacks);
- the capacity of confidential information to be embedded into the container;
- the visual quality of the stego-image.

Steganography as a scientific field is applied in numerous areas, such as confidential correspondence, medical, military, and other domains. For example, in hospitals, clinical information can be embedded into medical images and transmitted to a physician operating remotely. It is evident that in such cases even the slightest alteration of the original image may lead to the distortion of patient-related data, which in turn may result in an incorrect diagnosis—an outcome that is absolutely unacceptable.

The effectiveness of a secret information hiding algorithm is primarily characterized by the following factors:

- the total volume of confidential information;
- the visual quality parameters of the digital image serving as the information carrier;
- the volume of the hidden confidential information.

By the volume of hidden confidential information, it is meant the total number of confidential information bits that can be embedded into the container image using the applied hiding algorithm.

A container image with embedded information is referred to as a stego-image, and in order to assess the quality of the hiding algorithm, the degree of similarity between the original and stego-images must be measured and verified using established methods. A compromise must be reached between embedding capacity and visual quality, since as the embedding volume increases, distortions in the image also increase, thereby reducing its quality. Every researcher working in the field of information hiding strives to achieve this balance.

The three main parameters characterizing algorithms embedding capacity, visual quality, and robustness are inherently contradictory. Therefore, reaching a compromise among them remains a major challenge for researchers. The conducted studies demonstrate that the use of newly developed information hiding algorithms with higher performance compared to existing ones makes it possible to establish systems for the confidential transmission of information among

interested parties. For malicious actors, such a transmission process appears as an ordinary file exchange.

Thus, it can be concluded that the role of research in the field of information system security is indisputable. However, the development of more efficient new information hiding algorithms is considered one of the most pressing issues today, which in turn confirms the relevance of the present research.

Object of the Research. The concealment of large volumes of confidential information transmitted over open communication channels within digital images using steganographic methods.

Subject of the Research. The development of steganographic algorithms that enable the transmission of large amounts of confidential information within grayscale and color images used as containers, without leaving perceptible visual traces.

Purpose of the Research. The investigation of steganographic methods and algorithms that ensure the protection of confidential information transmitted through open communication channels; the selection and comparative analysis of promising steganographic methods and algorithms; and the development of new steganographic algorithms.

For this purpose, the dissertation addresses the following objectives:

- To study recent steganographic methods and algorithms published in foreign literature and to formulate the research problem, in order to determine the level of investigation of the subject on a global scale;
- To develop steganographic algorithms that ensure the embedding of large amounts of confidential information into digital images at the input of the stegosystem and its extraction from the stego-image at the output;
- To design an algorithm for information hiding based on the Least Significant Bit (LSB) substitution method;
- To develop an algorithm that enables the hiding of large volumes of information based on image interpolation;
- To propose an algorithm for embedding large volumes of confidential information using quorum functions;

- To develop an information hiding algorithm for color images by employing the Scale Invariant Feature Transform (SIFT) method.

Research Methods. To address the objectives presented in the dissertation, the following methods were employed: embedding confidential information into container images using spatial domain techniques, image interpolation, least significant bit (LSB) substitution, pixel difference values, and SIFT algorithms; steganographic analysis; measurement of similarity between images using Peak Signal-to-Noise Ratio (PSNR); histogram methods; and structural analysis of images.

Key Statements Submitted for Defense:

- Comprehensive study of existing high-performance hiding algorithms in recent domestic and international research;
- Development of a priority-based visual quality information hiding algorithm;
- Design of a data hiding algorithm based on interpolation;
- Development of a steganographic algorithm ensuring the hiding of large volumes of confidential information and maintaining visual quality based on quorum functions;
- Development of confidential information hiding algorithms for color images using the SIFT algorithm.

Scientific Novelty. The dissertation presents the following results characterized by scientific and practical novelty:

- Development of a new steganographic algorithm for embedding information into images;
- Analysis of recently published, high-performance, exemplary hiding methods and algorithms in the scientific literature;
- Development of a high-robustness, visual quality-prioritized algorithm for hiding large volumes of confidential information;
- Creation of a new steganographic algorithm enabling large-volume information hiding based on image interpolation;
- Design of a steganographic algorithm capable of hiding large volumes of confidential information based on quorum functions;
- Development of a high-quality confidential information hiding algorithm for color images using the SIFT method.

Theoretical and Practical Significance.

- The results of the analysis and experiments can be used in the development of new steganographic algorithms;
- Developed algorithms can be applied in confidential correspondence, medical imaging, copyright protection, and other fields;
- Each proposed algorithm can be used to securely hide and transmit large volumes of confidential information via open communication channels in stego-images;
- Due to the high visual quality of the stego-images, each algorithm can be widely applied in scenarios requiring high confidentiality and robustness;
- Each algorithm offers simple computational implementation compared to alternatives, ensuring broader applicability;
- The work can serve as a valuable resource for students specializing in information security.

Approval and Application. The main results of the dissertation were presented and extensively discussed at the following national and international scientific-practical conferences:

- *Current Scientific-Practical Problems of Software Engineering. II Republican Conference* – Baku, May 17, 2017;
- *Technical Sciences in Russia and Abroad: VII International Scientific Conference* – Moscow, November 2017;
- *Current Problems of Information Security. III Republican Scientific-Practical Seminar* – Baku, December 8, 2017;
- *Current Problems of Infocommunications in Science and Education: VII International Scientific-Technical and Methodological Conference* – Saint Petersburg, February 28–March 1, 2018;
- *Current Multidisciplinary Scientific-Practical Problems of Information Security. IV Republican Conference* – Baku, December 14, 2018;
- *Current Multidisciplinary Scientific-Practical Problems of Information Security. V Republican Conference* – Baku, November 29, 2019;

- *Advances in Computing, Communication, Embedding and Secure Systems. II International Conference* – India, September 2–4, 2021 (Scopus);
- *Advances in Computing, Communication, Embedding and Secure Systems. III International Conference* – India, May 18–20, 2023 (Scopus).

Scientific Publications. The main results of the dissertation are reflected in five publications: three articles were published in journals listed in the Russian AAK database—one in a Scopus-indexed international journal, one in the Russian indexing system RINC, and one in another AAK-listed journal. Two articles were published in Azerbaijan in journals meeting AAK requirements.

Institution Where the Research Was Conducted. The dissertation was carried out at the Department of Computer Engineering and Telecommunications, Azerbaijan Technological University.

Structure and Volume of the Dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a bibliography of 109 references, and an appendix. It includes 23 tables and 47 figures. The total volume of the dissertation is 169 pages, with the main text covering 140 pages. The total character count of the dissertation is 179,248. The character count by sections is as follows: Title page – 408 characters; Table of contents – 1,454 characters; Introduction – 10,361 characters; Main body (chapters, paragraphs, sections) – 165,647 characters; Conclusion – 1,367 characters; References – 18,644 characters; Appendix – 3,610 characters; List of abbreviations and symbols – 1,702 characters.

THE MAIN CONTENT OF THE DISSERTATION

The introduction substantiates the relevance of the dissertation topic, defines the research problem, and outlines the scope of the work undertaken.

In the first chapter *(*The significance and directions of information security*)* [1,2,5,13], the concept of information security, the role and importance of steganography in information security, the distinctions between steganography and cryptography, the evaluation of

steganographic methods, categories of steganographic techniques, image steganography, current unresolved problems in the field of steganography, and the assessment of algorithm security using steganalysis methods are examined and analyzed. Various algorithms based on different techniques are employed to hide confidential information in image steganography, and this chapter reviews recently proposed methods.

The interpolation-based information hiding method was first introduced as the *Neighbor Mean Interpolation (NMI[1])* method in 2009 by Ki-Hyun Jung and Kee-Young Yoo. This method enables the generation of pixels with higher clarity. The algorithms and operational principles of this and other selected methods are presented in detail and comprehensively analyzed in the dissertation.

When evaluating the main parameters of the selected algorithms, the same example images used by the authors in their publications were adopted as container images, and confidential information of the same size was embedded. The hiding process for each algorithm was carried out according to its specific procedural steps.

Analysis of the reviewed studies indicates that a single interpolation method has been combined with various hiding algorithms over different years, resulting in the development of new algorithms. Examples include the NMI and other interpolation-based algorithms. To validate the proposed algorithms, the same original image was used as the container, and confidential information of identical size was embedded using the respective algorithms. Subsequently, the resulting stego-image was evaluated in terms of PSNR, MSE, SSIM, histogram correlation (HC), and total embedding capacity was calculated using the formulas presented below.

Mean Squared Error – MSE

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (C_{i,j} - S_{i,j})^2. \quad (1)$$

here M the image width, N image height, C the pixel set of the container image, and S the pixel set of the stego-image are given. The Root Mean Square Error (RMSE)

[1] Jung K.H, Yoo K.Y. Data hiding method using image interpolation //Comput Stand Interfaces,- 2009.№ 31,- p.465-470.

$$RMSE = \sqrt{MSE} \quad (2)$$

here MSE is the mean squared error (as defined above). RMSE is the square root of the MSE and expresses the error in the same units as the original data. It provides a more interpretable and comparable result. Signal-to-Noise Ratio – SNR (Signal To Noise Ratio)

$$SNR = 10 \times log_{10}\left(\frac{\sum_{i=1}^{M\times N}(C_i)^2}{\sum_{i=1}^{M\times N}(C_i - S_i)^2}\right) \quad (3)$$

here C_i is the i -th element of the original signal, S_i is the i -th element of the estimated signal. SNR measures the ratio of signal power to noise (error) power in decibels (dB). A higher SNR indicates better signal quality.

Peak Signal-to-Noise Ratio – PSNR (Peak Signal To Noise Ratio)

$$PSNR = 10 \times log_{10}\left(\frac{Max^2}{MSE}\right) \quad (4)$$

here Max is the maximum possible pixel value (e.g., 255 for 8-bit images), MSE is the mean squared error. PSNR measures the ratio between the maximum possible signal and the error, expressed in decibels. A higher PSNR means higher image quality.

Structural Similarity Index Measure – SSIM (Structural Similarity Index Measure).

$$SSIM(x, y) = \left(\frac{((2\cdot\mu_x\cdot\mu_y + C_1)\cdot(2\cdot\sigma_{xy} + C_2))}{((\mu_x{}^2 + \mu_y{}^2 + C_1)\cdot(\sigma_x{}^2 + \sigma_y{}^2 + C_2))}\right) \quad (5)$$

here μ_x, μ_y – the mean (luminance) values of images x and y, $\sigma_x{}^2$, $\sigma_y{}^2$ – the variance (contrast) of the images, σ_{xy} – the covariance between the two images (structural similarity), C_1, and C_2– small constants to prevent division by zero. SSIM evaluates the similarity between two images in terms of structure, brightness, and contrast, with values ranging from 0 (no similarity) to 1 (identical images).

Amount of Hidden Secret Information: Another steganographic evaluation parameter, embedding capacity, indicates the number of secret information bits embedded per pixel.

$$EC = \frac{tutum}{W\times H} \quad (6)$$

here, W and H represent the width and height of the image, respectively.

The results of the conducted analysis are presented in Table 1.3.1 of the dissertation. In this table, the highest total embedding capacity is observed in the proposed data hiding algorithm based on the interpolation method called New Interpolation Expansion (NIE[2]). In this method, the total embedding capacity reaches 445,644. However, the visual quality of the image is significantly reduced (PSNR = 24.05), and although the mean squared error (MSE) is within acceptable limits, the image exhibits more distortions.

From this, it can be concluded that visual distortions in the proposed algorithm limit the possibility of embedding more information.

The highest PSNR value in the table belongs to the algorithm proposed by Sabeen G. et al., which is based on interpolation using the Enhanced Neighbor Mean Interpolation (ENMI[3]) method. In this algorithm, while the visual quality of the image is high (PSNR = 47.69), the mean squared error (MSE) indicates the presence of more distortions in the image (MSE = 0.016).

In contrast, the NIE method, despite having a lower PSNR value of 24.05, has a lower MSE of 0.009, suggesting fewer pixel-level errors. Therefore, when developing new algorithms, the results obtained here should be carefully considered.

As a result of the analysis of the most successful steganographic methods in recent years, it is concluded that the algorithms proposed for information hiding, in terms of quality, necessitate the development of new steganographic algorithms that can provide higher embedding capacity.

In Chapter 2 (Development of new steganographic algorithms), the essence of three newly proposed steganographic algorithms is explained. The proposed algorithms in this chapter are:

---

[2] Ahmad A. M., Al-.Haj, A., Mahmoud, F. An improved capacity data hidin technique based on image interpolation // Multimedia Tools and Applications, Springer,- 2019. № 78, 6,- p.7181-7205**.**

[3] Sabeen, G. P. V. Sajila, M. K. Bindiya, M. V. A two stage data hiding scheme with high capacity based on interpolation and difference expansion // Procedia Technology, Elsevier,-2016. 24(1), -p. 1311 – 1316.

- A secret data hiding algorithm based on the Least Significant Bit (LSB) replacement method;
- A secret data hiding algorithm based on image interpolation;
- An information hiding algorithm based on the quorum function.

Each step of the implementation of the proposed steganographic algorithms is explained in detail in the dissertation.

In the algorithm based on the Least Significant Bit (LSB) replacement method [9, 13], priority is given to preserving the visual quality of the image, and the algorithm is built upon a newly proposed LSB-based steganographic approach.

The main goal of this section is to develop a data hiding algorithm that prioritizes large-capacity embedding, high robustness, and preservation of visual quality of the stego-image. The problem is addressed in two stages [9].

In the first stage, the secret data is embedded using LSB substitution based on a secret key.

In the LSB algorithm, the least significant bits of each byte of the image pixels are replaced with bits of the secret information. This replacement can be done sequentially from the beginning or end of the image, or applied to specific pixels randomly selected using a pseudo-random number generator.

In this approach, although bit replacement is carried out from the beginning to the end of the file, a stego-key is used to randomly select pixels via a pseudo-random function, and the secret data is embedded in those pixels.

The use of a stego-key increases security, as the secret data cannot be extracted without the key during the decryption process.

In the second stage, the input container image is divided into 2×2 blocks, and the minimum pixel value within each block is selected. Then, the differences between the minimum pixel and the remaining three pixels are calculated.

These differences, in decimal, are converted to binary values. This operation is performed across all 2×2 blocks of the container image.

Afterwards, excluding the minimum pixels, the LSBs of the pseudo-randomly selected remaining pixels are replaced with secret bits. These

modified binary values are then converted back to decimal and added to the minimum pixel value.

Thus, the entire secret message is embedded into the randomly selected pixels within the 2×2 blocks (excluding the minimum pixel), resulting in the formation of the stego-image.

The processes of embedding and extraction of the secret data are carried out using the same stego-key.

The goal of the new algorithm is to generate a stego-image with higher robustness and minimal distortion of the original image.

A more detailed explanation of the proposed algorithm is provided in the following section.

The process of embedding secret information into the container image:

Step 1. Let us assume that N is the number of available container bits, and P_0^N is a permutation of the numbers from 0 to $N-1$. The pixels where we will embed the secret information bits are defined as $P_0^N(0), P_0^N(1),.....P_0^N(n-1)$. The permutation function we use must be random and dependent on a secret key K, because the selected bits should be chosen randomly. As a result, the secret information bits can be spread throughout the container.

To achieve this, a pseudo-random permutation generator is required. This function takes the secret key K as an input and generates different values in the range $\{0,...N-1\}$. Without knowing the secret key K, no one should be able to guess where the secret information bits are located.

Step 2. To create a pseudo-random permutation generator, a pseudo-random function can be used. This can be easily achieved by concatenating the secret key K with the input argument $i\{i=0,...n-1\}$, and then applying any secure hash function H:

$$f_K(i) = H(K \circ i) \quad \textbf{(7)}$$

here, $(K \circ i)$ represents the concatenation of the key K with the argument i. In this way, we obtain a pseudo-random function $f_K(i)$ that is dependent on the parameter K.

For the pseudo-random permutation generator, it is necessary to define an operation that performs a bitwise XOR (modulo 2 addition) between a and b, such that the result has the same bit length as :

$$(a \oplus b)$$

This ensures the output remains within the defined bit size and maintains the randomness required for the permutation.

Step 3. The binary argument i, which is of length $2l$, is divided into two parts of equal length:

- X (the last L bits), and
- Y (the first L bits).

Similarly, the secret key K is divided into four parts as K_1, K_2, K_3, K_4, each representing a portion of the key.

Step 4. By repeating the following algorithm 2^{2l-1} times, the pseudo-random permutation of $\{0,.....2^{2l-1}\}$ is obtained:

$$\begin{aligned} Y &= Y \oplus f_{K1}(X) \\ X &= X \oplus f_{K2}(Y) \\ Y &= Y \oplus f_{K3}(X) \\ Y &= X \oplus f_{K4}(Y) \\ &geri\ dönüş\ X \circ Y \end{aligned} \tag{8}$$

Step 5. The repeated values of X and Y determine the coordinates where the secret information bit will be embedded:

$$\begin{aligned} Y &= i\ div\ x \\ X &= i \bmod x \\ Y &= (Y + f_{K1}(X)) \bmod y \\ X &= (X + f_{K2}(Y)) \bmod x \\ Y &= (Y + f_{K3}(X)) \bmod y \\ &sonda\ Y * x + X \end{aligned} \tag{9}$$

Step 6. The original image is divided into 2×2 blocks, and within each block, the pixel with the lowest value is identified and designated as the minimum pixel (see Figure 1).

I_{11}	I_{12}
I_{21}	I_{22}

Figure 1. Container image block

Step 7. From each of the other three pixels, the value of the minimum pixel is subtracted. The difference value $D(i, j)$ is then calculated using formula (10):

$$D(i, j) = I(i, j) - \min \quad (10)$$

Step 8. The difference value $D(i, j)$, which is in decimal, is converted into the binary number system.

Step 9. In this step, the secret information bits are embedded by replacing the least significant bits (LSBs) of the binary $D(i, j)$ difference values of the randomly selected pixels in the container image.

Step 10. After the LSB operation is completed, the previously subtracted minimum value in each block is added back to the other pixels.

A numerical example of the solution and the extraction of secret information from the stego-image is explained in detail in the dissertation.

A Secret Information Hiding Algorithm Based on Image Interpolation [10]. In this section, a new algorithm is proposed for hiding secret information based on image interpolation. The advantage of the algorithm is its ability to embed a large amount of secret information using the interpolation method while maintaining the visual quality of the image.

The proposed method consists of the following stages:

- Image downscaling
- Image upscaling
- Embedding secret information using a new algorithm
- Extracting secret information from the stego-image

In the proposed algorithm, the process of embedding secret information is as follows: The digital implementation of the algorithm used to embed secret bits and the step-by-step execution of image processing operations are described below.

Step 1. The original image is divided into 3x3 blocks and interpolated. For this purpose, equation (11) is used.

$$
\begin{aligned}
&C(0,0) = O(0,0)\\
&C(0,1) = \left(O(0,0) + O(0,2)\right)/3 + \left(O(2,0) + O(2,2)\right)/6\\
&C(1,0) = \left(O(0,0) + O(2,0)\right)/3 + \left(O(0,2) + O(2,2)\right)/6\\
&C(1,1) = \left(O(0,0) + O(0,2) + O(2,0) + O(2,2)\right)/4
\end{aligned}
\tag{11}
$$

Here, $O(i, j)$ represents the pixels of the original image, and $C(i, j)$ represents the pixels of the container image generated using the interpolation method.

Step 2. The generated container image is divided into 2x2 blocks.

According to the proposed secret data hiding algorithm, the secret information bits should be embedded into the pixels located at the top-right, bottom-left, and bottom-right parts of the block. Based on the coordinates, the difference values between pixels are calculated using equation (12).

$$
\begin{aligned}
&d_1 = \max\left(|C_1(0,1) - C_1(0,0)|, |C_1(0,1) - C_2(0,0)|\right),\\
&d_2 = \max\left(|C_1(1,0) - C_1(0,0)|, |C_1(1,0) - C_3(0,0)|\right),\\
&d_3 = \max\left(|C_1(1,1) - C_1(0,0)|, |C_1(1,1) - C_2(0,0)|, |C_1(1,1) - C_3(0,0)|, |C_1(1,1) - C_4(0,0)|\right)
\end{aligned}
\tag{12}
$$

Step 3. After calculating the difference values to determine the number of secret bits to be embedded in each pixel, the results obtained from these calculations are converted from the decimal number system to the binary number system. The total number of 1s and 0s in the binary values determines the number of secret bits to be embedded into the container pixel.

Step 4. Once the number of secret bits to be embedded into each pixel is determined in Step 3, the secret bits are embedded into the container pixel using equation (13).

$$
\begin{aligned}
&S_1(0,1) = \begin{cases} C_1(0,1) + b_1, C_1(0,1) \le O_1(0,1) \\ C_1(0,1) - b_1 \end{cases}\\
&S_2(1,0) = \begin{cases} C_1(1,0) + b_2, C_1(1,0) \le O_1(1,0) \\ C_1(1,0) - b_2 \end{cases}\\
&S_3(1,1) = \begin{cases} C_1(1,1) + b_3, C(1,1) \le O_1(1,1) \\ C_1(1,1) - b_3 \end{cases}
\end{aligned}
\tag{13}
$$

Here**,** C represents the pixels of the container image, S represents the pixels of the stego-image, and b_1, b_2, b_3 are the secret information bits (Figure2).

C(0,0)	C(0,1)
C(1,0)	C(1,1)

(a) Stego-image

S(0,0)	S(0,1)
S(1,0)	S(1,1)

(b) Container image

Figure 2.

In other studies where the Hartley formula is used for secret data hiding, replacing it with the method proposed in the algorithm by converting the obtained values from the decimal system to the binary system results in a greater number of secret bits being embedded into the container image pixels. This means an increase in embedding capacity. Moreover, when comparing the original image with the stego-image, the PSNR values are high due to the minimal differences between the two images.

Information hiding algorithm based on the quorum function [3, 12]. As is known, one of the main conditions of steganography is that the visual similarity between the original image and the stego-image containing the secret information should be maximized. However, every modification made to the original image causes its visual appearance to change. As a result of these changes, the PSNR values calculated between the original image and the stego-image decrease.

Research on reconstructing the container image after extracting the secret information from the stego-image has been dedicated to many works differing in terms of PSNR and the capacity to hide more secret information. In this section, the algorithm we propose achieves better results for the aforementioned metrics (PSNR and HC) compared to existing similar algorithms.

The process of extracting secret information from the stego-image is carried out using an algorithm that is the inverse of the embedding algorithm.

To ensure the robustness of the proposed quorum function-based information hiding algorithm against stego-attacks, i.e., to guarantee security, encryption of the secret information is used.

The secret information bits are fully encrypted using the Rijndael algorithm and then embedded into the container image using the proposed algorithm. The sequence of steps for the proposed steganographic algorithm is as follows.

Embedding secret information into the container image:

Step 1. The secret information bits are encrypted using the Rijndael algorithm.

$$B = b_1, b_2 b_3, \ldots\ldots b_n$$

Step 2. The container image is divided into 2x2 blocks (Figure 3).

a_{11}	a_{12}
a_{21}	a_{22}

Figure 3. Container image

Step 3. The pixel with the lowest value is subtracted from the other three pixels.

$$\begin{aligned} c_{12} &= a_{12} - \min \\ c_{21} &= a_{21} - \min \\ c_{22} &= a_{22} - \min \end{aligned} \tag{14}$$

In the algorithm, a 3-input quorum function is used for embedding and extracting secret information. The quorum function (QF) is widely used in Boolean algebra, hash functions, and others. The quorum function is defined as follows[4]:

$$QF(x_1, x_2, \ldots\ldots x_n) = \begin{cases} 1, \sum_{i=1}^{n} x_i \geq \dfrac{n}{2}, \\ 0 \end{cases} \tag{15}$$

The quorum function is used to hide secret information in the last 3 least significant bits of the pixels of the container image c_{12}, c_{21}, c_{22}. For this purpose, it is possible to use the three-input quorum function (3QF) defined by equation (16).

$$3QF(x_1, x_2, x_3) = (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \tag{16}$$

here, $3QF(x_1, x_2, x_3)$ represents the input values of the quorum function.

[4] Sabeen G., P.V., Bindiya, M. V., Judy, M. V. A high imperceptible data hiding technique using quorum function // Multimedia tools and applications, Springer,- 2021. 80(5),- pp. 20527 –20545.

As input values, the last 3 least significant bits of the corresponding pixels of the container image are used. It is known that these values can be either 0 or 1. If the input values of the function are equal to 1, then the output value of the quorum function is also equal to 1. If the input value is 0, the output value of the quorum function will be 0. After hiding the secret information bits using the quorum function, the minimum values in the blocks are added back to the respective pixels. The procedure of hiding information using the three-input quorum function (3QF) is described in detail in the dissertation work.

In the third chapter (Development of secret information hiding algorithms using the SIFT algorithm in color images), two new algorithms are proposed:

- A large-capacity secret information hiding algorithm;
- A high visual quality-priority secret information hiding algorithm.

Large-capacity secret information hiding algorithm. In this chapter, the main goal is to ensure that the steganographic algorithms comply with quality metrics while enabling the hiding of secret information in larger volumes. To guarantee robustness, the Scale Invariant Feature Transform (SIFT) algorithm, which is scale-invariant, is used.

In the proposed secret information hiding algorithm, secret bits are embedded into the pixels selected by the SIFT algorithm in the blue channel of the container image. The SIFT algorithm is used to identify keypoint features in an image. It also possesses characteristics useful for object or scene recognition, 3D structure modeling, motion tracking, and for comparing between images.

Before starting the information hiding process, keypoint pixels in the color image are identified using the SIFT algorithm.

The chaotic embedding of secret information bits improves both the visual quality and security of the algorithm. The sequence for embedding secret bits into the keypoint pixels identified by the SIFT algorithm is as follows [6].

Step 1. Keypoint pixels are detected using the SIFT algorithm (Figure 4).

Figure 4. Original image Keypoint-detected image

Step 2. Among the detected keypoint pixels, those located in the blue channel are selected.

Step 3. Since the secret information bits are converted to the octal number system for embedding, according to the proposed algorithm, the remainder obtained by dividing the pixels determined by equation (17) by eight is calculated:

$$n = p_{i,j} \bmod 8 \tag{17}$$

here, $p_{i,j}$ is a pixel of the container image.

Step 4. The remainder value n obtained in Step 3 is converted to the binary number system $n_{10} \to n_2'$.

Step 5. The number of secret information bits selected corresponds to the total number of ones and zeros in the binary bit sequence obtained.

Step 6. The selected secret information bits are converted to the octal number system $n_2 \to d_8$

Step 7. As shown in equation (18), the pixel of the container image is added to the secret information bit in octal form:

$$S_{ij}=p_{i,j}+d_8 \tag{18}$$

here, S_{ij} is the pixel of the stego-image, and d_8 is the secret information bit converted to the octal number system.

Thus, the secret information bits are embedded into the container image. The extraction of secret information (the inverse of hiding) is provided in the dissertation text.

High visual quality-priority secret information hiding algorithm. In another variant of the above-presented algorithm, to

preserve visual quality, the remainder obtained by dividing the corresponding pixels of the blue channel by 4 is calculated. Then, this remainder is converted to the binary number system, and secret information bits are selected according to the number of bits present. Next, the selected bits are converted to the quaternary (base-4) number system and added to the corresponding pixel in the blue channel of the container image.

In this case, compared to the octal-based hiding algorithm, fewer secret bits are hidden, but compared to binary-based hiding algorithms, more secret bits are embedded. The main goal of this algorithm is to preserve the visual quality of the container image. Indeed, this algorithm achieves higher visual quality compared to the algorithm proposed in Section 3.2. The algorithm is realized through the following steps:

Step 1. Keypoint pixels are detected using the SIFT algorithm.

Step 2. Among the detected keypoint pixels, those located in the blue channel are selected.

Step 3. Since the secret information bits are intended to be embedded after converting to the quaternary number system, the remainder obtained by dividing the pixels determined by equation (19) by 4 is calculated according to the proposed algorithm:

$$n = p_{i,j} \bmod 4 \tag{19}$$

here, $p_{i,j}$ is the pixel of the container image.

Step 4. The remainder value n obtained from Step 3 is converted into the binary number system as $n_{10} \rightarrow n_2'$.

Step 5. Based on the total number of ones and zeros in the obtained binary bit sequence, a corresponding number of secret information bits are selected.

Step 6. The selected secret information bits are then converted into the quaternary number system as $n_2 \rightarrow d_4$.

Step 7. These are added to the container image pixel as shown in formula (20):

$$S_{ij} = p_{i,j} + d_4 \tag{20}$$

here, S_{ij} is the stego-image pixel, and d is the secret information bit converted into the quaternary number system.

Thus, the secret information bits are embedded into the container image.

The experimental study of the algorithms proposed in Chapter 4 is presented.

EXPERIMENTAL STUDIES

The results of experimental studies of the secret information hiding algorithm based on the Least Significant Bit (LSB) substitution method [7, 9, 11] were obtained using standard images taken from the USC-SIPI image database. These experiments were conducted in order to verify the accuracy of the theoretical research. The experiments were carried out in the MATLAB/R2023b programming environment.

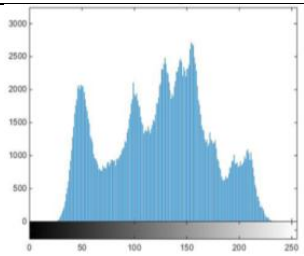
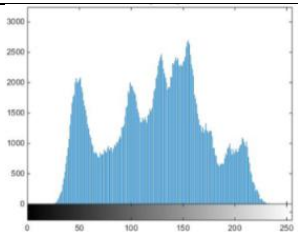
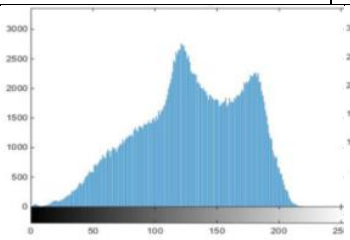
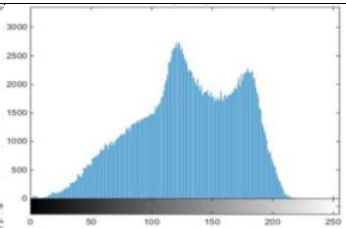
To evaluate the quality of the stego-image, the PSNR (Peak Signal-to-Noise Ratio) value is calculated in the usual manner. The obtained result determines the degree of similarity between the container image and the stego-image. The PSNR value is directly related to the visual quality of the stego-image: the higher this value, the greater the similarity between the compared images. Examples of the compared images are presented in Table 1.

Table 1. Compared Images

Images	Original Images	Stego-Images
Lena		
Baboon		

Table 2 presents the histograms of the original images and their corresponding stego-images. As can be seen from the table, the histograms of the compared images are almost indistinguishable from one another. This indicates that the compared images are highly identical, making it difficult to detect the presence of hidden information transmitted over an open communication channel.

Table 2. Histograms of the Compared Images

Images	Original Images	Stego-Images
Lena		
Baboon		

The PSNR values between the container and the stego-image have been compared with the metrics presented by various authors in recent scientific literature. The same test images were used for comparison. The results of the experiments are presented in Table 3.

From the figures shown in the table, it is evident that the proposed algorithm achieves relatively higher PSNR values and allows for embedding a larger amount of secret information compared to the other algorithms.

For each image, the PSNR exceeds 36 dB, which means that the inevitable distortions caused by embedding information into the container image are imperceptible to the human eye.
In addition to PSNR, the graphical histogram method was also used to obtain more accurate results.

Figure 5 presents a diagram based on **Table 3**. The diagram illustrates the difference between the PSNR values of the proposed algorithm and those presented in other studies, as well as their dependence on different images.

The robustness of the proposed algorithm has been evaluated not only through histogram steganalysis but also more extensively using the RS steganalysis method.

For this purpose, RS steganalysis was first applied to four empty container images (Lena**,** Baboon**,** Airplane**,** and Peppers), and the results are presented in Table 4**.**

Table 3. Comparison of Stego-Image Quality Indicators

Input Images	**Quality Metrics**	**Malik A., Sikka G.**[5] .	**Wahed M.A., Nyeem, H**[6]	**Ahmad A.M**[2]**.,**	**Yong-qing C.**[7]	**Jana B., Giri D.,**[8]	**Propo-sed algo-rithm**
Lena	HC (bit) PSNR (dB)	177777 31,67	198902 31,14	224528 33,60	226085 33,27	223031 38,25	240962 51,73

[5] Malik, A. Sikka, G., Verm, H.K. Image interpolation based high capacity reversible data hiding scheme//Multimedia Tools Application,- 2018. №76,- p. 2454-7190.
[6] Wahed, M.A. Nyeem, H. Reversible data hiding with interpolation and adaptive embedding // Multimedia Tools and Applications,- 2019. 78(3),-p.10795-10819.
[7] Chen, Y., An efficient general data hiding scheme based on image interpolation / W. Sun, L. Li, X. Chang, C. Wang, // Journal of Information Security and Applications, - 2020. № 54,- p. 271–350**.**
[8] Jana, B. Giri, D. Mondal, S. K. Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation// Computational Intelligence in Data Mining, Springer,- 2015. №2, -p. 239-248.

Baboon	HC (bit) PSNR (dB)	262272 22,57	125562 22,29	259737 28,77	231401 23,70	273235 35,85	277492 50,62
Airplane	HC (bit) PSNR (dB)	185676 30,01	179961 29,66	228863 31,67	213460 31,43	211321 42,34	208392 52,74
Peppers	HC (bit) PSNR (dB)	175669 29,78	195490 29,78	223295 33,18	227493 31,13	232563 35,12	247864 51,53
Average Values	HC (bit) PSNR (dB)	**200348** **28,50**	**189978** **28,22**	**234106** **31,8**	**224609** **29,88**	**235037** **37,89**	**243677** **51,65**

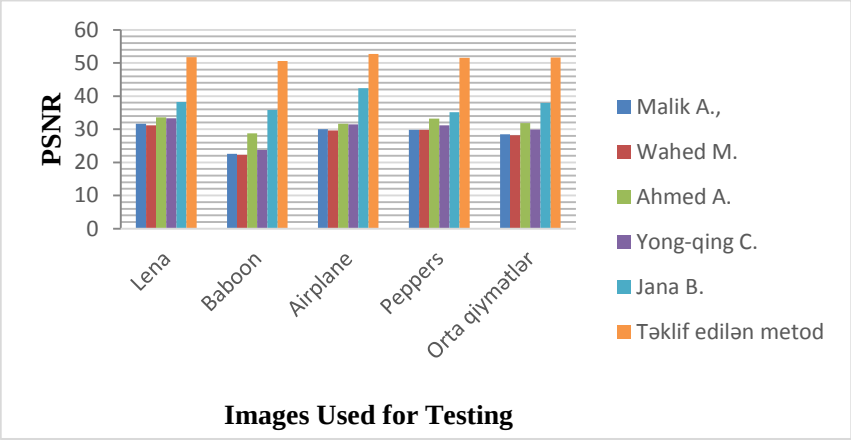


Figure 5. Dependence of PSNR Values on Different Images

Table 4. Results of RS Steganalysis on container images

Container Image	$\lvert R_m - R_{-m}\rvert$ (dB)	$\lvert S_m - S_{-m}\rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067

Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

After embedding secret information bits of various sizes into the container image (in this case, the container image becomes a stego-image), the values of $|R_m - R_{-m}|$ and $|S_m - S_{-m}|$ were calculated, and the results are presented in Table 5**.**

Table 5. Results of RS Steganalysis on Stego-Images

Stego-Image	**RS Steganalysis**	**Embedded Secret Information Size (bytes)**			
		1000	5000	10000	15000
Lena	$\|R_m - R_{-m}\|$ (dB)	0,0080	0,0087	0,0093	0,0099
	$\|S_m - S_{-m}\|$ (dB)	0,0091	0,0095	0,0097	0,0099
Baboon	$\|R_m - R_{-m}\|$ (dB)	0,0064	0,0079	0,0093	0,0752
	$\|S_m - S_{-m}\|$ (dB)	0,0073	0,0163	0,0231	0,0243
Airplane	$\|R_m - R_{-m}\|$ (dB)	0,0093	0,0095	0,0099	0,0103
	$\|S_m - S_{-m}\|$ (dB)	0,0082	0,0086	0,0205	0,0216
Peppers	$\|R_m - R_{-m}\|$ (dB)	0,0097	0,0098	0,0100	0,0109
	$\|S_m - S_{-m}\|$ (dB)	0,0085	0,0085	0,0092	0,0098

In the table above, the fact that the difference between the $|R_m - R_{-m}|$ and $|S_m - S_{-m}|$ values obtained from the RS steganalysis results is close to zero confirms the robustness of the algorithm.

The experiments of the steganographic data hiding algorithm based on image interpolation [7, 10, 11] were conducted using standard 512×512-sized images. These images were used as input images to evaluate the effectiveness of the proposed information hiding algorithm.

The experiments were carried out on the same set of images used in four successful algorithms previously proposed in the literature. Each image was processed according to the algorithm proposed in this dissertation.

Let us first examine the amount of secret information that can be embedded using the new algorithm. The experimental results comparing the performance of the proposed algorithm with other algorithms are presented in Figure 6.

Here, based on the diagrams, the values of the interpolated container image pixels in the interval 1 to 7 and the corresponding number of secret information bits that can be embedded in those pixels are shown

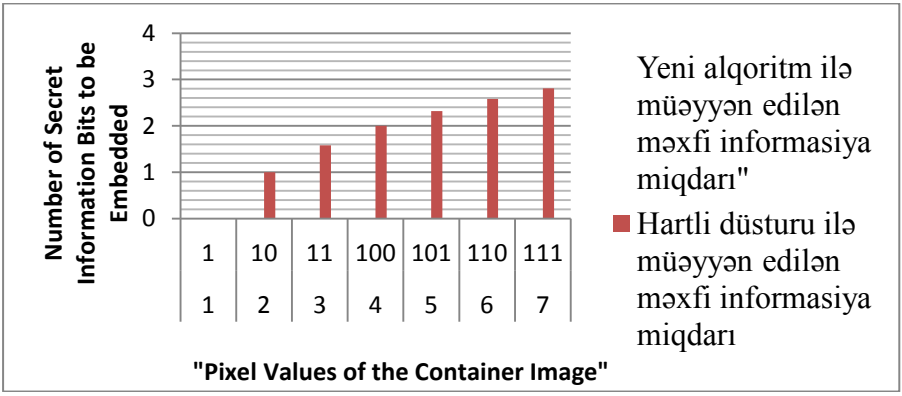


Figure 6. Comparison of secret information bit embedding at

Pixel Values in the 1–7 Range of the Container Image.

As shown in Figure 6, the number of secret bits embedded at pixel values within the 1–7 range of the container image is higher, regardless of the specific pixel value.

To evaluate the effectiveness of the proposed algorithm, its experimental results were compared with those of algorithms published in recent years. The aim of the proposed new algorithm is to achieve the embedding of a larger volume of secret information in standard reference images with minimal distortion.

The comparative results of the experiments are presented in Table 6. As can be seen from the table, while the embedding capacity of the proposed algorithm is approximately similar to that of the other algorithms, it ensures significantly higher visual quality. The ability to maintain high visual quality even after embedding a large amount of secret information is considered a key advantage of the proposed algorithm.

The experimental images are fully provided in the dissertation. At the same time, the secret information embedding procedure is implemented in a simple manner, with no noticeable computational complexity. Regardless of the image type, the PSNR value exceeds 50 dB.

It is clearly shown in Table 6 that the proposed algorithm outperforms the others in terms of performance metrics and paves the way for embedding even larger volumes of secret information in future research.

The obtained PSNR values are also supported by the histogram steganalysis method. The histograms and the comparative table of stego-image quality metrics are provided in the dissertation.

Table 6. Comparison of stego-image quality indicators

Input Images	**Quality Metrics**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9].,**	**Proposed algorithm**
Lena	HC (bit) PSNR	226085 33,27	177777 31,67	223031 38,25	564744 39,56

	(dB)				
Baboon	HC (bit) PSNR (dB)	231401 23,70	262272 22,57	273235 35,85	676791 36,47
Airplane	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	524719 35,88
Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	656611 39,32
Sailboat	HC (bit) PSNR (dB)	364589 31,80	175183 29,04	236132 29,03	378123 33,36
Boat	HC (bit) PSNR (dB)	343589 29,82	124236 32,22	295325 31,26	369563 35,93
Couple	HC (bit) PSNR (dB)	381589 26,82	354137 24,36	378256 23,48	400021 29,68
House	HC (bit) PSNR (dB)	236589 32,02	235325 31,32	217482 33,27	282753 36,21
Average Values	**HC (bit) PSNR (dB)**	**278099 29,99**	**211284 28,87**	**258418 33,575**	**481666 35,80**

To more accurately evaluate the robustness of the proposed algorithm, RS steganalysis was used in addition to histogram steganalysis. The results of the RS steganalysis are presented in Tables 7 and 8. As before, RS steganalysis was first applied to the unmodified (empty) container images. The results of this analysis are shown in Table 7.

Table 7. Results of RS steganalysis on container images

Container Image	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

As can be seen, the RS indicators in each image are slightly above zero and very close to one another. This, in turn, is a key factor contributing to the robustness of the algorithm.

Subsequently, after embedding secret information bits of varying sizes into the container image using the corresponding algorithm, RS steganalysis was applied to test the robustness. The results of the steganalysis are presented in Table 8.

Experiments on the information hiding algorithm based on the quorum function [3, 7, 11, 12] were conducted using 512x512 images taken from an image database. To evaluate the effectiveness of the proposed new algorithm and obtain accurate results, tests were performed on various successful algorithms using 50 standard reference images. The images are provided in the dissertation and its appendix

Table 8. Results of rs steganalysis on stego-images

Stego-Image	**RS Steganalysis**	**Embedded Secret Information Size (bytes)**			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m} \rvert$ (dB)	0,0080	0,0087	0,0093	0,0099
	$\lvert S_m - S_{-m} \rvert$ (dB)	0,0091	0,0095	0,0097	0,0099
Baboon	$\lvert R_m - R_{-m} \rvert$	0,0064	0,0079	0,0093	0,0752

	(dB)				
	$\lvert S_m - S_{-m} \rvert$ (dB)	0,0073	0,0163	0,0231	0,0243
Airplane	$\lvert R_m - R_{-m} \rvert$ (dB)	0,0093	0,0095	0,0099	0,0103
	$\lvert S_m - S_{-m} \rvert$ (dB)	0,0082	0,0086	0,0205	0,0216
Peppers	$\lvert R_m - R_{-m} \rvert$ (dB)	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m} \rvert$ (dB)	0,0085	0,0085	0,0092	0,0098

The reference images were used as input images for the proposed algorithm. To verify the accuracy of the obtained results, the tests were conducted using methods employed by the compared algorithms. At the same time, each image was also tested based on the proposed algorithm.

For comparison, recent successful research works in this field were selected.

The experimental results are presented in Table 9. As seen from the table, our proposed algorithm demonstrates higher values for both indicators. This, in turn, confirms the superiority of the proposed algorithm.

The main objective of the applied secret information hiding algorithm is to embed a larger volume of secret bits in the stego-image while minimizing distortions using the new algorithm. As shown in Table 5, this goal has been achieved.

In addition to the PSNR values, the images were also tested using the histogram method. The histograms are provided in the dissertation. From the given histograms, it can be observed that the difference between the input images and the stego-images is negligibly small.

Table 9. Comparative table of stego-image quality metrics

Input Images	**Quality Metrics**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9].,**	**Sabeen G[4].**	**Proposed algorithm**
Lena	HC (bit) PSNR (dB)	226085 33,27	177777 31,67	223031 38,25	303318 48,01	301465 49,56
Baboon	HC (bit) PSNR (dB)	231401 23,70	262272 22,57	273235 35,85	191365 48,21	283115 50,47
Airplane	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	112721 46,05	256982 48,88
Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	296993 47,69	393216 49,32
Orta qiy-mət	**HC (bit) PSNR (dB)**	**224610 29,88**	**200349 28,50**	**235038 37,89**	**226099 47,49**	**308695 49,55**

To verify the robustness of this algorithm, RS steganalysis was used alongside histogram steganalysis. As with the previous algorithms, RS steganalysis was first applied to the empty containers, and the results are presented in Table 10.

Table 10. RS Steganalysis of container images

Container Image	$\lvert R_m - R_{-m} \rvert$ (dB)	$\lvert S_m - S_{-m} \rvert$ (dB)
Lena	0,0078	0,0088
Baboon	0,0057	0,0067
Airplane	0,0063	0,0065
Peppers	0,0093	0,0083

Subsequently, according to the algorithm's procedures, secret information of varying sizes was embedded into the container image using the proposed algorithm, and the corresponding PSNR values and embedding capacities for the stego-images were recorded. The experimental results are presented in Table 11.

Analysis of the experimental data shows that during the embedding of secret information in varying amounts, the RS statistic values vary within a very small range and do not exceed the threshold

for high robustness. Therefore, if information is hidden using the proposed algorithm, the stego-system remains fully protected from malicious attacks during transmission over an open communication channel.

Table 11. Results of RS steganalysis on stego-images

Stego-Image	RS Steganalysis	Embedded secret information size (bytes)			
		1000	5000	10000	15000
Lena	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0086	0,0087	0,0103	0,0108
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0095	0,0098	0,0098	0,0099
Baboon	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0074	0,0083	0,0097	0,0752
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0077	0,0083	0,0094	0,0099
Airplane	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0086	0,0089	0,0095	0,0097
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0084	0,0089	0,0095	0,0099
Peppers	$\lvert R_m - R_{-m}\rvert$ (dB)	0,0097	0,0098	0,0100	0,0109
	$\lvert S_m - S_{-m}\rvert$ (dB)	0,0090	0,0094	0,0098	0,0100

Experimental Study of Secret Information Hiding Algorithms Using the SIFT Algorithm in Color Images

To ensure the accuracy of the experiments, the same standard color images used in the compared algorithms were examined. In this algorithm, secret information bits are hidden in the pixels selected by the SIFT algorithm in the blue channel of the color image. During the

experiments, it was observed that the secret information bits were not distorted.

After testing various types of attacks, it can be concluded that the use of the SIFT algorithm in the proposed method provides robustness against these kinds of attacks. The proposed algorithms were also tested using the analysis methods presented in the following section.

PSNR was used to measure the visual quality.

A comparison of the proposed algorithm with other existing algorithms is given in Table 12. The indicators of the tested images, i.e., the PSNR difference values between the container image and the stego-image, as well as the comparison of PSNR and the capacity of secret information bits (HC) embedded in the stego-image by the proposed algorithm with recently developed methods, are shown.

Table 12. Comparison of quality metrics for stego-images

Input Images	**Quality Metrics**	**Yong-qing C.[8]**	**Malik A., Sikka G[6].**	**Jana B., Giri D[9].,**	**Proposed algo-rithm**	
					IV algo-rithm [7]	**V algo-rithm [7]**
Lena	HC (bit) PSNR (dB)	226085 33,27	177777 31,67	223031 38,25	464744 41,03	398562 43,23
Baboon	HC (bit) PSNR (dB)	231401 23,70	262272 22,57	273235 35,85	663791 40,43	593652 45,32
Barbara	HC (bit) PSNR (dB)	213460 31,43	185676 30,01	211321 42,34	423719 43,08	412356 48,03

Peppers	HC (bit) PSNR (dB)	227493 31,13	175669 29,78	232563 35,12	399511 39,32	386592 42,02
Orta qiymət -lər	**HC (bit) PSNR (dB)**	**224609 29,88**	**200348 28,50**	**235037 37,89**	**487941 40,96**	**447791 44,65**

Note: Algorithm IV – High-capacity secret information hiding algorithm;

Algorithm V – Secret information hiding algorithm with high visual quality priority.

As can be seen from the table, the proposed algorithms achieve higher similarity values (PSNR) between the container image and the stego-image even when embedding a larger volume of secret information bits compared to the other algorithms.

The ability to maintain a high degree of similarity between the container and stego-image after embedding a large amount of secret data is considered a significant advantage of the proposed algorithms.

In addition to PSNR values, histogram steganalysis is used to more accurately assess the similarity between the input and stego images, and to evaluate the robustness of the algorithms. Histogram steganalysis was conducted on both the reference and stego-images. The histograms confirm the effectiveness of the stego-images and reveal no significant changes when compared to the container image histograms.

To verify the robustness of the proposed algorithms, RS steganalysis was also applied in addition to the steganalysis methods presented above.

In each image, RS indicator values were found to be less than zero and very close to each other, which is a key factor indicating high robustness of the algorithm.

After embedding secret information bits of varying sizes into the container image using the respective algorithms, RS steganalysis was applied to test the robustness.

The results of this steganalysis are presented in Tables 4.4.2 and 4.4.3 of the dissertation.

The results show that increasing the volume of hidden information does not affect the robustness of the proposed algorithms. Since the secret information is imperceptible, it can be transmitted through an open communication channel. The execution time of each proposed algorithm has also been tested and confirmed to be shorter than that of other algorithms.

CONCLUSION

During the research conducted within the framework of the dissertation topic, the set objectives were achieved, and the following results were obtained:

- A comprehensive review of information hiding algorithms proposed in foreign scientific literature on image steganography was carried out [1, 2, 7, 8, 11, 13]. Based on this review, the current level of development of the subject was analyzed, and the key problems to be addressed in the dissertation were identified [7, 11, 13]. Among the recent studies in the field of image steganography, algorithms with high performance and those similar to the dissertation topic were selected as examples and thoroughly investigated [4, 7].
- A steganographic algorithm was developed that prioritizes the visual quality of the image**,** ensure**s** high robustness against stego-attacks, and enables embedding large volumes of secret information [8, 9].
- An interpolation-based steganographic algorithm was designed to allow the container image to be reconstructed without any distortion [10].
- A steganographic algorithm based on a three-input quorum function with high performance was developed [3, 12].
- To ensure high robustness of the algorithm, the AES encryption standard was applied [3].
- Two new effective algorithms were proposed for hiding secret information in keypoint pixels of color images (RGB color scheme) using the SIFT algorithm [6, 11].

THE FOLLOWING SCIENTIFIC WORKS HAVE BEEN PUBLISHED ON THE DISSERTATION MATERIALS:

1. Verdiyev, S.Q., Nağıyeva, A.F. Kompüter Steqanoqrafiyası və onun əsas prinsipləri // **Proqram mühəndisliyinin aktual elmi-praktiki problemləri üzrə I respublika konfransı**, - Bakı: İnformasiya Texnologiyaları, – 17 may 2017, – s. 79-81.

2. Вердиев, С.Г., Нагиева, А.Ф., Гусейнов З.Н. Симметричное (одноключевое) шифрование данных при защите информации в компьютерных сетях // **VII Международная научная конференция** Технические науки в России и за рубежом, – Москва: Издательский дом Буки-Веди, – 20–23 ноября, – 2017, –с. 5-7.

3. Вердиев, С.Г., Нагиева, А.Ф. О возможностях использования стандарта AES в Корпоративных сетях для защиты информации // Самара: **Инфокоммуникационные технологии**, – 2017. № 4.– с. 366-370.

4. Verdiyev, S.Q., Nağıyeva, A.F. İnformasiyanın steqanoqrafik gizlədilməsi proseduralarının eksperimental analizi // **İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi - praktik seminarının əsərləri**, – Bakı: İnformasiya Texnologiyaları,– 8 dekabr, – 2017, – s. 51-56.

5. Алмадатова, А.Ф., Вердиев, С.Г., Нагиева, А.Ф. Защита информации криптографическим методом разделения секрета // **VII Международная научно-техническая и научно-методическая конференция** Актуальные проблемы инфотелекоммуникаций в науке и образовании, – Санкт-Петербург: – 28 февраля-1 марта, – 2018, – с. 29-33.

6. Nağıyeva, A.F., Verdiyev, S.Q. Rəqəmli təsvirlərin watershed üsulu ilə seqmentləşdirilməsi // **İnformasiya təhlükəsizliyinin aktual multi-dissiplinar elmi-praktiki problemləri**, – Bakı: İnformasiya Texnologiyaları, – 14 dekabr, – 2018, – s. 53-58.

7. Verdiyev, S.Q., Nağıyeva, A. F., Hüseynova R. Y., Hüseynov Z. N. Steqoanaliz üsullarının icmalı // **İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri V respublika konfransı**, – Bakı: İnformasiya Texnologiyaları, – 29 noyabr, – 2019, – s. 204-206.

8. Verdiyev, S.G., Naghiyeva, A.F. A brief overview of data hiding

methods in digital images // – Самара: **Инфокоммуникационные технологии**, – 2020, vol. 18, No. 4, – c. 427-437.
9. Naghiyeva, A.F., Akbarzadeh, K., Verdiyev, S.G. New steganography method of reversible data hiding with priority to visual quality of image // **IEEE II International Conferance on Advances in computing, communication, embedding and secure systems,** – India: – 2-4 september, – 2021, – p. 329-333. (Scopus)
10. Нагиева, А.Ф., Вердиев, С.Г. Реверсивный стеганографический метод сокрытия информации основанный на интерполяции изображений // – Москва: **Компьютерная оптика**, – 2022. Том 46, № 3,– c. 465-472. (Scopus)
11. Verdiyev, S.G., Naghiyeva, A.F., Ajay, K. Experimental study of a novel technique of data hiding with high PSNR // **IEEE III International Conferance on Advances in Computing Communication, Embedding and Secure Systems,** – India: – 18-20 may, – 2023, – p. 77-80. (Scopus)
12. Nağıyeva, A.F. Məxfi informasiyanın ötürülməsində informasiya gizlədilmə metodu // – Bakı: **Elmi əsərlər**, Azərbaycan Texniki Universiteti, - 2023. № 2,– s. 60-66.
13. Nağıyeva, A.F., İnformasiya təhlükəsizliyində steqanoqrafik metodlar // **Elmi xəbərlər məcmuəsi**, Azərbaycan Texnologiya Universiteti, – 2023. № 4, – s. 98-104.

The Applicant's Personal Contribution in Co-Authored Publications

[1] – The application problems of methods and tools for computer steganography and the formation of covert information transmission channels in stegosystems were examined. Their practical limitations were identified, and a comprehensive analysis of advantages and shortcomings was carried out.
[2] – Methods and tools for the protection of confidential information transmitted over open communication channels through symmetric encryption were investigated. Implementation challenges were discussed, and the results were presented, including a comparative analysis of advantages and disadvantages.
[3] – The iterative sequence of the encryption process implemented within a state institution was described. Additionally, an encryption

example was demonstrated using a plaintext document employed in postal communication and the Advanced Encryption Standard (AES).
[4] – A systematic review and experimental evaluation of existing steganographic methods were performed. The strengths and weaknesses of each method were analyzed individually. Furthermore, a methodological framework for the information hiding procedure within the MATLAB environment was developed.
[5] – Approaches for embedding and transmitting confidential information within various multimedia files were elaborated.
[6] – In order to enhance the effectiveness of images as steganographic containers, segmentation—an image processing technique—was employed. Specifically, the characteristics of the watershed method and its implementation in MATLAB were presented. As an illustrative case, segmentation of a color digital image using the gradient method was carried out, confirming the applicability of segmentation techniques in color image processing.
[7] – To ensure the security of digital container images during circulation in open networks, an overview and analytical study of steganographic methods and their counter-techniques—steganalysis—were undertaken, and a concrete example was provided.
[8] – Based on recent research, a detailed classification of steganographic methods was proposed. Widely applied approaches in image steganography were examined, with emphasis on their advantages and disadvantages. Various data-hiding strategies were discussed, and the outcomes were systematized. Stegoanalytic techniques for calculating statistical differences between original and stego-images were studied, and corresponding results were presented.
[9] – A novel steganographic algorithm based on the Least Significant Bit (LSB) method was designed, achieving higher efficiency in concealing confidential information.
[10] – The problem of developing a new steganographic method for data embedding based on image interpolation was formulated and solved. A technique was proposed that ensures increased embedding capacity, robustness, and preservation of the visual quality of the stego-image.
[11] – An experimental investigation of the robustness of various developed steganographic methods aimed at ensuring the protection of

confidential information was conducted. The reliability of the algorithm against stegoanalytic attacks was verified through the RS steganalysis method. Moreover, the computational complexity of the algorithm was analyzed, and the obtained results were presented.

The defense of the dissertation will be held on _____, 2025, at _____ at the meeting of the ED1.35 Dissertation Council operating under the Institute of Information Technology of the Ministry of Science and Education of Azerbaijan.

Address: AZ 1141, Baku city, B. Vahabzade Street, 9a

It is possible to review the dissertation at the library of the Institute of Information Technology of the Ministry of Science and Education of Azerbaijan.

The electronic versions of the dissertation and the author's abstract have been made available on the official website of the Institute of Information Technology of the Ministry of Science and Education of Azerbaijan.

The author's abstract was sent to the required addresses on _____, 2025.

Signed for print
Paper format
Volume
Print run