Image Steganography Method using LSB and AES Encryption Algorithm*

Tamara Radivilova[1,*,†], Ihor Dobrynin[1,†], Arkadii Snihurov[1,†], Svitlana Stanhei[1,†] and Serhii Bulba[2,†]

[1] *Kharkiv National University of Radio Electronics, 14 Nauky ave., 61166 Kharkiv, Ukraine*
[2] *State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine*

Abstract

In today's world, data security is a key issue in many industries. Cryptography ensures data confidentiality, while steganography is used to conceal information transmitted over unsecured communication channels. This paper proposes methods based on a combination of the fast LSB steganography algorithm and the AES symmetric encryption algorithm to protect images. The proposed methods include shifting from the beginning of the container to increase the security of encrypted data and protect against image cropping. Also, algorithms are proposed to increase the amount of information transmitted with data recording in the last 2 bits of the blue pixel channel and data recording in each pixel channel in the last bit. The following concealment indicators were used for the analysis: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Normalized Cross-Correlation (NCC). The study yielded results suggesting that the fastest algorithm for steganography and encryption is a modification with the insertion of two characters into the last bit of the blue pixel channel (LSB+AES-os+2bit). The slowest algorithm is the modification using AES encryption and a shift from the beginning of the steganocontainer (LSB+AES-os). In the case of decoding, modifications using AES encryption and a change from the start of the steganographic container (LSB+AES-os) show almost identical results and are the fastest when decoding messages. The slowest algorithm is the one with message embedding in all three channels in the last bit (LSB+AES-os+3ch), but it should be noted that it is the most complex and includes all other modifications of the LSB algorithm. Increasing the amount of data embedded in the container negatively affects the display statistics. Still, this effect does not reduce the metrics of standard indicators, which are sufficient for steganography. The number of bits suitable for embedding depends on the source file and linearly on the number of LSB bits used for encoding. The number of bits ideal for encoding also depends on the shift percentage. The message embedding is not visually noticeable when using any developed methods. Experimental results demonstrate that the proposed algorithms effectively protect data with a high peak signal-to-noise ratio (PSNR) and low mean square error (MSE), ensuring high image quality and reliable encryption and decryption of information. Depending on the reliability requirements of the steganographic system, the presented methods can be varied, thereby changing the maximum amount of hidden information.

Keywords

AES, LSB, steganography, encryption, decryption, peak signal-to-noise ratio, structural similarity index measure, normalised cross-correlation

1. Introduction

A comprehensive modern information security system cannot be implemented using only one information security method [1, 2]. Ensuring data confidentiality is a pressing issue, as there are many attacks aimed at violating data confidentiality [3–5]. Therefore, scientists and professionals are developing new and improving existing methods for ensuring data confidentiality and information security [6–8].

* *CQPC 2025: Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
tamara.radivilova@nure.ua (T. Radivilova); ihor.dobrynin@nure.ua (I. Dobrynin); arkadii.snihurov@nure.ua (A. Snihurov); svitlana.shtanhei@nure.ua (S. Stanhei); s.bulba@knute.edu.ua (S. Bulba)
0000-0001-5975-0269 (T. Radivilova); 0000-0001-8910-2609 (I. Dobrynin); 0000-0003-1355-7978 (A. Snihurov); 0000-0002-9200-3959 (S. Stanhei); 0009-0004-5330-2632 (S. Bulba)

Modern steganography hides the fact that data is being transferred by using a masking algorithm that modifies a specific array of open data, adding a confidential message to it. There are many methods and techniques of steganography, varying in computational complexity, capacity, and targeting different data formats. Today, steganography is used for covert communication, image copyright protection (authentication), fingerprinting (intruder tracking), adding captions to images, adding additional information such as subtitles to videos, protecting image integrity (detecting fraud), copy control in DVD recording and smart browsers, and automatically providing copyright information [9–11].

In cryptography, mathematical transformations are used to ensure data confidentiality, thanks to which data takes on a confused form [12, 13]. In steganography, secret messages are embedded in images or multimedia files during their invisible transmission via open communication channels [14]. Steganography hides confidential data and the connection between the sender and the recipient, while cryptography hides confidential data and identifies the sender and recipient [15, 16]. An effective and one of the most popular approaches is to combine cryptographic and steganographic methods to protect information from unauthorized access [17, 18].

The synergistic combination of AES encryption and LSB steganography provides a powerful two-layer security mechanism [18]. In this hybrid approach, secret data is first encrypted using a reliable AES algorithm, which guarantees its confidentiality even if detected. This encrypted data is then hidden in an image using the LSB steganography method, concealing its existence [19]. This combined strategy significantly increases the overall security, confidentiality, and integrity of the transmitted information, making it resistant to detection and decryption by unauthorized persons.

Recent research and publications analysis. Recent research indicates a significant interest in combining steganography and cryptography [20, 21]. Many scientific works are devoted to combining the AES cryptographic method and the LSB steganographic method [22], as they are the fastest and have a low level of distortion. However, further research has consistently introduced additional levels of complexity and complementary techniques. This includes using compression algorithms such as Deflate or Discrete Wavelet Transform (DWT) to reduce the size of the secret message, thereby increasing the efficiency or capacity of embedding [12, 23]. In addition, randomization techniques such as random pixel selection and random shuffling are widely used to make embedding locations less predictable, significantly improving protection against statistical steganalysis [23–26]. In [27], the authors propose a combination of LSB and RSA and Caesar encryption. However, these methods do not allow changing the amount of confidential information embedded.

In [28], the primary methodology involves embedding LSB in combination with AES encryption. Options for integrating RSA with LSB and AES are also explored, and these hybrid approaches are compared with the Pixel Locator Sequence (PLS) method. In [29], the authors proposed a technique that uses LSB matching for data embedding, and in the previous stage, AES encryption is used to provide a two-layer security architecture. The novelty lies in using mosaic images as a cover medium, which inherently supports higher embedding capabilities and reduces visual distortion. However, the operating time of these systems is quite long.

The approach developed by the authors [30] involves encrypting the target image using AES and then hiding the target text data inside the encrypted AES image using the LSB method, further enhancing data security and potentially simplifying key management by eliminating the need for direct key exchange. However, the amount of embedded information is reduced, and the processing time of this approach is quite long.

Integrating error correction codes like Reed-Solomon demonstrates a desire to ensure message recovery even if the steganographic image data is damaged during transmission or storage [25]. The methodology proposed by the authors includes Fernet encryption (AES-128 CBC), Reed-Solomon encoding for error correction, and LSB steganography for embedding. This multifaceted approach aims to improve security and robustness and achieves a high data payload of 3 bits per pixel for RGB images without noticeable distortion. However, the runtime of this system is quite long.

Thus, there is a pressing need to develop steganography and encryption methods with the ability to select a process depending on the amount of information to be hidden and the reliability requirements of the steganographic system.

The purpose of the paper. This work aims to develop and analyze data hiding methods based on steganographic and cryptographic encryption algorithms to ensure data confidentiality and integrity. To achieve this goal, the following tasks need to be solved:

1. Develop secure and effective methods for hiding confidential data in images with minimal changes to the quality of the steganographic images.
2. Develop solutions for encrypting hidden messages using the Advanced Encryption System (AES) and integrate it with Least Significant Bits (LSB) steganography to protect the content of secret messages from disclosure.
3. Ensure data integrity and confidentiality by preventing unauthorized access.
4. Minimize visual distortions in the steganographic image while maximizing embeddability.
5. Make the steganographic process resistant to visual attacks that could lead to the detection of hidden messages.

These tasks aim to create methods of steganographic information protection to select one of them depending on the amount of information to be hidden and the reliability requirements of the steganographic system.

2. Methodology

2.1. Least significant bit replacement method

A set of characteristics is used to analyze and subsequently select steganographic algorithms [31], including:

- Bandwidth is the number of bits of the hidden message that can be transmitted using this method in an image of a fixed size.
- Robustness is the ability to extract hidden information after general image processing operations: linear and non-linear filters, lossy compression, contrast adjustment, recoloring, resampling, scaling, rotation, noise addition, cropping, printing/copying/scanning, pixel rearrangement in a small neighborhood, color quantization, etc.
- Invisibility is perceptual transparency, a concept based on the properties of the human visual or auditory systems.
- Security is embedded information that cannot be removed by targeted attacks based on a known embedding and extraction algorithm and knowledge of at least one medium with a hidden message.
- The complexity of embedding and detection is the number of standard operations that will be performed to embed and detect a hidden message.

According to most of the above characteristics, the Least Significant Bits (LSB) replacement method is the most common among replacement methods in the spatial domain. The general principle of these methods is to replace the redundancy, the insignificant part of the image, with bits of the secret message, i.e., to hide information by replacing the last bits of the image that encode color with bits of the hidden message [22]. The principle of information hiding is to convert text into a byte sequence. The difference between empty and filled containers should not be noticeable to human vision and entropy analysis systems. To extract the message, you must know the algorithm to place the hidden information in the container. The popularity of this method is due to its simplicity and the fact that it allows you to hide relatively large amounts of information in relatively small files. The NZB method has low steganographic resistance to passive and active attacks. Its primary disadvantage is its high sensitivity to the slightest changes in the container. Noise-resistant encoding is often used to reduce this sensitivity.

In BMP format, an image is stored as a matrix of color values, with an image stored for each point. If each component of the RGB space (also called color channels) is stored in one byte, it can

take values from 0 to 255 inclusive, corresponding to 24-bit color depth. The peculiarity of human vision is that it poorly distinguishes between slight color variations. For 24-bit color, a change in each of the three channels of the least significant bit (i.e., the rightmost bit) results in a change of less than 1% in the intensity of a given point, allowing them to be changed imperceptibly to the eye at will.

Let's calculate the throughput of the method. Suppose we discard the service information at the beginning of the file, which is insignificant in relation to the image size. In that case, we can transmit a message that is 1/8 the size of the container or 1/4 the size of the container (when using the last 2 bits in bytes, respectively).

The principle of the LSB steganographic method is as follows.

Let there be a 24-bit grayscale image. Each pixel is encoded with 3 bytes containing the RGB channel values. By changing the least significant bit, we change the value of the byte to one. Such gradations are invisible to the human eye and may not be displayed at all when using low-quality output devices.

The example below (Fig. 1) shows how a message can be hidden in the first eight bytes corresponding to three pixels in a 24-bit image.

```
Pixels: (00100111 11101001 11001000)
        (00100111 11001000 11101001)
        (11001000 00100111 11101001)
A: 01000001
Result: (00100110 11101001 11001000)
        (00100110 11001000 11101000)
        (11001000 00100111 11101001)
```

Figure 1: Example of message hiding using the LSB method

In the example, only the three bits that were changed are highlighted. Using the LSB steganographic method requires, on average, that only half of the bits in the container image be changed.

A slight modification of this steganographic technique allows two or more of the least significant bits per byte to be used to embed a message. This increases the amount of hidden information in the container object, but the concealment is significantly reduced, making it easier to detect the steganography. Other variations of this method include levelling statistical changes in the image. Some intelligent software for detecting steganography checks areas with a single solid color. Modifications to these pixels should be avoided to improve concealment.

To improve the performance of the LSB steganography algorithm, the following should be done:

- Throughput is developing an algorithm with double and triple capacity relative to standard performance indicators.
- Invisibility is developing a distortion analyzer to select the best algorithm.
- Security integrates the Advanced Encryption System (AES) symmetric information encryption module.
- The algorithm modifies detection complexity to scramble unused image space in the invisible spectrum.

Let us consider modifications of the LSB steganographic algorithm.

To ensure the security of the LSB steganographic algorithm, we will add an algorithm for encrypting embedded messages using the AES encryption algorithm, the general scheme of which is shown in Fig. 2.

The AES algorithm, or Rijndael, is a symmetric block cipher that encrypts messages in 128-bit blocks and uses a 128/192/256-bit key.

Encryption with a secret key is used to maintain data confidentiality. This method can be used for authentication and data integrity. The work uses an encryption algorithm with a key length of 256 bits.

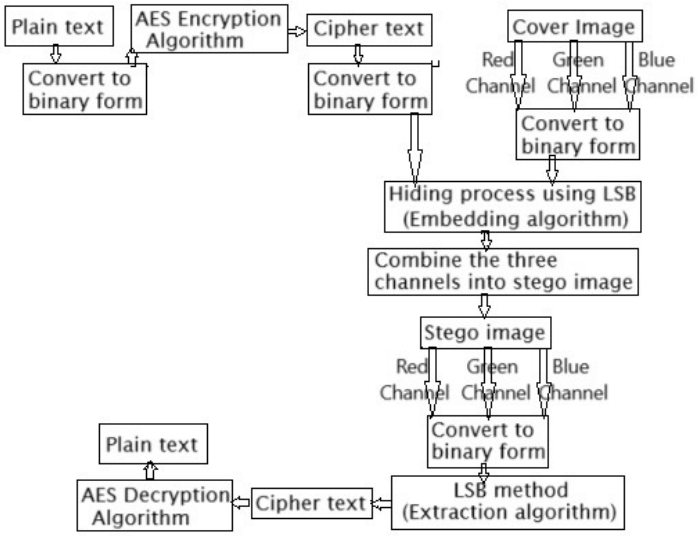

Figure 2: General diagram of the LSB steganographic algorithm combined with the AES encryption algorithm.

Not only was AES encoding used, but there was also a change in the message end search algorithm. Previously, it was searched "on the fly" in the bitwise decoding cycle itself. Still, here, all the last bits of the blue channel of the entire image are taken, and only then is the message length determined using a binary search in the whole line where the marker occurs.

Modification with message offset. Shifting the message from the beginning of the stegaconteiner protects the latter from truncation attacks. Also, the algorithm assumes that the decoding side does not know the shift percentage; the algorithm determines the encrypted message's beginning and end. At the start of the algorithm, an image, a key, and the shift value from the beginning of the container in percent are obtained; then the width and length of the image are determined, which are multiplied, and the shift percentage is taken; the length of the message to be encrypted by the AES algorithm is taken.

Modification of information encoding in the last 2 bits of the blue channel. A slight modification of this steganographic method allows two or more lower bits per byte to be used for embedding messages. The pixel index is taken, and from it, the blue channel index is converted to a binary string and then to a binary array; the last two bits are replaced with 2 bits from the message string, and then the algorithm is followed. This allows twice as much information to be embedded in the channel that is least noticeable to the human eye.

In the modification with encoding of information in the last bit of each RGB channel, the same is done as in the previous modification with encoding of information in the last 2 bits of the blue channel, not only for the blue channel, but for each RGB channel, one bit. In this modification, AES encoding and message shift from the beginning of the steganographic container were used, and embedding was performed in the last bit of the message in all pixel channels. This allows embedding three times more information.

Thus, the work implements and analyzes the LSB steganographic algorithm and its subsequent modifications: LSB is simple implementation of the LSB algorithm; LSB+AES is modification of LSB using AES encryption; LSB+AES-os is modification of LSB using AES encryption and shifting from the beginning of the steganographic container; LSB+AES-os+2bit is modification of LSB using AES encryption, shifting from the beginning of the steganographic container, and recording data in the last two bits of the blue pixel channel; LSB+AES-os+3ch is modification of LSB using AES encryption and shifting from the beginning of the steganographic container and writing data to each pixel channel in the last bit.

2.2. Evaluation of the quality of the steganographic system

Creating and operating a reliable steganographic method requires specific tools for its control and evaluation. Quantitative assessment of the resistance of a steganographic protection system to external influences is a rather complex task, which is usually implemented in practice by methods of system analysis, mathematical modelling, or experimental research.

As a rule, a professionally designed steganographic system provides a three-level model of information protection, solving two main tasks:

1. Concealing the very fact of the existence of protected information (first level of protection).
2. Blocking unauthorized access to information by selecting an appropriate method of information concealment (second level of protection).

Finally, it is necessary to take into account the possibility of a third level is preliminary cryptographic protection (encryption) of the concealed information.

The quality of the main characteristic of a steganographic system is the level of concealment is assessed by conducting analytical studies (steganographic analysis) and field tests.

Most distortion indicators or quality criteria belong to the group of differential distortion indicators. These indicators are based on the difference between the original container (undistorted signal) and the result container (distorted signal). The second group includes indicators based on the correlation between the original and distorted signals (so-called correlation distortion indicators).

To conduct a comparative analysis of steganographic algorithms, a software solution was developed that compares images based on quality indicators: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Normalized Cross-Correlation (NCC) [31].

The formula for calculating the Peak Signal-to-Noise Ratio (PSNR) is as follows:

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right), \tag{1}$$

where MSE is the mean squared error between the original and modified images (stegoimage). MAX_I is the maximum possible pixel brightness (intensity) (for 8-bit images, $MAX_I = 255$, and for 10-bit images, $MAX_I = 1023$:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[C(x,y) - S(x,y) \right]^2, \tag{2}$$

where m is the number of rows (height) of the image; n is the number of columns (width) of the image; $C(x,y)$ is the pixel value in the original image at coordinates (x,y); $S(x,y)$ is the pixel value in the modified image at coordinates (x,y).

A high PSNR value indicates that the modified image is very similar to the original, i.e., the "noise" (changes) level is low.

The Structural Similarity Index Measure (SSIM) is more complex than PSNR because it considers three key components that correspond to the characteristics of human vision: brightness, contrast, and structure.

The SSIM index for two images (or windows) o and p is calculated as the product of three components:

$$SSIM(c,s) = [l(o,p)]^{\alpha} \cdot [c(o,p)]^{\beta} \cdot [s(o,p)]^{\gamma}, \tag{3}$$

where $l(o,p)=\frac{2\mu_o\mu_p+const_1}{\mu_o^2+\mu_p^2+const_1}$ is the luminance component, μ_o and μ_p are the average pixel intensity values in windows o and p; $c(o,p)=\frac{2\sigma_o\sigma_p+const_2}{\sigma_o^2+\sigma_p^2+const_2}$ is the contrast component, σ_o and σ_p are the standard deviations of pixel intensity (contrast measurement) in windows o and p; $s(o,p)=\frac{\sigma_{op}+const_3}{\sigma_o\sigma_p+const_3}$ is structure component, σ_{op} is covariance between pixels in windows o and p (structural similarity measurement); α, β, and γ are coefficients determining the importance of each element (usually their values are equal to 1); $const_1$, $const_2$, and $const_3$ are small constants added to avoid division by zero when the denominators are close to zero. Their values are calculated using the formulas $const_1 = (K_1,MAX_I)^2$ and $const_2 = (K_2,MAX_I)^2$, where K_1 and K_2 are constants (usually $K_1 = 0.01$, $K_2 = 0.03$).

Normalised Cross-Correlation (NCC) is a metric used in steganography to assess the similarity between two images. In steganography, NCC helps determine how similar a steganographic image (with hidden data) is to the original container image. Unlike PSNR or MSE, which focus on pixel-by-pixel differences, NCC measures the degree of linear dependence between two images.

The formula for NCC is as follows:

$$NCC=\frac{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left(C(x,y)-\overline{C}\right)\left(S(x,y)-\overline{S}\right)}{\sqrt{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left(C(x,y)-\overline{C}\right)^2\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left(S(x,y)-\overline{S}\right)^2}}, \quad (4)$$

where $C(x,y)$ is the pixel value in the original image; $S(x,y)$ is the pixel value in the steganographic image; $\overline{C}$ and $\overline{S}$ are the average pixel intensity values in the original and steganographic images, respectively; m and n are the image dimensions (height and width).

The NCC value ranges from −1 to +1. An NCC value close to 1 indicates a very high similarity between images. This means the steganographic image has an almost identical structure and pixel intensity distribution to the original. A high NCC value (e.g., above 0.99) is a positive indicator for a steganographic algorithm, as it demonstrates that the embedding of data has not significantly altered the overall structure of the image, making the hidden data difficult to detect.

Generalized analysis algorithm:

1. Obtaining the original image and container images, recognizing the extension, and converting to a pixel array.
2. Comparing each container with the original, obtaining coefficients for each value of the number of embedded bits for each distortion indicator.
3. Determining the maximum and minimum values of the coefficients for each distortion indicator.
4. Forming a data array and constructing a graph.

Limitations on the use of the developed approach:

1. The message should not exceed 1/8 of the image file size; otherwise, the text will be shortened to the maximum possible size. When specifying the offset from the beginning of the container, subtract this percentage from the message accordingly; otherwise, the message will also be forcibly shortened.
2. For embedding, a BMP format container is recommended.
3. The container should allocate 8 bits per pixel.

3. Analysis of the effectiveness of the steganography system

3.1. Experimental part

The purpose of the experiments was to analyze the effectiveness of the image in terms of data hiding. The data set for transmitting the secret message consisted of a text file (.txt). The experiment was conducted on a computer with an Intel(R) Core(TM) i9-13900HX processor with a clock speed of 5.40 GHz, 32.0 GB of RAM, and a 64-bit Windows 11 operating system.

The work implements and analyzes the LSB steganographic algorithm and its subsequent modifications, which are listed above:

1. LSB is a simple implementation of the LSB algorithm.
2. LSB+AES is a modification of LSB using AES encryption.
3. LSB+AES-os is a modification of LSB using AES encryption and shifting from the beginning of the steganographic container.
4. LSB+AES-os+2bit is a modification of LSB using AES encryption and shifting from the beginning of the steganographic container and writing data to the last 2 bits of the blue pixel channel.
5. LSB+AES-os+3ch is a modification of LSB using AES encryption, shifting from the beginning of the steganographic container and recording data in each pixel channel in the last bit.

The paper developed software for implementing steganographic algorithms based on the LSB method and analyzed their effectiveness. For this purpose, the image shown in Fig. 3 was taken, and the steganographic methods were analyzed.

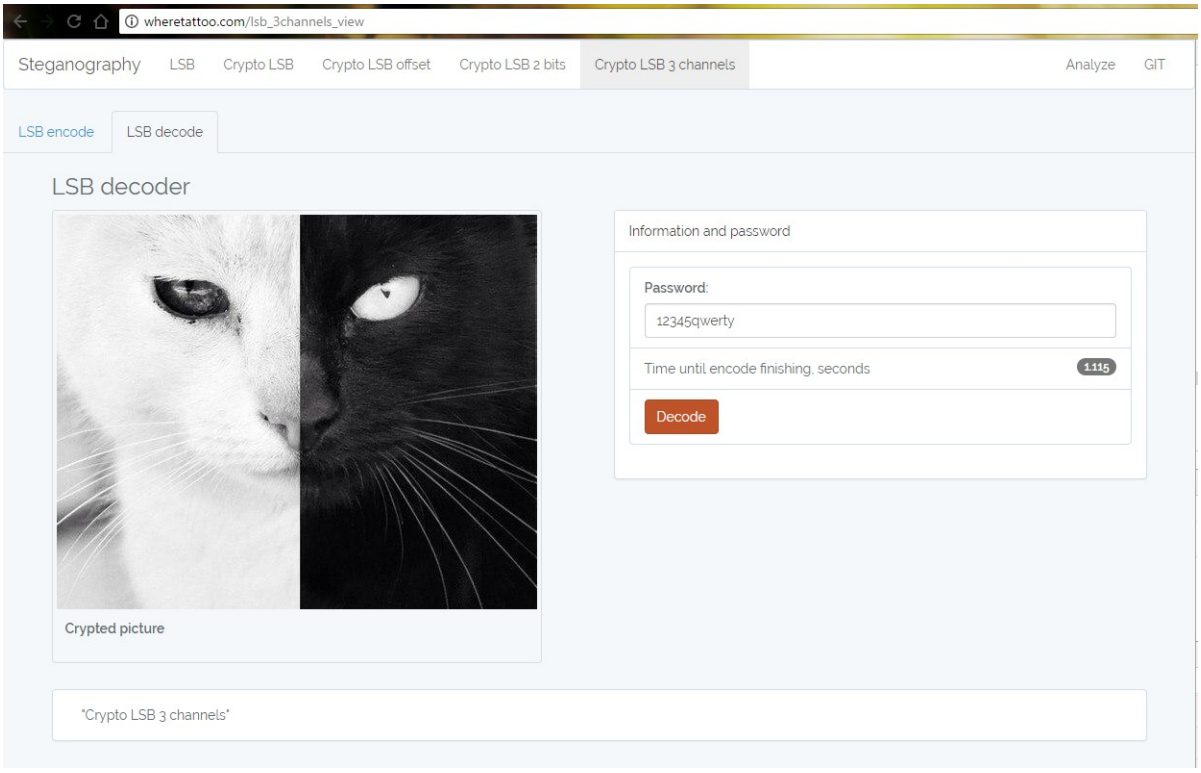

Figure 3: Image used in experimentation for analysis of steganographic algorithms

3.2. Analysis of the effectiveness of the steganographic system based on performance indicators

Analysis by speed. The proposed algorithms' speed data about the encrypted message's capacity are shown graphically in Fig. 4.

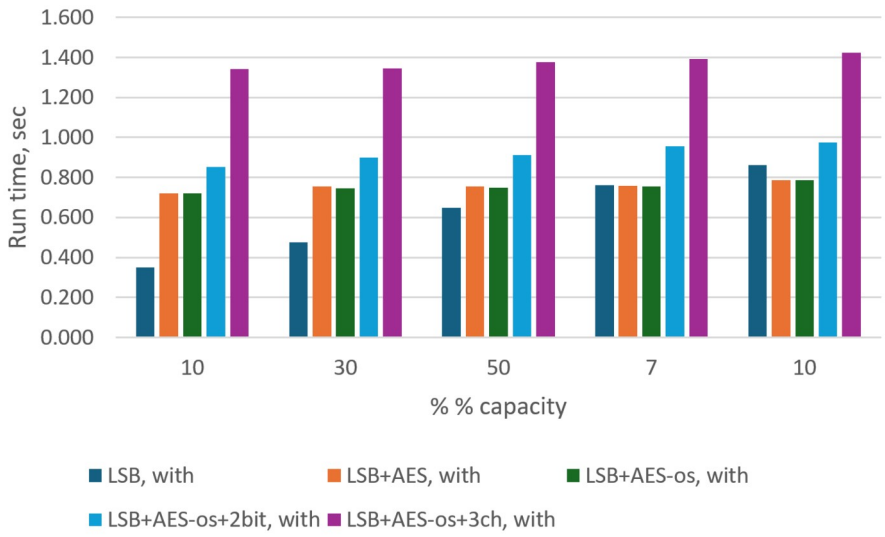

Figure 4: Encoding speed of algorithms

Based on the results obtained, we can conclude that the fastest algorithm for steganography is a modification with the insertion of two characters into the last bit of the blue channel of the pixel (LSB+AES-os+2bit). The slowest modifications are those using AES encryption and shifting from the beginning of the steganocanister (LSB+AES-os). The algorithm's speed-to-decoding ratio is shown in Fig. 5.

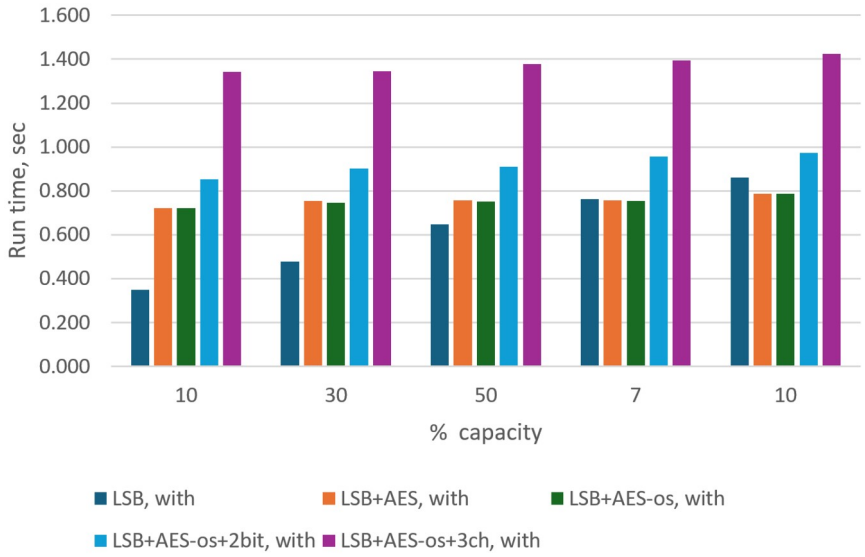

Figure 5: Decoding speed of algorithms

The analysis results show that in the case of decoding, almost identical results are obtained by the following modifications with AES encryption and with a shift from the beginning of the steganographic container (LSB+AES-os), which are the fastest in decoding messages. The slowest algorithm is the one with the message embedded in all three channels in the last bit (LSB+AES-os+3ch), but it should be noted that it is the most complex and includes all other modifications of the LSB algorithm.

Analysis by distortion indicators. To understand the extent of distortion introduced into an image, it is necessary to compare metrics for different amounts of embedded data. The study was conducted on the same image with a size of 29 kilobytes. Various percentage values of character

capacity relative to a simple implementation of the LSB algorithm were taken as typical data sizes for embedding, i.e., 25617 characters were taken as 100%.

The summary results for each steganography system quality assessment indicator and the level of concealment are given in Tables 1, 2, and 3.

Table 1
The value of the PSNR distortion indicator for stegacontainer algorithms

Number of symbols	Capacity, %	LSB	LSB+AES	LSB+AES-os	LSB+AES-os+2bit	LSB+AES-os+3ch
2558	10	53.6837	54.24700	62.5119	77.0763	82.1796
7603	30	48.9452	49.53100	61.1486	76.5698	81.3349
12885	50	46.6389	47.23800	60.4665	74.7570	78.0761
17958	70	45.2100	45.80259	59.1421	73.6600	76.6260
25617	100	43.6800	44.25108	54.4413	71.6930	62.0836

Table 2
SSIM distortion index values for algorithms

Number of symbols	Capacity, %	LSB	LSB+AES	LSB+AES-os	LSB+AES-os+2bit	LSB+AES-os+3ch
2558	10	0.994	0.9978	0.9994	0.9996	0.999
7603	30	0.9939	0.9976	0.999	0.999	0.9877
12885	50	0.9934	0.9972	0.9988	0.9988	0.9786
17958	70	0.993	0.9965	0.9985	0.9976	0.9623
25617	10	0.981	0.9884	0.9875	0.9866	0

Based on the results obtained, we can conclude that the best quality indicators are achieved by algorithms where information encoding took place in the last bit of the blue channel, i.e., the original algorithm embedded in the last bit, a modification using AES encryption with embedding in the last pixel bit, and a modification with a shift based on the least significant bit. Accordingly, embedding in the last bits of the three pixel channels shows the algorithm's worst performance. Increasing the amount of data embedded in the container negatively affects the display statistics. Still, this effect does not reduce the metrics of standard indicators, which are sufficient for steganography.

Table 3
NCC stegagraphic container distortion index values for algorithms

Number of symbols	Capacity, %	LSB	LSB+AES	LSB+AES-os	LSB+AES-os+2bit	LSB+AES-os+3ch
2558	10	0.999948	0.999978	1.000000	1.000000	0.999993950
7603	30	0.999930	0.999976	1.000000	1.000000	0.999981520
12885	50	0.999914	0.999922	0.999900	0.999900	0.999968930
17958	70	0.999800	0.999865	0.999985	0.999976	0.999995661
25617	1	0.999700	0.999740	0.999975	0.999960	0.999993811

The normalized average absolute difference, which indicates the degree of difference between the original container and the container with the embedded secret file, predictably increases with the length of the message, but the increase is not significant. The image quality deviates from 1 by

an average of 0.02%. Visually, container changes cannot be detected in any algorithm modification, and even mathematical analysis does not show a significant distortion value.

Conclusions

In the course of this work, an analysis of steganographic methods based on LSB was proposed and carried out. The following concealment indicators were used for the analysis: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Normalized Cross-Correlation (NCC). The study yielded results suggesting that the fastest algorithm for steganography is a modification involving the insertion of two characters into the last bit of the blue channel of a pixel (LSB+AES-os+2bit). The slowest algorithm is the modification using AES encryption and a shift from the beginning of the stegacontainer (LSB+AES-os). In the case of decoding, modifications using AES encryption and a change from the start of the steganographic container (LSB+AES-os) show almost identical results and are the fastest when decoding messages. The slowest algorithm is the one with message embedding in all three channels in the last bit (LSB+AES-os+3ch), but it should be noted that it is the most complex and includes all other modifications of the LSB algorithm. Increasing the amount of data embedded in the container negatively affects the display statistics. Still, this effect does not reduce the metrics of standard indicators, which are sufficient for steganography.

Depending on the reliability requirements of the steganographic system, the methods presented can be varied, thereby changing the maximum amount of hidden information. The number of bits suitable for embedding depends on the source file and linearly on the number of LSB bits used for encoding. The number of bits ideal for encoding also depends on the percentage of shift. The message embedding is not visually noticeable when using any developed methods.

The practical significance of the results obtained lies in their potential application for covert information transfer with high reliability and resistance to visual detection in open communication channels. Further development of steganographic systems may include fractal analysis and wavelet analysis, as well as the development of a framework for selecting the best steganographic algorithm based on various quality indicators.

Declaration on Generative AI

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

References

[1] A. Ilyenko, et al., Practical aspects of using fully homomorphic encryption systems to protect cloud computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3550, 2023, 226–233.

[2] R. Chernenko, et al., Encryption method for systems with limited computing resources, in: Cybersecurity Providing in Information and Telecommunication Systems, 3288, 2022, 142–148.

[3] T. Radivilova, at al., Intrusion detection based on machine learning using fractal properties of traffic realizations, in: 2019 IEEE Int. Conf. on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, 218–221. doi:10.1109/ATIT49449.2019.9030452

[4] L. Kirichenko, T. Radivilova, I. Zinkevich, Forecasting weakly correlated time series in tasks of electronic commerce, in: 2017 12th Int. Sci. and Technical Conf. on Computer Sci. and Information Technologies (CSIT), Lviv, Ukraine, 2017, 309–312, doi:10.1109/STC-CSIT.2017.8098793

[5] L. Kirichenko, T. Radivilova, Analyzes of the distributed system load with multifractal input data flows, in: 2017 14th Int. Conf. the Experience of Designing and Application of CAD

Systems in Microelectronics (CADSM), Lviv, Ukraine, 2017, 260–264, doi:10.1109/CADSM.2017.7916130

[6] T. Radivilova, et al., The complex method of intrusion detection based on anomaly detection and misuse detection, in: 2020 IEEE 11th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, 133–137. doi:10.1109/DESSERT50317.2020.9125051

[7] Y. I. Daradkeh, L. Kirichenko, T. Radivilova, Development of QoS methods in the information networks with fractal traffic, in: Int. J. Electron. Telecommun. 64(1) (2018) 27–32. doi:10.24425/118142

[8] S. Dovgiy, O. Kopiika, O. Kozlov, Architectures for the information systems, network resources and network services, in: CEUR Workshop Proceedings Cybersecurity Providing in Information and Telecommunication Systems II, 3187, 2021, 293–301.

[9] S. Buchyk, et al., Improvement of steganographic methods based on the analysis of image color models, in: Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2923, 2021, 117–124.

[10] A. Bessalov, et al., Multifunctional CRS encryption scheme on isogenies of nonsupersingular Edwards curves, in: Classic, Quantum, and Post-Quantum Cryptography, 3504, 2023, 12–25.

[11] A. Bessalov, et al., CSIKE-ENC combined encryption scheme with optimized degrees of isogeny distribution, in: Cybersecurity Providing in Information and Telecommunication Systems, 3421, 2023, 36–45.

[12] V. Shah, C. K. Kumbharana, Design, development, and implementation of an image steganography algorithm for encrypted (using AES) and non-encrypted text into an image, in: Rising Threats in Expert Applications and Solutions. Advances in Intelligent Systems and Computing, 1187, 2021, 313–320. doi:10.1007/978-981-15-6014-9_36

[13] I. Ivanisenko, L. Kirichenko, T. Radivilova, Investigation of multifractal properties of additive data stream, in: 2016 IEEE 1st Int. Conf. on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 2016, 305–308, doi:10.1109/DSMP.2016.7583564

[14] S. Talasila, et al., The hybrid model of LSB-technique in image steganography using AES and RSA algorithms, in: Soft Computing and Signal Processing, ICSCSP, Lecture Notes in Networks and Systems, 840, 2024, 403–413. doi:10.1007/978-981-99-8451-0_34

[15] O. O. Kuznetsov, et al., Algebraic immunity of non-linear blocks of symmetric ciphers, Telecommun. Radio Eng. 77(4) (2018) 309–325.

[16] A. Kuznetsov, et al., Research of cross-platform stream symmetric ciphers implementation, in: 2018 IEEE 9th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, 300–305, doi:10.1109/DESSERT.2018.8409148

[17] M. Alanzy, et al., Image steganography using LSB and hybrid encryption algorithms, in Appl. Sci. 13 (2023) 11771. doi:10.3390/app132111771

[18] K. Harshini et al., Enhanced security with crystography using AES and LSB, in: ICCCE 2021. Lecture Notes in Electrical Engineering, 828, 2022, 1063–1071. doi:10.1007/978-981-16-7985-8_111

[19] S. Bilgaiyan, R. Ahmad, S. Sagnika, Adaptive image steganography using rotating color channels and inverted LSB substitution, SN Comput. Sci. 4 (2023) 565, doi:10.1007/s42979-023-01949-0

[20] H. T. Alrikabi, H. Tuama Hazim, Enhanced data security of communication system using combined encryption and steganography, Int. J. Interact. Mob. Technol. 15(16) (2021) 144–157. doi:10.3991/ijim.v15i16.24557

[21] R. I. H. Nasution, A. Fauzi, H. Khair, Hybrid cryptosystem algorithm vigenere cipher and Base64 for text message security utilizing least significant bit (LSB) steganography as insert into image, J. Artif. Intell. Eng. Appl. 2(3) (2023) 89–98. doi:10.59934/jaiea.v2i3.201

[22] A. Gupta, at al., Metamorphic cryptography using AES and LSB method, in: 2022 Int. Conf. on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India, 2022, 1–8. doi:10.1109/ICACCM56405.2022.10009381

[23] M. Loganathan, R. Bharathiraja, (2020). Advanced image security using new combined approach AES cryptography and LSB steganography, Int. J. Adv. Multidiscip. Sci. Res. 3(1) (2020) 98–109. doi:10.31426/ijamsr.2020.3.10.3819

[24] T. Soni, et al., Using least-significant bit and random pixel encoding with encryption for image steganography, in: National Cyber Summit (NCS) Research Track 2020, Advances in Intelligent Systems and Computing, 1271, 2021, 139–153. doi:10.1007/978-3-030-58703-1_9

[25] S. R. Raiyan, M. H. Kabir, SCReedSolo: A secure and robust LSB image steganography framework with randomized symmetric encryption and Reed-Solomon coding, in: arXiv preprint, 2025. doi:10.48550/arXiv.2503.12368

[26] M. Iavich, et al., Classical and post-quantum encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, 3829, 2024, 70–78.

[27] I. Diop, K. Tall, A new hybrid approach of data hiding using LSB steganography and caesar cipher and RSA algorithm (S-ccr), in: 2022 Int. Conf. on Computer Communication and Informatics (ICCCI), 2022, 1–4. doi:10.1109/ICCCI54379.2022.9740979

[28] K. Tiwari, S. J. Gangurde, LSB steganography using pixel locator sequence with AES, in: 2021 2nd Int. Conf. on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, 302–307, doi:10.1109/ICSCCC51823.2021.9478162

[29] S. Roy, M. M. Islam, A hybrid secured approach combining LSB steganography and AES using mosaic images for ensuring data security, SN Comput. Sci. 3 (2022) 153. doi:10.1007/s42979-022-01046-8

[30] M. S. Hasan Talukder, et al., An enhanced method for encrypting image and text data simultaneously using AES algorithm and LSB-based Steganography, in: 2022 Int. Conf. on Advancement in Electrical and Electronic Engineering (ICAEEE), Gazipur, Bangladesh, 2022, 1–5. doi:10.1109/ICAEEE54957.2022.9836589

[31] I. Haverkamp, D. K. Sarmah, Evaluating the merits and constraints of cryptography-steganography fusion: A systematic analysis, Int. J. Inf. Secur. 23 (2024) 2607–2635. doi:10.1007/s10207-024-00853-9