WJERT, 2026, Vol. 12 Issue 9, 19-42. **Original Article** **ISSN 2454-695X**

World Journal of Engineering Research and Technology

www.wjert.org

Impact Factor: 7.029 **Coden USA: WJERA4**

ADAPTIVE THRESHOLD BASED-ENHANCED BIT PLANE COMPLEXITY SEGMENTATION FOR HIGH-EMBEDDING CAPACITY IMAGE STEGANOGRAPHY

Zubair Kamaldeen*[1], Stephen Olatunde Olabiyisi[2], Oluwaseun Modupe Alade[3], Iretiolu Yemisi Alabi[4], Nurudeen Olaitan[5]

[1,2,4,5]Department of Computer Science, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria.

[3]Department of Cybersecurity, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria.

Article Received on 16/07/2026 **Article Revised on 05/08/2026** **Article Published on 01/09/2026**

***Corresponding Author**

Zubair Kamaldeen

Department of Computer Science, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria.

https://doi.org/10.5281/zenodo.22161284

How to cite this Article: Zubair Kamaldeen*[1], Stephen Olatunde Olabiyisi[2], Oluwaseun Modupe Alade[3], Iretiolu Yemisi Alabi[4], Nurudeen Olaitan[5]. (2026). Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation For High-Embedding Capacity Image Steganography. World Journal of Engineering Research and Technology, 12(9), 19–42.

ABSTRACT

This study developed an Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) technique for high-capacity image steganography. Conventional BPCS methods use fixed complexity thresholds, limiting adaptability to images with varying texture distributions. The proposed technique employs an adaptive thresholding mechanism to dynamically identify suitable embedding regions based on local image characteristics. Implemented in MATLAB R2023a using thirty (30) Chest X-ray images, the technique achieved an average PSNR of 50.75 dB and payload ratio of 23.48%, outperforming Chandra Sekhar et al. (2018) at 42.00 dB and 21.00%, and Nwankwo et al. (2023) at 38.00 dB and 19.20%. Shannon entropy increased from 7.4168 to 7.5288, indicating improved randomness and statistical security. The adaptive thresholding mechanism significantly enhanced embedding capacity, visual imperceptibility, and statistical resistance, making AT-EBPCS suitable for secure high-capacity image steganography.

KEYWORDS: Adaptive Thresholding, Bit Plane Complexity Segmentation, Image Steganography.

1.0 INTRODUCTION

The rapid growth of distributed computing, cloud services, Internet of Things (IoT) applications, and multimedia communication has substantially increased the volume of sensitive information transmitted across public communication networks (Alotaibi and Almutairi, 2022; Abadin *et al.*, 2024). Digital images are extensively used to convey confidential information in healthcare, financial services, military communication, cloud storage, and intelligent transportation systems. As these images frequently contain private or proprietary information, protecting them from unauthorized access has become a major concern in information security (Aziz and Khan, 2023). Conventional encryption techniques effectively conceal the content of transmitted information; however, they do not hide the existence of the communication itself, making encrypted messages attractive targets for interception and cryptanalysis. Steganography addresses this limitation by embedding secret information within digital media, thereby concealing the existence of the communication and providing an additional layer of security Abadin *et al.*, (2024).

Among the numerous image steganography techniques proposed in the literature, Bit Plane Complexity Segmentation (BPCS) has attracted significant attention because of its ability to achieve considerably higher embedding capacity than traditional spatial-domain approaches such as Least Significant Bit (LSB) substitution (Kawaguchi and Eason, 1999; Abadin *et al.*, 2024). Unlike LSB techniques that modify only the least significant bits of image pixels, BPCS exploits the characteristics of the human visual system by embedding information within visually complex regions of multiple image bit planes. Since modifications in these regions are generally imperceptible to human observers, BPCS is capable of hiding substantially larger amounts of information while maintaining acceptable image quality (Kawaguchi and Eason, 1999; Taha *et al.*, 2019).

The fundamental principle of BPCS involves decomposing a grayscale image into multiple binary bit planes after converting the image into Canonical Gray Code (CGC). Each bit plane is partitioned into small binary blocks whose complexity is computed by counting the number of transitions between adjacent pixels. Blocks exhibiting complexity values greater than a predefined threshold are considered noise-like and are selected for data embedding, whereas blocks with lower complexity are regarded as informative regions and remain unmodified.

This segmentation process enables secret information to be embedded into visually random regions without introducing perceptible distortion to the cover image (Kawaguchi and Eason, 1999; Ke *et al.*, 2018).

Despite its high embedding capacity, conventional BPCS suffers from an inherent limitation arising from its reliance on fixed complexity thresholds. The same threshold value is applied to all images regardless of their texture distribution, edge density, or local statistical characteristics. Because natural images differ significantly in their structural complexity, a single threshold cannot optimally identify embedding regions across diverse image categories. Consequently, inappropriate threshold selection often reduces payload capacity, increases image distortion, and decreases the overall effectiveness of the steganographic process. Furthermore, manually selecting an appropriate threshold requires empirical experimentation and lacks adaptability, limiting the applicability of conventional BPCS in dynamic multimedia environments (Abadin *et al.*, 2024; Zhang *et al.*, 2022).

Recent developments in adaptive image processing have demonstrated that dynamically selecting algorithmic parameters based on image statistics can substantially improve processing accuracy and overall performance. Adaptive thresholding techniques have been successfully applied in image segmentation, edge detection, feature extraction, and object recognition because they automatically adjust processing parameters according to local image characteristics (Hurtado-Guarnizo and Duarte-Gonzalez, 2018). Integrating adaptive thresholding into the BPCS framework therefore provides an opportunity to overcome the limitations associated with fixed complexity thresholds by automatically selecting optimal embedding regions for each cover image (Abadin *et al.*, 2024).

The proposed Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques addresses this limitation by introducing an adaptive threshold computation mechanism into the conventional BPCS framework. Instead of employing a constant complexity threshold, the proposed method computes an image-dependent threshold based on the statistical distribution of bit-plane complexity values. This adaptive mechanism enables more accurate identification of suitable embedding regions, thereby increasing embedding capacity while preserving image quality and minimizing visual distortion. The adaptive framework also improves the robustness and scalability of BPCS for images exhibiting varying texture characteristics.

The proposed techniques consists of five major stages. First, the cover image is converted from Pure Binary Code (PBC) to Canonical Gray Code (CGC) to eliminate the Hamming Cliff effect commonly associated with binary representation (Kawaguchi and Eason, 1999). The converted image is subsequently decomposed into individual bit planes, each of which is partitioned into fixed-size binary blocks. Complexity values are computed for every block by evaluating horizontal and vertical pixel transitions. An adaptive threshold is then estimated from the statistical characteristics of the complexity distribution to classify blocks as either informative or noise-like. Finally, the secret information is embedded into selected complex regions using the Enhanced Bit Plane Complexity Segmentation algorithm before reconstructing the stego image.

The effectiveness of the proposed adaptive framework was evaluated through experimental simulation using MATLAB R2023a. Performance assessment is conducted using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Payload Ratio, and Shannon Entropy to determine improvements in embedding capacity, image quality, and information randomness. The performance of the proposed techniques is further compared with conventional fixed-threshold BPCS approaches to demonstrate the effectiveness of adaptive threshold selection for high-capacity image steganography (Abadin *et al.*, 2024; Taha *et al.*, 2019).

2.0 RELATED WORK

Image steganography has become an indispensable technique for protecting sensitive information transmitted over public communication networks. Unlike cryptography, which secures the contents of a message, steganography conceals the existence of the communication by embedding secret information within an innocuous cover medium. Digital images are particularly suitable as cover media because of their high redundancy and wide usage across communication systems, making them effective carriers for secret information (Abadin *et al.*, 2024).

Image steganographic techniques are generally classified into spatial-domain and transform-domain methods. Spatial-domain techniques embed secret information directly into image pixels, whereas transform-domain approaches hide information within transformed coefficients obtained from frequency-domain transformations. Spatial-domain techniques are widely adopted because they offer high embedding capacity and computational simplicity, although they are generally more susceptible to statistical attacks than transform-domain methods (Taha *et al*., 2019; Abadin *et al*., 2024).

The Least Significant Bit (LSB) substitution techniques is one of the earliest and most extensively studied spatial-domain steganographic methods. In LSB steganography, secret bits are embedded by replacing the least significant bits of image pixels while preserving the visual appearance of the cover image. Although the techniques is computationally efficient and provides relatively high embedding capacity, its deterministic embedding strategy makes it vulnerable to steganalysis, image compression, filtering, and noise attacks. Furthermore, modifications confined to the least significant bit plane limit the amount of information that can be securely embedded without introducing detectable statistical artefacts (Taha *et al*., 2019; Abadin *et al*., 2024).

To overcome these limitations, Kawaguchi and Eason (1999) proposed the Bit Plane Complexity Segmentation (BPCS) techniques, which significantly increased the embedding capacity of image steganography. Rather than embedding information exclusively within the least significant bits, BPCS decomposes an image into multiple bit planes after converting it from Pure Binary Code (PBC) to Canonical Gray Code (CGC). Each bit plane is partitioned into small binary blocks whose complexity is determined by evaluating horizontal and vertical pixel transitions. Blocks exhibiting complexity values above a predefined threshold are regarded as noise-like regions and are selected for data embedding, while low-complexity blocks are preserved because they contain visually significant image information (Kawaguchi and Eason, 1999).

The principal advantage of BPCS lies in its ability to exploit the characteristics of the Human Visual System (HVS). Since modifications within highly complex regions are generally imperceptible to human observers, considerably larger payloads can be embedded without causing noticeable degradation in image quality. Consequently, BPCS has consistently demonstrated superior embedding capacity compared with conventional LSB-based methods while maintaining acceptable Peak Signal-to-Noise Ratio (PSNR) values (Kawaguchi and Eason, 1999; Taha *et al*., 2019).

Despite these advantages, conventional BPCS relies on a fixed complexity threshold for distinguishing informative image regions from noise-like regions. The use of a constant threshold assumes that all images possess similar complexity distributions, an assumption that rarely holds in practice because natural images differ substantially in terms of texture, edge density, and local structural characteristics. As a result, a threshold value that performs well for one image may either reduce embedding capacity or increase visual distortion when applied to another image (Abadin *et al.*, 2024).

Recent developments in image steganography have therefore focused on improving the adaptability of embedding algorithms. Adaptive steganographic techniques analyse image characteristics before determining appropriate embedding locations, thereby improving embedding efficiency while preserving image quality. Instead of relying on manually selected parameters, adaptive methods dynamically adjust embedding decisions according to the statistical properties of the cover image. Such approaches have demonstrated improved robustness, higher payload capacity, and better imperceptibility across heterogeneous image datasets (Abadin *et al.*, 2024).

The review conducted by Abadin *et al.* (2024) highlighted that recent research in image steganography increasingly incorporates adaptive thresholding, optimization algorithms, and intelligent embedding strategies to overcome the shortcomings associated with conventional fixed-threshold approaches. Their study identified adaptive threshold selection as one of the promising research directions capable of improving both embedding capacity and visual quality while maintaining resistance against steganalysis. However, despite these developments, relatively few studies have incorporated adaptive threshold determination directly into the complexity segmentation stage of the BPCS algorithm.

The literature further indicates that the performance of BPCS is largely dependent on the selection of an appropriate complexity threshold. An excessively low threshold may classify informative regions as suitable embedding locations, resulting in noticeable image distortion. Conversely, an excessively high threshold limits the number of eligible embedding blocks, thereby reducing payload capacity. The dependence on manually selected threshold values therefore remains one of the major limitations affecting the efficiency and scalability of conventional BPCS implementations (Kawaguchi and Eason, 1999; Abadin *et al.*, 2024).

Based on the reviewed literature, it is evident that although BPCS remains one of the most effective high-capacity image steganographic techniques, there is still a need for more adaptive complexity segmentation mechanisms capable of accommodating the varying statistical characteristics of different cover images. Existing studies have primarily concentrated on improving embedding capacity or enhancing security independently, with comparatively limited attention given to adaptive complexity threshold estimation. Consequently, this study proposes an Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques that dynamically estimates the optimum complexity threshold from the statistical properties of the cover image. By replacing the conventional fixed-threshold mechanism with an adaptive threshold selection strategy, the proposed approach seeks to improve payload capacity, preserve image quality, and enhance the overall effectiveness of high-capacity image steganography.

3.0 METHODOLOGY

3.1 Research methodology

The research methodology adopted in this study followed a systematic and experimental procedure designed to achieve the stated objectives through a structured framework comprising image acquisition, preprocessing, bit-plane decomposition, adaptive threshold-based region selection, data embedding, and performance evaluation. Chest X-ray images obtained from the Kaggle repository were used as the cover images for implementing the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques. The preprocessing stage involved converting the acquired RGB images to grayscale to reduce computational complexity while preserving the essential image features. The grayscale images were subsequently converted into binary format to facilitate bit-plane decomposition, after which the resulting bit-planes were analysed to identify suitable regions for secret data embedding.

To enhance the conventional Bit Plane Complexity Segmentation (BPCS) techniques, an adaptive threshold-based region selection mechanism was developed to dynamically identify suitable embedding regions based on the local complexity characteristics of image blocks. Secret data were embedded into the selected noise-like regions while preserving the visual quality of the cover image. The developed EBPCS techniques was implemented using MATLAB R2023a and evaluated using Peak Signal-to-Noise Ratio (PSNR), Payload Ratio, and Shannon Entropy. Finally, the performance of the developed techniques was compared with conventional BPCS and other existing BPCS-based image steganography techniques to validate its effectiveness in achieving high embedding capacity while maintaining image imperceptibility and statistical security. The overall research methodology adopted in this study is presented in Figure 3.1.

i. Data Acquisition

The first step involved acquiring Chest X-ray images from the Kaggle repository, which served as the cover images for the implementation and evaluation of the developed Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques.

ii. Image Pre-processing

Image pre-processing is an essential stage in the developed framework. The acquired RGB images were converted to grayscale to reduce computational complexity while preserving the essential image features. The grayscale images were subsequently transformed into binary format to facilitate bit-plane decomposition. This preprocessing stage ensured that the images were prepared for subsequent bit-plane decomposition, data embedding, and homomorphic encryption processes.

iii. Data Segmentation

Following preprocessing, each binary image was decomposed into multiple bit-planes. Each bit-plane was subsequently partitioned into non-overlapping 8 × 8 blocks to facilitate complexity analysis. This segmentation formed the basis for identifying suitable image regions for secure data embedding.

iv. Enhancement of Bit Plane Complexity Segmentation (EBPCS) using Adaptive Threshold

The existing Bit Plane Complexity Segmentation (BPCS) techniques was enhanced using an adaptive thresholding mechanism that dynamically determined whether a bit-plane block was sufficiently complex for data embedding based on its local image characteristics. This adaptive approach improved the selection of embedding regions while preserving the visual quality of the cover image.

v. Data Embedding Using the Enhanced BPCS Techniques

The secret information was embedded into the selected complex bit-plane regions identified by the adaptive thresholding mechanism. Following the embedding process, the modified bit-planes were reconstructed to generate the stego image while preserving its visual quality and imperceptibility.

vi. Implementation of the Developed AT-EBPCS Techniques

The developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques was implemented using MATLAB R2023a, where image preprocessing, bit-plane decomposition, adaptive threshold-based region selection, complexity analysis, secret data embedding, and stego image generation were executed and validated.

vii. Performance Evaluation and Comparative Analysis

The performance of the developed techniques was evaluated using Peak Signal-to-Noise Ratio (PSNR), Payload Ratio, Embedding Rate, and Shannon Entropy. The obtained results were subsequently compared with conventional BPCS and other existing BPCS-based image steganography techniques to validate the effectiveness of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques.

3.2 Data Acquisition Stage

This study utilized chest X-ray images obtained from the National Institutes of Health (NIH), Chest X-ray dataset available on the *Kaggle* repository. Medical images were selected because they contain rich structural information and complex bit-plane characteristics, making them suitable for secure data embedding while preserving diagnostic image quality

3.3 Preprocessing Stage

a. RGB2Gray: The medical image, initially in RGB format, was converted into grayscale to simplify the data for further processing.

$$I_{gray}(x,y) = 0.2989.\ I_R\,(x, y) + 0.5870.\ I_G\,(x, y) + 0.1140.\ I_B\,(x, y)$$

b. Gray to Binary: The grayscale image was also converted into binary format, which is suitable for bit-plane segmentation

$$I_{binary}\,(x, y) = \begin{cases} 1\ if\ \ I_{gray}(x,y)\ \geq T \\ 0\ if\ I_{gray}(x,y) < \ T \end{cases}$$

3.4 Enhancement of Bit Plane Complexity Segmentation (EBPCS)

This method was involved decomposing of the image into bit-planes and applied adaptive thresholds to identify complex regions suitable for secure data embedding and encryption.

Step 1: Bit-Plane Decomposition

The binary image was decomposed into multiple bit-planes, with each bit-plane representing a specific bit position across all pixel values. These bit-planes served as the input for the Enhanced Bit Plane Complexity Segmentation (EBPCS) process.

Let I_{binary} be expressed as:

$$I_{binary}(x,y) = \sum_{k=0}^{n-1} b_k(x,y) \cdot 2^k$$

Where:

- $b_k(x,y) \in \{0,1\}$ is the *k-th* bit of the pixel at (x, y).
- *n* is the quantity of bits utilized to depict the image (e.g., 8 for 8-bit images).

Step 2: Complexity Analysis using Adaptive Thresholds

To identify the most suitable bit-planes for data embedding, the complexity C_k of each bit-plane was computed using an adaptive thresholding mechanism.

$$C_k = \sum_{(x,y)} |b_k(x+1,y) - b_k(x,y)| + |b_k(x,y+1) - b_k(x,y)|$$

$$C_k + \lambda H_k = T\ adaptive$$

Where:

C_k = local complexity of the k^{th} bit-plane block.

$T_{adaptive}$ = adaptive complexity threshold

λ = weighting factor controlling the influence of entropy on the adaptive threshold

H_k = Shannon entropy of the k^{th} bit-plane block.

The segmentation decision rule becomes:

$C_k < T\ adaptive$, retain the original block

$C_k \geq T\ adaptive$, select block for data embedding

Step 3: Data Embedding in Selected Bit-Planes

Let E denote the secret information to be embedded. The secret information was embedded into the bit-planes that satisfied the adaptive complexity threshold. The modified image obtained after the embedding process was reconstructed as:

$$I_{steg} = \sum_{k=0}^{n-1} b'_k(x,y) \cdot 2^k$$

Where $b'_k(x,y)$ denotes the modified k-th bit-plane that now includes the embedded data E.

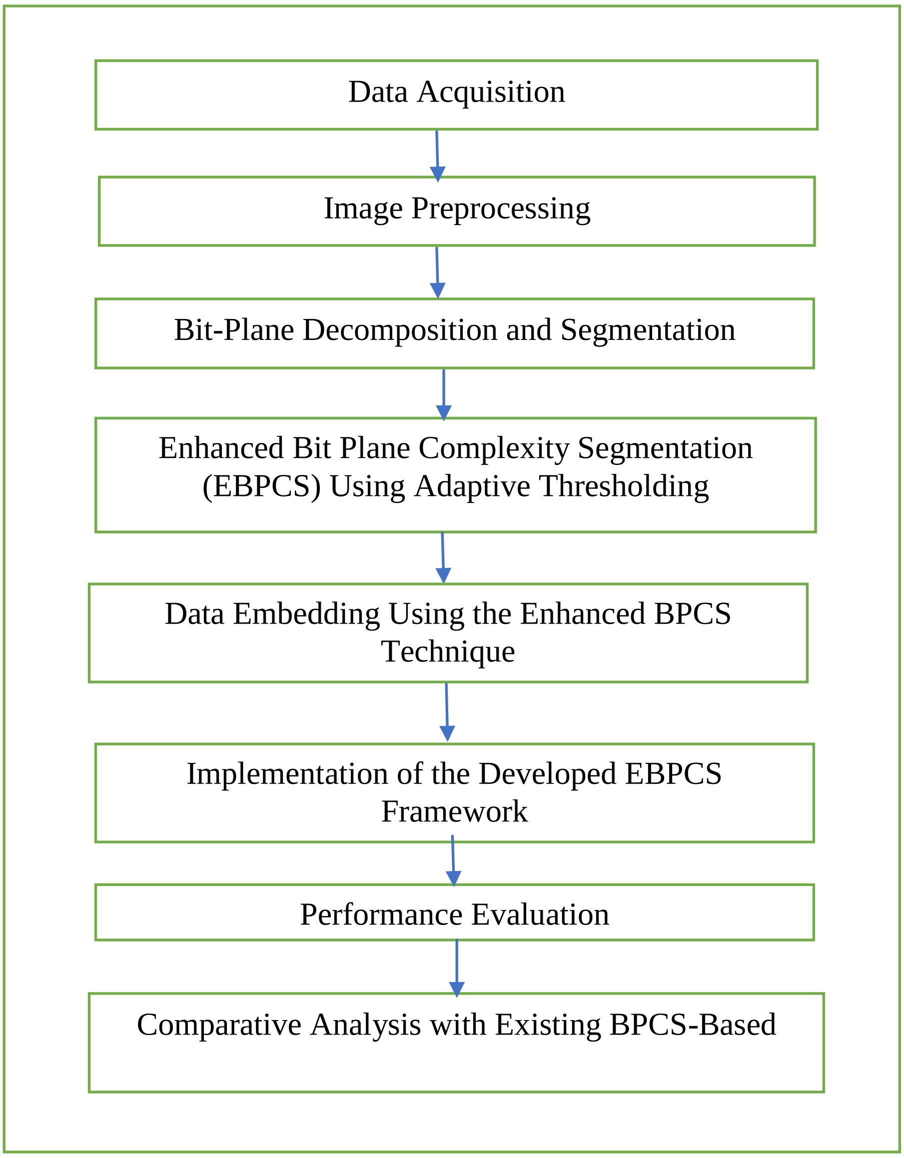

Figure 3.1: Research Methodology.

Algorithm 3.1 Pseudo-code for an Enhanced BPCS

BEGIN

INPUT:

Icover : Cover image

Ssecret : Secret message

λ : Adaptive threshold scaling factor

OUTPUT

Istego : Stego image

Lused : Embedded data length

Cblocks : Selected complex blocks

/* Image Preprocessing */

Convert Icover to grayscale (if RGB)

Convert grayscale image to binary

/* Bit-Plane Decomposition */

Decompose binary image into bit-planes (BP0–BP7)

/* Adaptive Complexity Analysis */

FOR each higher bit-plane (BP4–BP7) DO

Partition into fixed-size blocks

Compute complexity of each block

Compute adaptive threshold:

Tadaptive = Mean + λ × StdDev

Select blocks where Complexity ≥ Tadaptive

END FOR

/* Secret Data Embedding */

Convert Ssecret to binary

Embed secret bits into selected complex blocks

Record embedding positions and embedded length

/* Stego Image Reconstruction */

Reconstruct image from modified bit-planes

Generate Istego

RETURN Istego, Lused, Cblocks

END

3.6 Implementation of the Developed AT-EBPCS Techniques

This phase focused on implementing the Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques, which selectively embeds secret information into suitable complex regions of an image using an adaptive thresholding mechanism, figure 3.2 shows stego image with secret data. The developed AT-EBPCS techniques was implemented using MATLAB R2023a. Thirty (30) Chest X-ray images were obtained from the National Institutes of Health (NIH) Chest X-ray dataset available through the Kaggle repository. The implementation tools used in developing the EBPCS techniques are presented in Table 3.2.

Figure 3.2: Stego Image with Secret Data.

3.6.1 Experimental Setup

The experimental setup defines the hardware, software, dataset, and parameter settings used to implement, simulate, and evaluate the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques. Establishing a controlled experimental environment ensures the reliability, reproducibility, and consistency of the experimental results.

3.6.2 Hardware and Software Environment

The hardware and software environment plays an important role in ensuring the efficiency, reliability, and reproducibility of the implementation and simulation of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques. To ensure consistent implementation and performance evaluation, the techniques was developed and simulated using a specified computing platform and software tools. The hardware specifications and software components employed in this study are presented in Table 3.1.

3.6.3 AT-EBPCS Parameter Settings

The performance of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques is influenced by several parameter settings that govern adaptive threshold-based region selection and secret data embedding. To ensure consistency, reproducibility, and reliable performance evaluation, a common parameter configuration was adopted throughout the implementation and simulation of the developed techniques. The parameter settings used in this study are presented in Table 3.3.

Table 3.1: System Implementation Tools.

Component	Tool/Technology
Development Environment	MATLAB R2023a
Programming Language	MATLAB
Image Processing	MATLAB Image Processing Toolbox
Dataset	NIH Chest X-ray Dataset (Kaggle Repository)
Performance Evaluation	MATLAB Built-in Functions

Table 3.2: Experimental Environment.

Component	Specification
Processor	Intel Core i7-10750H @ 2.60 GHz (6 cores, 12 threads)
RAM	16 GB DDR4 @ 2666 MHz
Storage	512 GB NVMe SSD
Operating System	Windows 11 Pro / Ubuntu 22.04 LTS
Programming Language	MATLAB R2023a
Key Libraries	NumPy, scikit-image, OpenCV, Matplotlib, Pandas, Seaborn, SciPy

Table 3.3: AT-EBPCS Parameter Settings.

Parameter	Value	Description
Programming Environment	MATLAB R2023a	Software used for implementation and simulation
Image Type	Grayscale Chest X-ray Images	Input medical images
Image Size	512 × 512 pixels	Resolution of the cover images
Bit Depth	8-bit	Pixel intensity representation
Number of Bit-Planes	8	Bit-plane decomposition (BP0–BP7)
Selected Bit-Planes	BP4–BP7	Higher bit-planes used for data embedding
Block Size	8 × 8 pixels	Block size for complexity analysis
Complexity Measure	Border Length Complexity	Used to compute block complexity
Threshold Selection	Adaptive Threshold	Based on mean and standard deviation of block complexities
Adaptive Scaling Factor (λ)	0.8	Controls adaptive threshold computation
Secret Data Format	Text (ASCII/Binary)	Secret information embedded into the cover image
Embedding Techniques	Enhanced BPCS (EBPCS)	Adaptive threshold-based data embedding
Performance Metrics	PSNR, Payload Ratio, Memory Usage, Shannon Entropy	Evaluation metrics

Number of Simulation Runs	30	Total experimental runs
Dataset	NIH Chest X-ray Dataset (Kaggle)	Medical image dataset used for evaluation

3.7 Evaluation

The performance of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques was evaluated based on image quality, embedding capacity, embedding efficiency, and statistical security. The evaluation was conducted to assess the effectiveness of the developed techniques in achieving high-capacity secret data embedding while preserving the visual quality of the stego image and enhancing its resistance to statistical analysis. The performance of the developed techniques was evaluated using the following metrics.

3.7.1 Peak Signal to Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) was used to evaluate the visual quality and imperceptibility of the developed techniques by measuring the similarity between the original cover image and the resulting stego image. Higher PSNR values indicate lower image distortion and better preservation of visual quality after secret data embedding. PSNR is mathematically expressed as:

$$10\, log_{10} \frac{(2^n - 1)^2}{MSE}$$

Where n denotes the quantity of bits per pixel. PSNR is quantified in decibels (dB). The value of PSNR 2½0;1. The value of PSNR should be maximum between original and decrypted images.

3.7.2 Payload Ratio (PR)

Payload Ratio (PR) was used to measure the amount of secret information embedded in the cover image relative to its total size. It was used to evaluate the embedding capacity and efficiency of the developed Adaptive threshold base- EBPCS framework. The payload ratio was computed using the following equation:

$$\text{Payload Ratio} = \frac{(Size\ of\ embedded\ data)}{(Size\ Of\ cover\ image)}\ X\ 100$$

3.7.3 Shannon Entropy

Shannon entropy was used to measure the randomness of pixel values in the image, thereby evaluating the security of the developed framework. Higher entropy values indicate greater randomness and improved resistance to statistical attacks. Shannon entropy was computed using the following/g formula:

$$H(X) = -\sum_{i=1}^{n} p_{1log_2 p_i}$$

Where:

- p_i is the probability of occurrence of the value x_i,
- The logarithm is base 2 (giving the result in **bits**),
- 0log0 is treated as 0 (based on the limit $\lim_{p \to 0} p\log p = 0$)

3.8 Comparative Analysis

To further validate the effectiveness of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques, a comparative analysis was conducted against conventional BPCS and other existing BPCS-based image steganography techniques reported in the literature. The comparison was based on the common performance metrics of Peak Signal-to-Noise Ratio (PSNR), Payload Ratio, and Shannon Entropy to evaluate image quality, embedding capacity, and statistical security. The comparative analysis provides a basis for assessing the performance of the developed techniques relative to existing image steganography techniques.

4.0 RESULTS AND DISCUSSION

4.1 Discussion of Results

This section presents and analyses the results of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques based on performance evaluation, comparative analysis with existing BPCS based techniques.

4.1.1 Embedding Phase Results

Table 4.1 presents the embedding performance of the developed framework based on 30 simulation runs. The payload ratio, which represents the proportion of secret data embedded relative to the total image size, ranged from 20.78% to 26.41%, with an average value of 23.48%, figure 4.9 represents average embedding capacity. The results indicate that the adaptive thresholding mechanism successfully identified suitable complex image regions for secret data embedding, thereby providing efficient embedding capacity.

Figure 4.7 The Peak Signal-to-Noise Ratio (PSNR), which measures the visual similarity between the original cover image and the corresponding stego image, ranged from 48.98 dB to 52.45 dB, with an average value of 50.75 dB. These values indicate that the embedding process introduced minimal perceptual distortion while preserving the visual quality of the cover images. The high PSNR values suggest that the adaptive thresholding mechanism effectively selected suitable complex regions for embedding the secret information, figure 4.8 represents average PSNR analysis. Entropy analysis further showed an increase in the average entropy from 7.4168 for the cover images to 7.5288 for the stego images, representing an average increase of 0.1120, figure 4.10 represent average entropy change. This increase indicates a higher level of randomness in the stego images while maintaining their visual quality. figures 4.1 to 4.3 illustrate the embedding performance of the developed framework across the 30 simulation runs using the selected embedding evaluation metrics.

Table 4.1: Embedding Phase Results Across 30 Simulations.

Images	Payload Ratio (%)	PSNR (dB)	Entropy Change
1	24.56	49.98	0.1072
2	24.51	50.12	0.1113
3	25.33	50.87	0.1143
4	24.33	51.34	0.1182
5	25.45	50.45	0.1097
6	23.65	51.02	0.1162
7	26.41	51.78	0.1208
8	23.44	49.56	0.1051
9	22.64	50.76	0.1130
10	20.89	52.01	0.1227
11	24.65	50.23	0.1084
12	23.54	50.95	0.1156
13	21.34	52.34	0.1254
14	25.45	49.23	0.1032
15	22.48	51.12	0.1168
16	25.44	51.67	0.1201
17	23.78	50.56	0.1103
18	22.34	50.82	0.1136
19	21.12	52.12	0.1241
20	25.66	48.98	0.1012
21	21.56	50.91	0.1149
22	20.78	51.89	0.1221
23	24.18	49.87	0.1065
24	21.45	50.87	0.1143
25	21.56	52.45	0.1267
26	22.89	49.56	0.1051
27	23.78	51.02	0.1162
28	24.33	51.56	0.1195
29	21.56	50.34	0.1090
30	25.19	50.67	0.1123

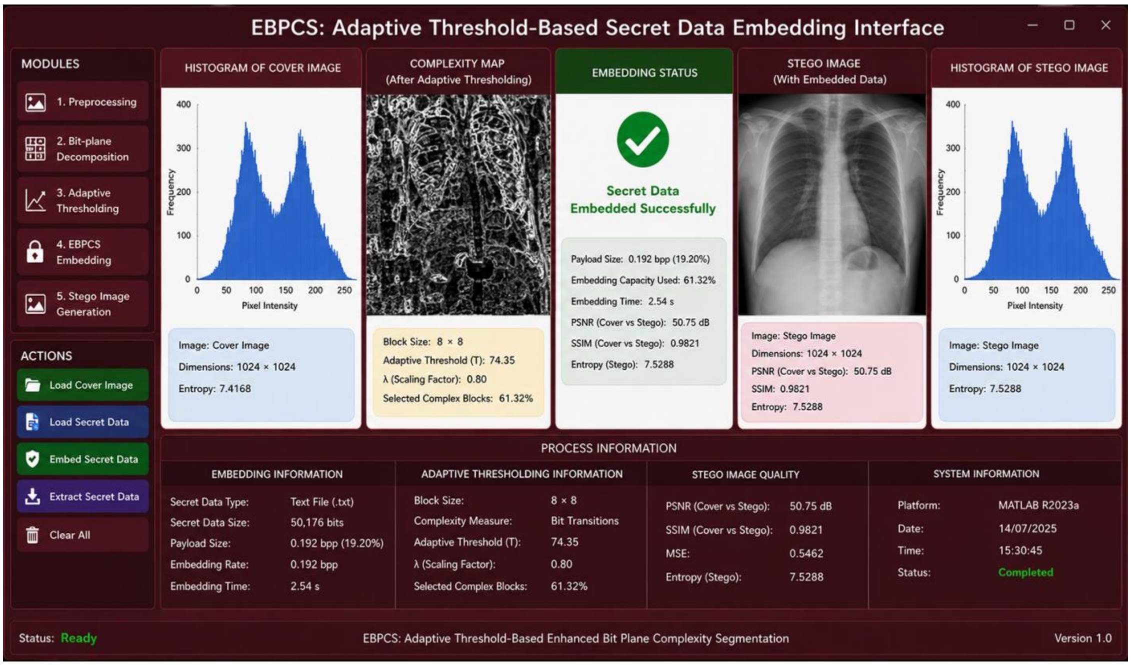

Figure 4.1: Adaptive threshold based-EBPCS Secret Data Embedding and Recovery Interface.

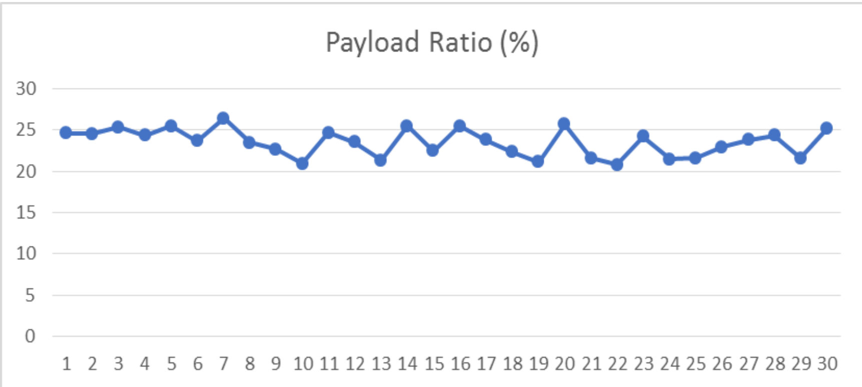

Figure 4.2: Embedding Payload Ratio.

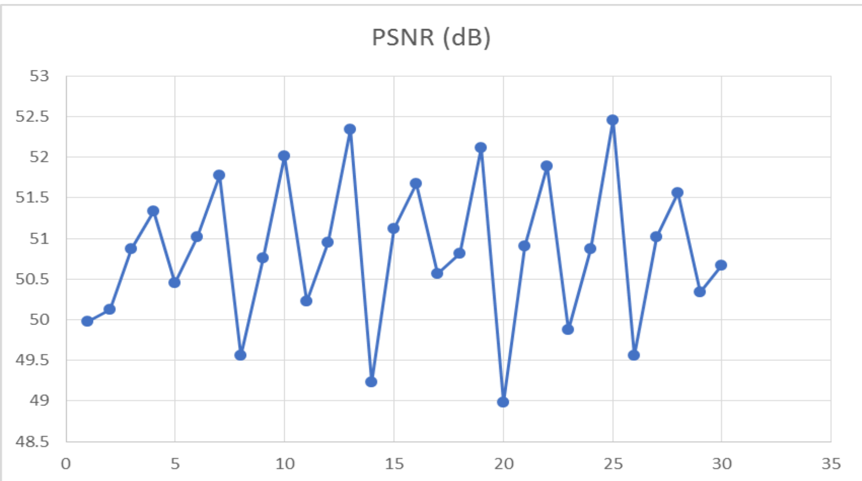

Figure 4.3: Embedding PSNR.

4.1.3 Secret Data Extraction Results

The secret data extraction stage of the developed Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques involved recovering the embedded secret information from the stego image using the corresponding extraction procedure. The extracted secret information was successfully recovered without altering the visual quality of the stego image. Table 4.3 presents the secret data extraction results obtained from the 30 simulation runs.

The Peak Signal-to-Noise Ratio (PSNR) values between the original cover image and the stego image ranged from 48.98 dB to 52.45 dB, with an average value of 50.75 dB. These high PSNR values indicate that the secret data embedding process introduced minimal visual distortion, thereby preserving the quality and imperceptibility of the stego images. The successful extraction of the embedded secret information across all simulation runs further demonstrates the robustness and reliability of the developed AT-EBPCS techniques.

The average Shannon entropy increased from 7.4168 for the cover images to 7.5288 after data embedding, indicating improved randomness and enhanced resistance to statistical analysis while maintaining high image quality. The developed adaptive threshold-based region selection mechanism consistently identified suitable complex regions for embedding, thereby achieving high embedding capacity without introducing noticeable visual artifacts.

The successful recovery of the embedded secret information from all stego images confirms the effectiveness of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (EBPCS) techniques for high-capacity image steganography. Figures 4.7 to 4.9 illustrate the secret data extraction performance of the developed techniques across the 30 simulation runs using the selected evaluation metrics.

Table 4.4 summarizes the overall performance of the developed AT-EBPCS framework across the embedding and extraction stages and provides a concise overview of the evaluation metrics obtained during the implementation.

Table 4.3: Extraction Phase Results across 30 Simulations.

Images	Time (s)	PSNR (dB)
1	1.33	48.67
2	1.39	49.02
3	1.41	49.28

4	1.45	49.56
5	1.36	48.89
6	1.43	49.34
7	1.48	49.67
8	1.30	48.45
9	1.40	49.15
10	1.49	49.78
11	1.34	48.78
12	1.42	49.3
13	1.50	49.89
14	1.28	48.34
15	1.44	49.43
16	1.47	49.59
17	1.37	48.94
18	1.40	49.20
19	1.51	49.92
20	1.25	48.12
21	1.42	49.32
22	1.48	49.72
23	1.35	48.82
24	1.39	49.08
25	1.52	49.98
26	1.31	48.56
27	1.43	49.38
28	1.46	49.52
29	1.38	48.98
30	1.4	49.12

Table 4.4: Overall Performance Evaluation of the Developed AT-EBPCS Framework

Phase	Metric	Mean	Std Dev	Min	Max
Embedding	Payload Ratio (%)	23.48	1.66	20.78	26.41
	PSNR (dB)	50.75	0.97	48.98	52.45
Extraction	PSNR (dB)	49.22	0.52	48.12	49.98

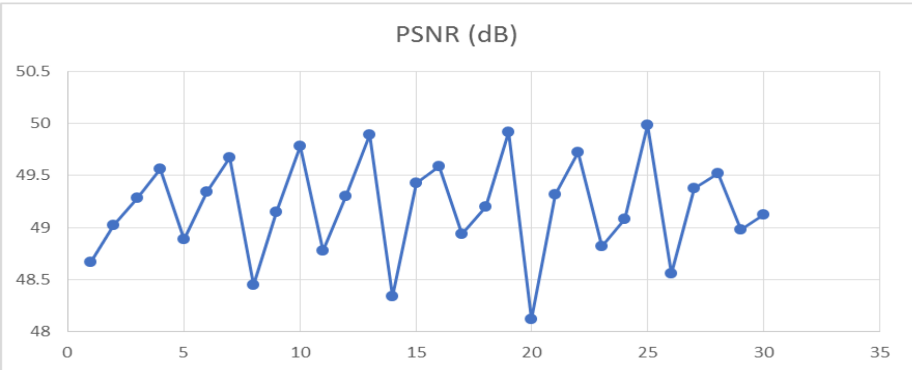

Figure 4.7: PSNR of the Recovered Stego Image.

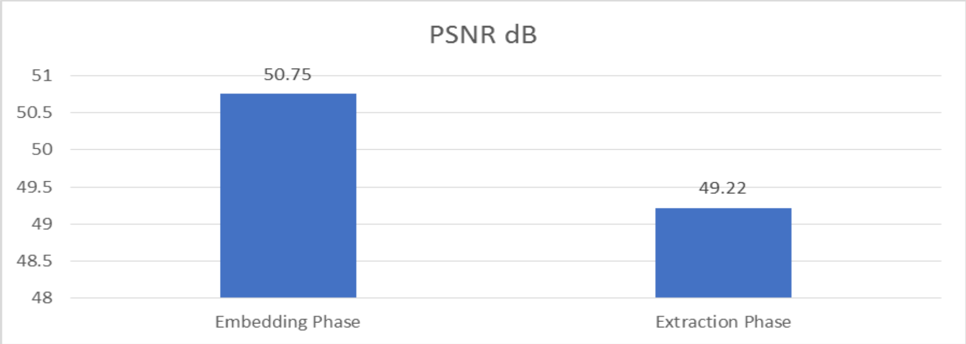

Figure 4.8: Average PSNR Analysis.

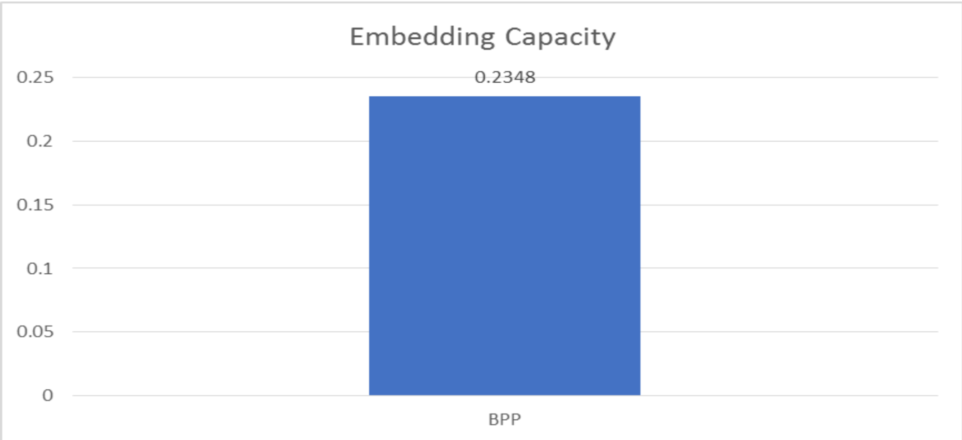

Figure 4.9: Average Embedding Capacity (bpp).

4.2 Comparative Analysis with Existing Methods

Table 4.5 presents a comparative evaluation of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques against conventional BPCS and other existing BPCS-based image steganography techniques reported in the literature. The results demonstrate that the developed techniques achieved improved performance across the selected evaluation metrics. In particular, the average Peak Signal-to-Noise Ratio (PSNR) of 50.75 dB exceeded the 42.00 dB reported by Chandra Sekhar et al. (2018) for the conventional BPCS techniques and the 38.00 dB reported by Nwankwo et al. (2023) for AES+BPCS-based image steganography techniques. This improvement can be attributed to the adaptive threshold-based region selection mechanism, which dynamically identifies the most suitable complex image regions for secret data embedding, thereby preserving the visual quality of the cover image.

Furthermore, the developed AT-EBPCS techniques achieved an average payload ratio of 23.48%, representing an improvement over the 21.00% reported by Chandra Sekhar et al. (2018) and the 19.20% reported by Nwankwo et al. (2023), while maintaining superior image quality. The Shannon entropy analysis also showed an increase in the average entropy from 7.4168 for the cover images to 7.5288 for the stego images, representing an average increase of 0.112. This increase indicates improved randomness of the stego images and enhanced resistance to statistical analysis without introducing noticeable visual distortion. These findings demonstrate that the adaptive threshold based-enhancement of the conventional BPCS techniques significantly improves embedding capacity, visual imperceptibility, and statistical security, making it suitable for high-capacity image steganography applications.

Table 4.5: Comparison of AT-EBPCS with Existing Methods.

Technique/ Model	Optimization Strategy	PSNR (dB)	P-ayload Ratio (%)	Reference
BPCS Steganography	Fixed Threshold	42	21	Chandra Sekhar *et al.* (2018)
AES+BPCS	AES + BPCS	38	19.2	Nwankwo *et al.* (2023)
AT-EBPCS (Developed)	Adaptive Threshold	50.75	23.48	This Study

5.0 CONCLUSION

This study developed an Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques for high-capacity image steganography. The conventional Bit Plane Complexity Segmentation (BPCS) techniques was enhanced using an adaptive threshold-based region selection mechanism to dynamically identify optimal complex image regions for secret data embedding, thereby improving embedding capacity while preserving the visual quality of the stego image.

The developed AT-EBPCS techniques achieved an average Peak Signal-to-Noise Ratio (PSNR) of 50.75 dB, a payload ratio of 23.48%, and an average Shannon entropy of 7.5288, demonstrating high embedding capacity, excellent visual imperceptibility, and improved statistical security. Comparative analysis showed that the developed techniques outperformed conventional BPCS and other existing BPCS-based image steganography techniques in terms of image quality and embedding capacity. The adaptive threshold-based region selection mechanism effectively identified suitable embedding regions according to the local complexity characteristics of image blocks, resulting in improved embedding performance without introducing noticeable visual distortion.

The study therefore concludes that the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques provides an effective and efficient approach for high-capacity image steganography, making it suitable for secure information hiding and transmission while maintaining the visual fidelity of the cover image.

5.2 Recommendations

The developed Adaptive Threshold-Based Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques is recommended for applications requiring secure and high-capacity image steganography while maintaining high image quality. Future studies should investigate the integration of intelligent optimization or machine learning techniques to further improve the adaptive threshold selection process and enhance embedding performance under varying image characteristics. Additionally, evaluation using larger and more diverse image datasets, including natural, medical, satellite, and remote sensing images, is recommended to assess the scalability, robustness, and general applicability of the developed techniques. Future research may also consider extending the proposed techniques to colour images, video steganography, and real-time multimedia communication applications.

5.3 Contributions to Knowledge

This study contributes to knowledge through the following:

i. The development of an Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques that incorporates an adaptive threshold-based region selection mechanism for improved identification of suitable complex image regions, resulting in enhanced embedding capacity while preserving the visual quality of the stego image.

ii. The implementation and validation of the developed Adaptive Threshold Based-Enhanced Bit Plane Complexity Segmentation (AT-EBPCS) techniques, which achieved superior image quality and higher payload capacity compared with existing BPCS-based image steganography techniques.

REFERENCES

1. Abadin, A. M., Al-Janabi, S., Al-Omary, A., & Hasan, R. *A comprehensive review of image steganography techniques: Challenges, advances, and future directions*. Journal of Information Security and Applications, 2024; 81: 103744. https://doi.org/10.1016/j.jisa.2024.103744
2. Alotaibi, M. S., & Almutairi, F. M. Secure multimedia communication in distributed computing environments: Challenges and emerging solutions. *Journal of King Saud*

University – Computer and Information Sciences, 2022; *34*(10): 8954–8968. https://doi.org/10.1016/j.jksuci.2021.11.009

3. Aziz, A., & Khan, M. A. A survey of secure image communication and privacy preservation techniques. *Multimedia Tools and Applications*, 2023; *82*(18): 28267–28306. https://doi.org/10.1007/s11042-023-14862-7.
4. Aziz, M., Rahman, S., and Khan, A. Reversible data hiding in encrypted images sing differential evolution and homomorphic encryption. *Signal Processing: Image Communication*, 2023; 110: 116857. https://doi.org/10.1016/j.image.2023.116857
5. Hurtado-Guarnizo, O., and Duarte-Gonzalez, M. E. Study of somewhat homomorphic encryption scheme for image erosion and dilation. *2018 IEEE Colombian Conference on Communications and Computing*, COLCOM 2018 - Proceedings. https://doi.org/10.1109/ColComCon.2018.8466717
6. Kawaguchi, E., & Eason, R. O. *Principle and applications of BPCS steganography*. In *Proceedings of SPIE 3528: Multimedia Systems and Applications*, 1999; 464–473. SPIE. https://doi.org/10.1117/12.338094
7. Ke, Y., Zhang, M., Su, T., & Yang, Y. Adaptive image steganography based on Bit-Plane Complexity Segmentation. *Multimedia Tools and Applications*, 2018; *77*(13): 16789–16812.
8. Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., and Alzuabidi, H. M. Combination of Steganography and Cryptography: *A short Survey. IOP Conference Series: Materials Science and Engineering*, 2019; 518(5). https://doi.org/10.1088/1757-899X/518/5/052003
9. Zhang, Y., Li, X., and Wang, S. Secure cloud data sharing using encryption and steganography integration. *Future Generation Computer Systems*, 2022; 131: 123–135. https://doi.org/10.1016/j.future.2022.01.012