Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

Secure Medical Data Transmission Using S-DES Encryption and Pixel Value Differencing-Based Steganography

Tarik Fraraj Idbeaa [1 *], Ghofran Omran Almakhzoum [2], Fatimah Salem Elfandi [3]
[1] Department of Computer Science, Faculty of Science, University of Gharyan, Gharyan, Libya, Tarik.idbeaa@gu.edu.ly
[2] Department of Information Technology, University of Tripoli Alahlia, Tripoli, Libya
[3] Department of Information Technology, University of Tripoli Alahlia, Tripoli, Libya

[*] *Corresponding author:* Tarik.idbeaa@gu.edu.ly

Received: 30 Aug 2026	Accepted: 15 Sep 2026	Published: 25 Sep 2026

Abstract

The secure transmission of medical information requires effective protection of sensitive patient data while preserving the quality of medical images. This study proposes a hybrid data-hiding framework that combines Simplified Data Encryption Standard (S-DES) encryption with Pixel Value Differencing (PVD) steganography. Sensitive medical data are first encrypted using an 8-bit block and a 10-bit secret key, and the resulting ciphertext is then adaptively embedded into medical computed tomography (CT) images. The proposed framework was evaluated using brain, abdominal, and chest CT images with payloads ranging from 100 Bytes to 1 KB. Image quality and embedding performance were assessed using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Normalized Absolute Error (NAE), Average Difference (AD), and Structural Content (SC), while data-recovery reliability was evaluated using the Bit Error Rate (BER). The experimental results demonstrate high structural similarity between the original and stego images, with NAE and AD values remaining close to zero and SC values approximately equal to one. Increasing the payload resulted in the expected increase in MSE and decrease in PSNR, while maintaining limited image distortion within the investigated range. A BER of 0.00 was obtained for most recovered data, and 100% recovery was achieved under the evaluated compression condition. The results indicate that the proposed S-DES–PVD framework provides an effective combination of data confidentiality, embedding imperceptibility, and reliable data recovery for secure medical image data transmission.

Keywords: Medical Image Security, Steganography, Pixel Value Differencing, S-DES, Data Hiding, Medical CT Images, Telemedicine, Image Quality, Data Recovery

1. Introduction

The rapid development of information and communication technologies has significantly increased the use of digital systems and communication networks for storing, processing, and exchanging sensitive information. In healthcare environments, the widespread adoption of electronic medical records and digital medical imaging has created an increasing need for

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

reliable mechanisms capable of protecting confidential information against unauthorized access, interception, modification, and misuse.

Cryptography represents one of the fundamental approaches to information security and provides essential security services, including confidentiality, integrity, authentication, and non-repudiation. Cryptographic techniques transform plaintext into unintelligible ciphertext that can only be recovered by an authorized entity possessing the appropriate key. Hash functions can further support data integrity by enabling the detection of unauthorized modifications [1], [2].

Although encryption provides strong protection for the content of sensitive information, the transmission of encrypted data may itself attract attention because the existence of confidential communication remains apparent. Information hiding, particularly digital steganography, addresses this limitation by concealing secret information within an apparently innocuous digital carrier, such as an image, audio signal, or video [3], [4].

This concept is particularly relevant to healthcare applications. Medical information may contain personally identifiable information, patient histories, diagnostic findings, laboratory results, and medical images. Unauthorized disclosure or manipulation of such information may compromise patient privacy and potentially affect the reliability of healthcare services. Consequently, secure mechanisms for storing and transmitting medical information are required to preserve both confidentiality and data integrity [5].

Medical images present an attractive carrier for information hiding because of their large data volume and spatial redundancy. However, medical image steganography introduces an additional requirement that distinguishes it from conventional image data hiding: modifications introduced by the embedding process should remain sufficiently small to preserve the visual and structural characteristics of the image. This requirement is particularly important when the host image has diagnostic significance.

Motivated by these requirements, this study proposes a hybrid medical data-hiding framework that combines S-DES encryption with PVD-based steganography. Sensitive medical information is first encrypted and subsequently embedded into selected CT images using adaptive pixel-value differences. The proposed framework is evaluated in terms of image quality, payload size, file-size variation, data-recovery accuracy, and robustness under the investigated processing condition.

The main contributions of this study are as follows:

i. A hybrid framework combining S-DES encryption and PVD-based steganography for medical data hiding is developed.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

ii. Medical CT images representing different anatomical regions are employed to investigate the influence of host-image characteristics on embedding performance.

iii. The effect of different payload sizes on image quality is quantitatively evaluated using PSNR, MSE, NAE, AD, and SC.

iv. The effect of data embedding on medical image file size is investigated.

The reliability of data extraction is evaluated using BER, together with robustness assessment under the investigated compression condition.

2. Related Work

Medical imaging comprises a broad range of techniques used to acquire anatomical and functional representations of the human body for diagnostic, therapeutic, and research purposes [6]. Modern medical imaging modalities include computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, nuclear medicine, positron emission tomography (PET), and other specialized imaging technologies.

Medical image processing commonly involves operations such as segmentation, enhancement, feature extraction, and registration. Image segmentation is particularly important because it divides an image into meaningful regions and facilitates subsequent processing and analysis [7]. The structural characteristics and local statistical properties of medical images also make them suitable for selected information-hiding techniques.

Several studies have investigated reversible and non-reversible data-hiding approaches for protecting medical information. Reversible Data Hiding (RDH) techniques are particularly attractive in medical applications because they allow the original image to be completely recovered after the hidden information has been extracted.

Ni et al. [8] proposed a reversible data-hiding method based on histogram shifting. The technique exploits the statistical characteristics of image pixels and uses the distribution of pixel values to embed secret information while enabling recovery of the original image. Such approaches are particularly relevant to medical applications where preservation of the original diagnostic image is essential.

Kuo et al. [9] investigated an approach combining data hiding with lossless compression for secure transmission of medical information. Their framework embeds textual information into a medical image and subsequently applies Run-Length Encoding (RLE) to improve transmission efficiency. The reverse process allows both the hidden information and the

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

original image to be recovered.

Aharon et al. [10] proposed a high-capacity reversible approach based on Pixel-to-Block transformation. The method integrates watermarking and block-checksum mechanisms to detect and localize tampered regions. Intermediate Significant Bit Substitution (ISB) was employed to address limitations associated with conventional Least Significant Bit (LSB) substitution, while chaotic mechanisms were used for the encryption of electronic health records and clinical information.

Chang et al. [11] proposed a data-hiding method based on a Magic Cube generated using a magic matrix. The technique embeds nine secret bits into groups of four pixels and employs secret keys to scramble pixel values. The reported method achieved an embedding capacity of approximately 2.25 bits per pixel (bpp) and an average PSNR of approximately 44 dB.

Although these studies demonstrate the feasibility of combining image processing, encryption, and data hiding for medical applications, the trade-off among payload capacity, image quality, structural preservation, and data recovery remains an important research consideration. Accordingly, the present study investigates a hybrid framework based on S-DES encryption and PVD steganography and evaluates its behavior across different medical CT images and payload sizes.

3. Material and Methods

A. Proposed System Architecture

The proposed framework integrates cryptographic protection and spatial-domain steganography into a sequential processing pipeline. The overall system consists of the following stages:

i. Selection and preparation of the medical CT image.
ii. Preparation and validation of the confidential medical information.
iii. Conversion of the secret information into binary form.
iv. Encryption of the binary data using S-DES.
v. Embedding of the encrypted bitstream into the CT image using PVD.
vi. Generation and storage of the resulting stego image.
vii. Subjective and objective assessment of image quality.
viii. Extraction of the encrypted information using the inverse PVD procedure.
ix. Decryption of the extracted data using S-DES and the shared secret key.
x. Comparison of the recovered information with the original information to verify successful recovery.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

This architecture provides two complementary security layers. The encryption layer protects the semantic content of the confidential information, whereas the steganographic layer conceals the existence of the encrypted information within the medical image.

B. System Development Environment

The proposed system was implemented and experimentally evaluated using MATLAB R2015a. MATLAB was selected because of its capabilities in digital image processing, matrix manipulation, numerical computation, algorithm implementation, and Graphical User Interface (GUI) development.

The implementation includes functions for loading and displaying medical images, analyzing image characteristics, converting textual information into binary representation, performing S-DES encryption and decryption, embedding and extracting information using PVD, generating stego images, and calculating image-quality metrics.

The implemented system also provides automated computation of PSNR, MSE, NAE, AD, SC, embedding time, and BER, enabling systematic comparison between the original and stego images.

C. Medical Image Dataset and Selection Criteria

The selection of the medical image as the host medium is an important component of the proposed framework because image dimensions, anatomical structure, contrast, and local pixel variations directly influence embedding behavior.

A set of medical CT images representing three anatomical regions—brain, abdomen, and chest—was selected for the experimental evaluation. The selected images differ in their spatial dimensions, anatomical structures, intensity distributions, and local variations, as illustrated in Figure 1.

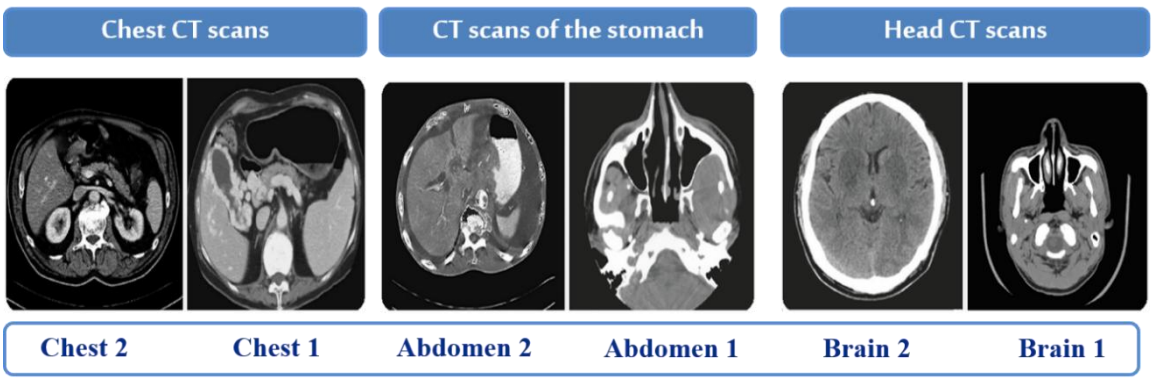


Figure 1: Medical CT images selected for evaluating the proposed data-hiding framework.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

The selected images were analyzed according to several characteristics, including image dimensions, anatomical structure, local intensity variations, contrast, smooth regions, pixel-value distribution, and potential embedding capacity.

D. Secret Data Preparation

The secret information consists of medical text and patient-related data entered through the system interface. Prior to encryption and embedding, the input information is checked for completeness and validity.

The confidential information is not embedded in its original textual form. Instead, it is converted into a binary representation suitable for cryptographic processing. The resulting binary data are then encrypted using S-DES before being passed to the steganographic embedding stage.

E. S-DES-Based Data Encryption

The cryptographic stage provides the first security layer of the proposed framework. S-DES operates on 8-bit plaintext blocks using a shared 10-bit secret key.

Let Pdenote an 8-bit plaintext block and Kdenote the 10-bit secret key. The ciphertext $C$is generated as:

$$C = E_{S-DES}(P, K) \quad (1)$$

where E_{S-DES} denotes the S-DES encryption function.

The resulting ciphertext blocks constitute the secret payload subsequently embedded into the medical image using PVD.

At the receiver side, the ciphertext is recovered and decrypted using the corresponding 10-bit secret key:

$$P = D_{S-DES}(C, K) \quad (2)$$

where D_{S-DES}denotes the S-DES decryption function.

F. PVD-Based Data Embedding

Following encryption, the ciphertext is converted into a continuous binary stream and embedded into the selected medical CT image using the Pixel Value Differencing (PVD) technique. The overall workflow of the proposed S-DES–PVD framework, including encryption, ciphertext generation, PVD-based embedding, stego-image generation, and subsequent evaluation, is illustrated in Figure 2.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

PVD exploits the intensity difference between neighboring pixels to determine the amount of information that can be embedded. Smoother regions generally exhibit smaller pixel differences, whereas edge and high-contrast regions exhibit larger differences. This adaptive characteristic enables the embedding process to distribute secret information according to local image properties.

The embedding procedure consists of:

i. Loading the selected medical CT image.
ii. Converting the encrypted ciphertext into a binary bitstream.
iii. Partitioning the image into neighboring-pixel pairs.
iv. Calculating the intensity difference between each pair.
v. Determining the embedding capacity according to the corresponding pixel difference.
vi. Embedding the encrypted bits by modifying pixel values.
vii. Generating and storing the stego image.

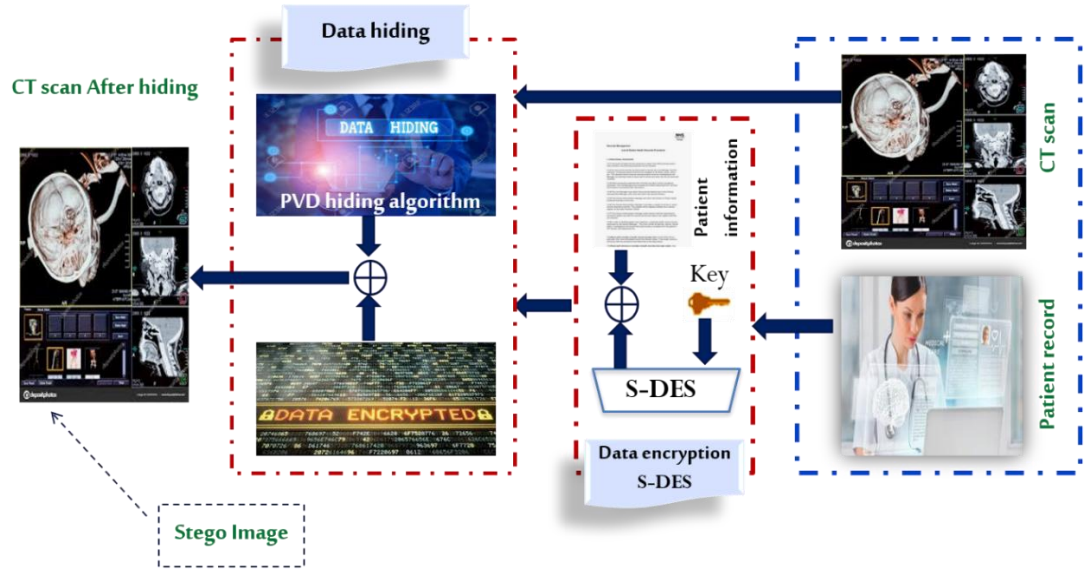


Figure 2: Overall workflow of the proposed S-DES–PVD medical image data-hiding framework.

G. Data Extraction

The inverse PVD procedure is applied to the stego image to recover the embedded encrypted bitstream. The general extraction process is illustrated in Figure 3, where the stego image is processed without requiring the original cover image.

The stego image is loaded into the system, and the inverse PVD procedure is applied to recover the embedded encrypted bitstream.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

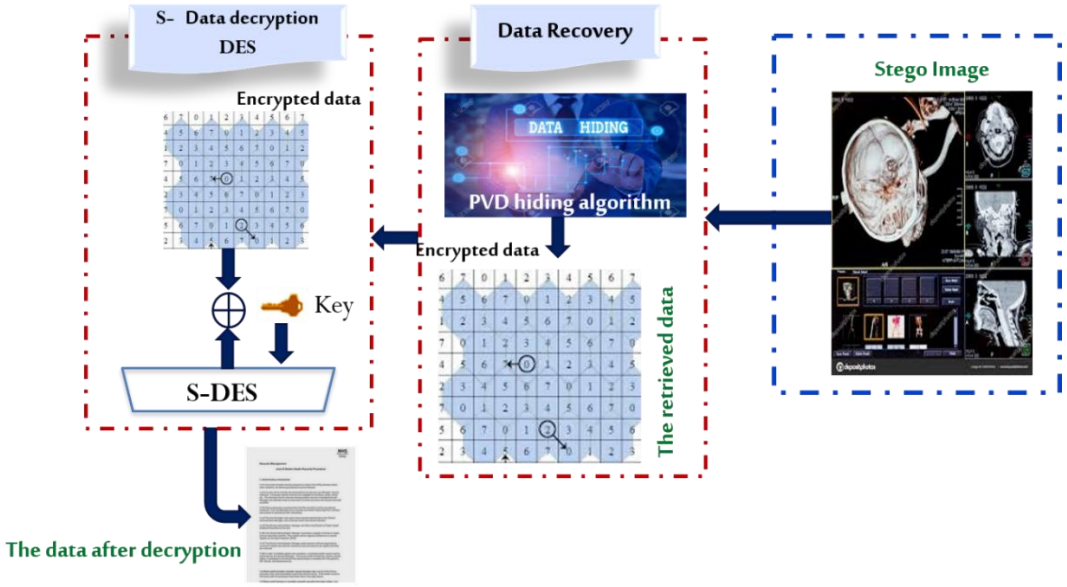


Figure 3: General framework of encrypted data extraction from the stego medical CT image.

The extracted information remains encrypted at this stage and is subsequently passed to the S-DES decryption stage.

H. Image Quality Assessment

Because medical images may contain diagnostically significant information, evaluating the effect of data embedding on image quality is essential. The quality of each stego image was assessed by comparing it with its corresponding original cover image.

The evaluation included subjective visual inspection and objective quantitative analysis using:

- Mean Squared Error (MSE);
- Peak Signal-to-Noise Ratio (PSNR);
- Normalized Absolute Error (NAE);
- Average Difference (AD); and
- Structural Content (SC).

In addition, embedding time and file-size variation were recorded.

I. S-DES-Based Data Decryption

The extracted ciphertext is decrypted using S-DES and the same 10-bit secret key used during encryption:

$$P = D_{S-DES}(C, K) \quad (3)$$

Following extraction, the recovered ciphertext is decrypted using S-DES and the same 10-bit secret key employed during encryption.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

J. Experimental Procedure

The experiments were conducted using the selected medical CT images according to a standardized procedure:

i. Select and characterize the medical CT image.
ii. Enter and validate the confidential medical information.
iii. Convert the input information into binary form.
iv. Encrypt the binary data using S-DES.
v. Embed the encrypted bitstream using PVD.
vi. Generate and save the stego image.
vii. Calculate the selected image-quality metrics.
viii. Repeat the experiment using different payload sizes.
ix. Extract the encrypted data using inverse PVD.
x. Decrypt the extracted information using the shared key.
xi. Compare the recovered information with the original information.
xii. Calculate BER to quantify data-recovery accuracy.

The investigated payload sizes were 100 Bytes, 300 Bytes, 500 Bytes, 700 Bytes, and 1 KB

4. Results and Discussion

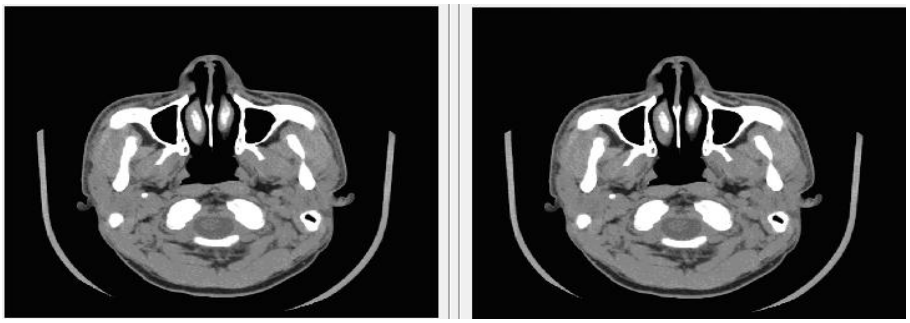
A. Subjective Assessment of Medical Image Quality

The first stage of evaluation focused on the visual effect of embedding encrypted information into the selected medical CT images. The visual quality of the stego images was initially evaluated by comparing the original CT images with their corresponding embedded versions. The brain CT images before and after data embedding are presented in Figure 4, while the corresponding abdominal and chest CT images are shown in Figures 5 and 6, respectively.

Visual inspection of Figures 4–6 reveals no apparent differences between the original and stego images. No clearly visible artifacts or substantial distortion were observed following the embedding process.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

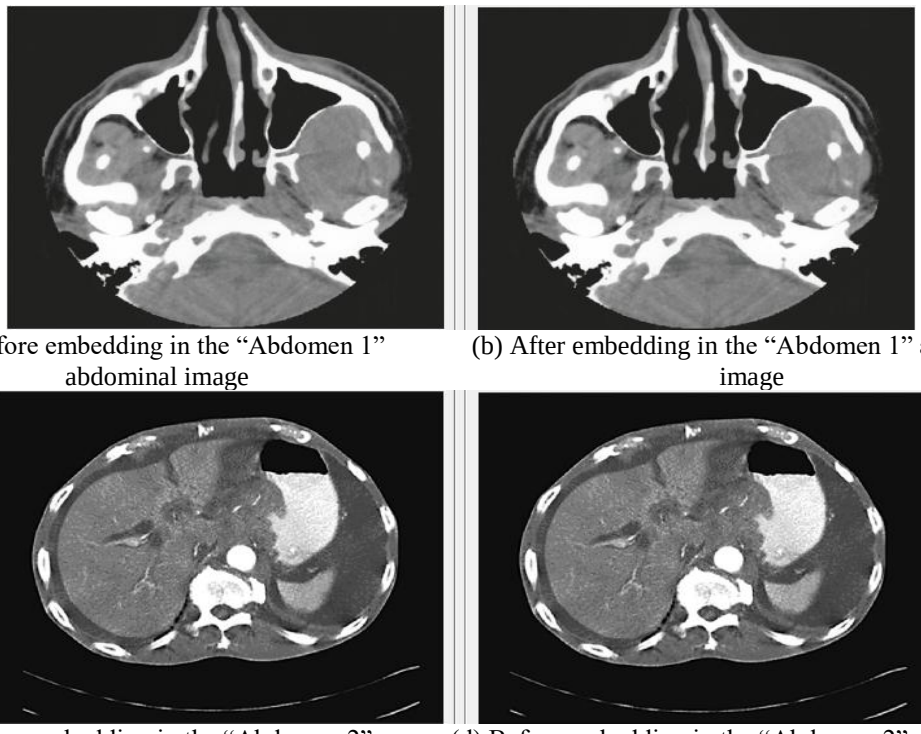
Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly



(a) Before embedding in the "Brain1" head image (b) After embedding in the "Brain1" head image

(c) Before embedding in the "Brain2" head image (d) After embedding in the "Brain2" head image

Figure 4: Brain CT images (Brain 1 and Brain 2) before and after data embedding.



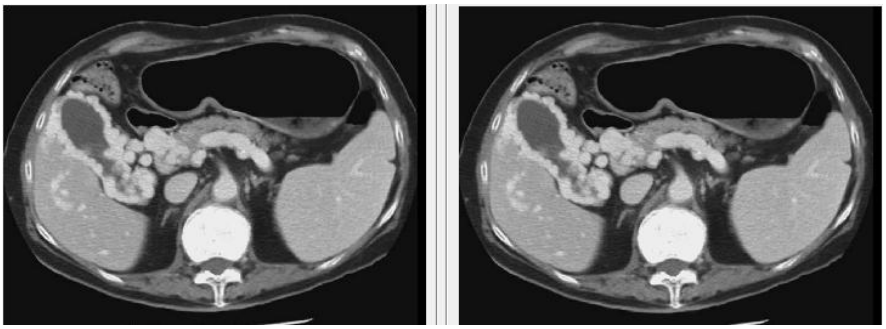
(a) Before embedding in the "Abdomen 1" abdominal image (b) After embedding in the "Abdomen 1" abdominal image

(c) Before embedding in the "Abdomen 2" abdominal image (d) Before embedding in the "Abdomen 2" abdominal image

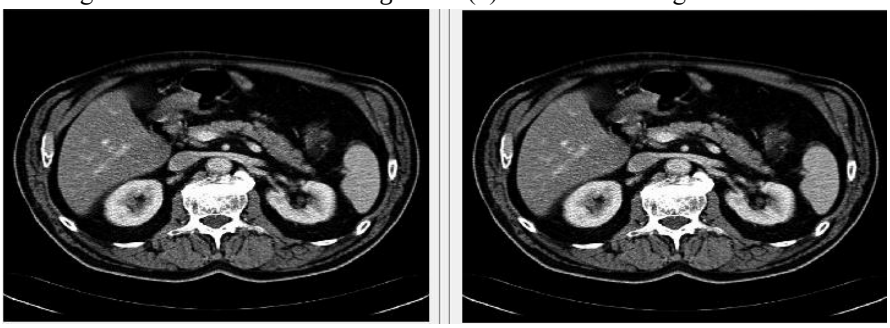
Figure 5: Abdominal CT images (Abdomen 1 and Abdomen 2) before and after data embedding.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly



(a) Before embedding in the "Chest 1" chest image (b) After embedding in the "Chest 1" chest image



(c) Before embedding in the "Chest 2" chest image (d)) After embedding in the "Chest 2" chest image

Figure 6: Chest CT images (Chest 1 and Chest 2) before and after data embedding.

These observations indicate that the proposed PVD-based embedding mechanism preserves the principal visual characteristics of the host medical images under the investigated conditions.

B. Objective Image Quality Assessment

A payload of 1 KB was embedded into each selected CT image to quantitatively evaluate the effect of data embedding. The resulting PSNR values for the investigated CT images are presented in Figure 7.

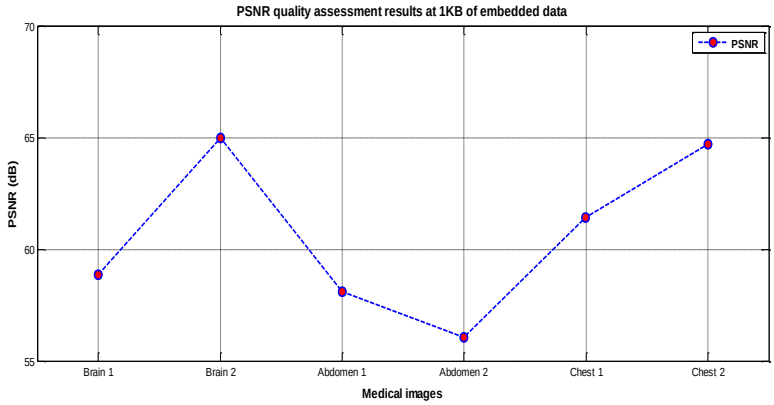


Figure 7: PSNR values obtained for the selected medical CT images after embedding 1 KB of encrypted data.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

I. PSNR Analysis

As shown in Figure 7, the PSNR response varied among the investigated medical images. For the brain CT images, the PSNR value of Brain 1 was 6.10 dB lower than that of Brain 2. For the abdominal CT images, Abdomen 1 exhibited a PSNR value 2.03 dB higher than Abdomen 2. For the chest CT images, the PSNR value of Chest 1 was 3.28 dB lower than that of Chest 2. These differences indicate that the impact of embedding depends not only on payload size but also on the structural and statistical characteristics of the host image.

II. NAE Analysis

The NAE results for the selected CT images are presented in Figure 8. For a payload of 1 KB, the NAE values ranged from 0.0000847736 to 0.0009770460, indicating small deviations between the original and stego images.

The abdominal CT images exhibited comparatively greater sensitivity to the embedding process, which may be associated with their anatomical complexity and variations in pixel intensity, brightness, and local contrast.

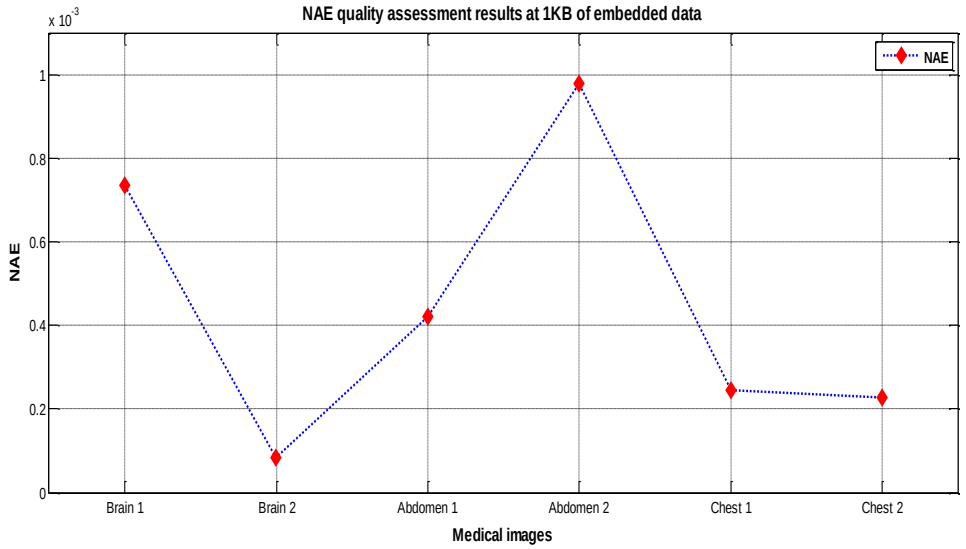


Figure 8: NAE values obtained for the selected medical CT images after embedding 1 KB of encrypted data.

III. AD Analysis

The AD metric was used to quantify the average pixel-level difference between the original and stego images are presented in Figure 9. The obtained AD values were approximately 0.00 across the investigated images, indicating that the embedding process introduced only limited pixel-level modifications.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

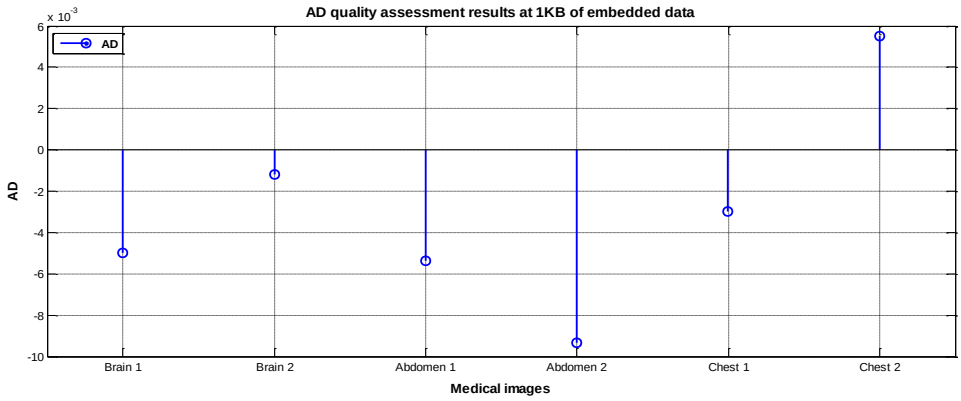


Figure 9: AD values obtained for the selected medical CT images after embedding 1 KB of encrypted data.

IV. SC Analysis

The SC results are presented in Figure 10. The obtained values were close to 1 for the investigated images, indicating a high degree of structural similarity between the original and stego images.

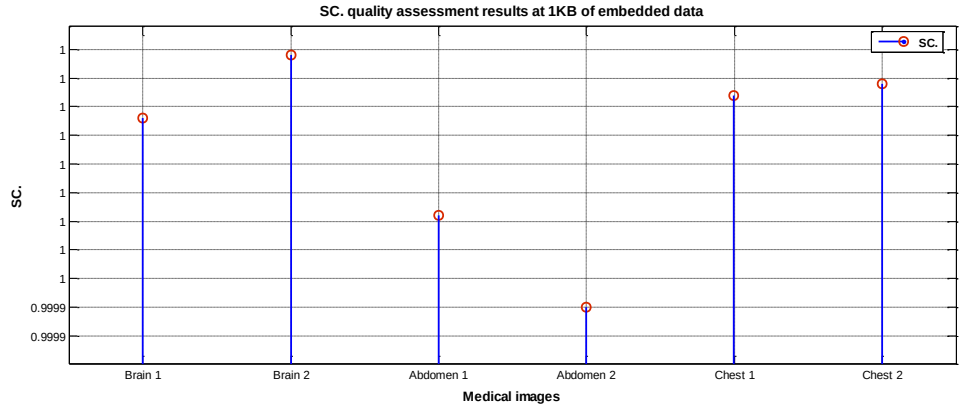


Figure 10: SC values obtained for the selected medical CT images after embedding 1 KB of encrypted data.

The combination of low NAE and AD values with SC values close to unity provides quantitative evidence that the proposed method introduces limited structural modifications under the investigated conditions.

V. Effect of Payload Size on Medical Image Quality

Five payload sizes—100 Bytes, 300 Bytes, 500 Bytes, 700 Bytes, and 1 KB—were investigated to determine the relationship between payload size and image quality.

a) Effect on PSNR and MSE

The variation of PSNR with payload size for the selected medical CT images is presented in

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

Figure 11. As shown in the figure, increasing the embedded payload generally resulted in an increase in MSE and a corresponding decrease in PSNR.

For Brain 1, increasing the payload from 100 Bytes to 1 KB resulted in an approximate 10 dB decrease in PSNR. A similar trend was observed for the other investigated CT images.

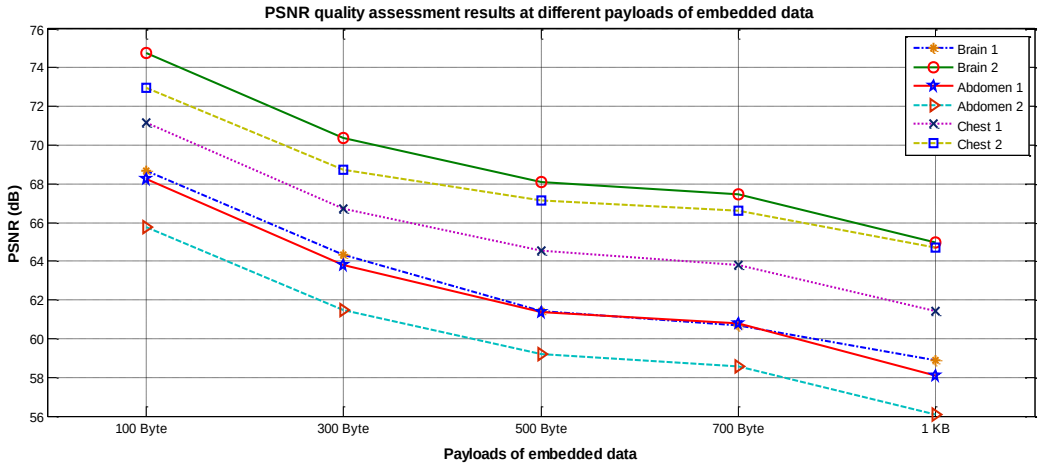


Figure 11: PSNR values for different payload sizes in the selected medical CT images.

b) Effect on NAE

The NAE variation as a function of payload size is presented in Figure 12. The NAE values remained close to zero across the investigated payload sizes, ranging from approximately 0.00008 to 0.00098.

These results indicate that the embedding process introduced relatively small deviations from the original images within the investigated payload range.

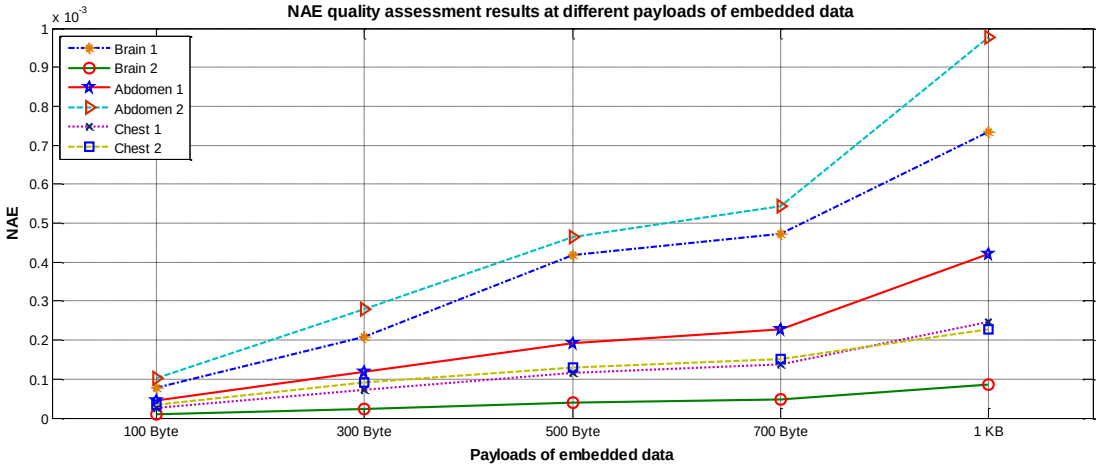


Figure 12: NAE values for different payload sizes in the selected medical CT images.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

c) Effect on AD

The relationship between AD and payload size is shown in Figure 13. The AD values increased gradually with payload size and ranged from 0.000127294 to 0.00328064. Although the increase indicates additional pixel-level modifications at larger payloads, the overall magnitude remained relatively small.

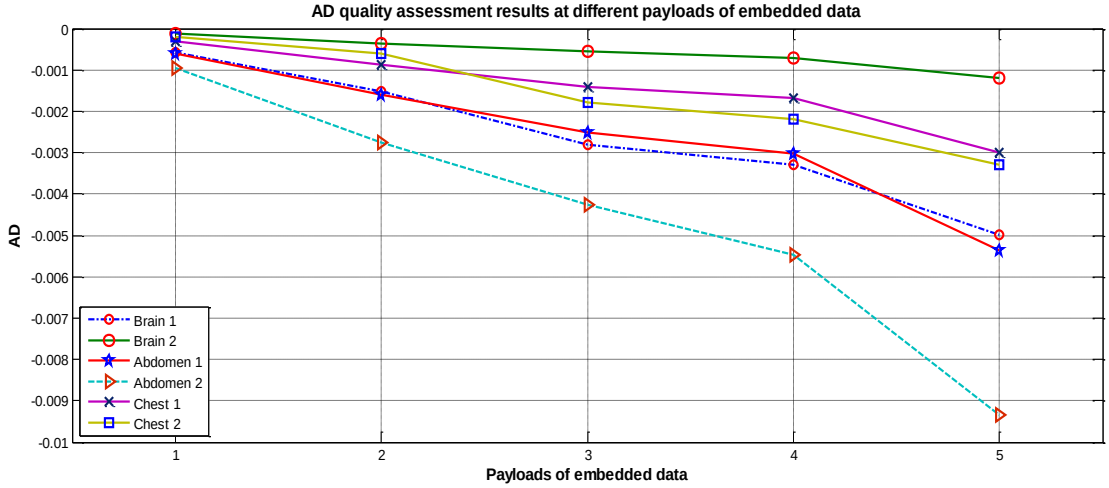


Figure 13: AD values for different payload sizes in the selected medical CT images.

d) Effect on SC

The SC values obtained for the different payload sizes are presented in Figure 14. The values remained approximately equal to 1 across the investigated payload range, with only a slight reduction observed at the largest payload of 1 KB.

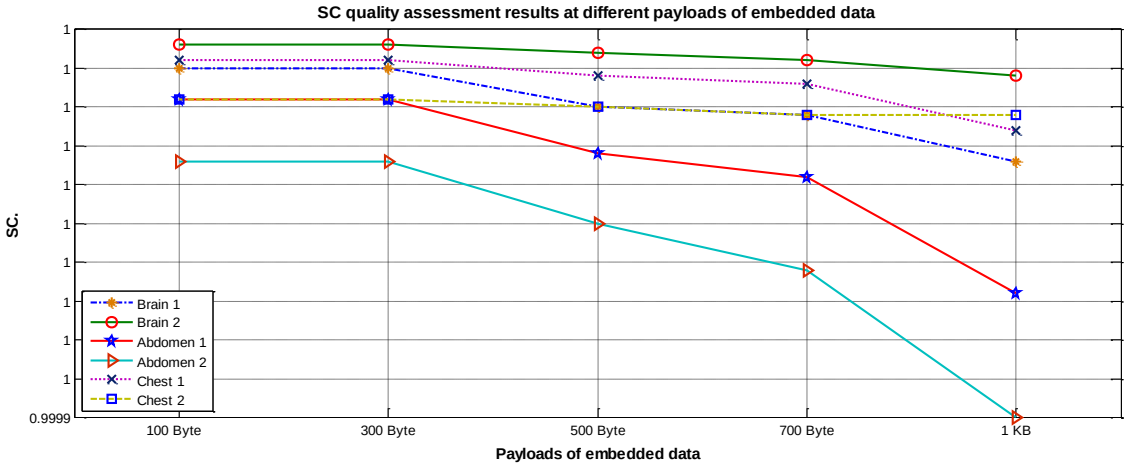


Figure 14: SC values for different payload sizes in the selected medical CT images.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

Overall, the results presented in Figures 11–14 demonstrate that increasing the payload produces measurable image modifications while maintaining high structural similarity within the investigated range.

VI. Effect of Data Embedding on Medical Image File Size

The effect of embedding 1 KB of encrypted data on file size is summarized in Table 1.

Table 1 Effect of 1 kb data embedding on medical CT image file size

Medical CT Image	Original File Size	File Size After Embedding	Percentage Change
Brain 1	76 KB	73.3 KB	%−3.55
Brain 2	496 KB	537 KB	%+8.27
Abdomen 1	185 KB	181 KB	%−2.16
Abdomen 2	89 KB	97.8 KB	%+9.88
Chest 1	238 KB	251 KB	%+5.46
Chest 2	424 KB	419 KB	%−1.18

As shown in Table I, data embedding does not necessarily produce a uniform change in file size. Brain 1, Abdomen 1, and Chest 2 exhibited decreases in file size, whereas Brain 2, Abdomen 2, and Chest 1 exhibited increases. This variation may be related to the characteristics and internal representation of the host images and the resulting modifications introduced by the embedding operation.

VII. Robustness and Data-Recovery Analysis

The robustness of the proposed framework was evaluated using the Bit Error Rate (BER) of the recovered data:

$$BER = \frac{N_{\text{error}}}{N_{\text{total}}} \tag{4}$$

where N_{error}denotes the number of incorrectly recovered bits and N_{total}denotes the total number of embedded bits.

A BER of 0.00 was obtained for most of the recovered data, indicating accurate extraction under the investigated conditions.

The robustness evaluation further showed that the proposed scheme achieved 100% recovery under the evaluated compression condition. This result indicates that the embedded information remained recoverable under the specific compression test applied in the experiment.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

However, this finding should be interpreted within the scope of the investigated attack and experimental parameters. A comprehensive robustness assessment would require additional tests involving different compression levels and other image-processing attacks.

VIII. Overall Discussion

The experimental results demonstrate that the proposed S-DES–PVD framework provides two complementary security layers. S-DES protects the semantic content of the confidential medical information, whereas PVD conceals the encrypted information within the spatial domain of the medical image.

The low NAE and AD values and the SC values close to unity indicate that the structural characteristics of the host images were largely preserved. At the same time, the decrease in PSNR with increasing payload confirms the expected trade-off between embedding capacity and image distortion.

The results also indicate that host-image characteristics influence embedding performance. Images with greater local intensity variation and complex anatomical structures may respond differently to embedding compared with relatively homogeneous images.

The recovery results further demonstrate the feasibility of the proposed framework. The low BER values indicate accurate data extraction under the investigated conditions, while the compression experiment demonstrated successful recovery under the specific evaluated compression condition.

5. Conclusion

This study presented a hybrid framework for secure medical information transmission based on the integration of Simplified Data Encryption Standard (S-DES) encryption and Pixel Value Differencing (PVD) steganography. The proposed framework encrypts confidential medical information before embedding it into selected medical CT images, thereby providing complementary protection of the information content and its presence within the host image.

The experimental evaluation was performed using brain, abdominal, and chest CT images with payload sizes ranging from 100 Bytes to 1 KB. The results demonstrated a high degree of visual and structural similarity between the original and stego images. In particular, the NAE and AD values remained close to zero, whereas the SC values remained approximately equal to unity, indicating limited pixel-level and structural modifications.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Increasing the payload resulted in the expected increase in MSE and decrease in PSNR. Nevertheless, the structural similarity remained high throughout the investigated payload range. The effect of embedding on file size varied among the selected images, indicating that file-size behavior depends on the characteristics and internal representation of the host image.

Regarding data recovery, a BER of 0.00 was obtained for most recovered data, demonstrating accurate extraction under the investigated conditions. In addition, 100% recovery was achieved under the evaluated compression condition, indicating successful recovery of the embedded information under that specific test scenario.

Overall, the findings demonstrate the feasibility of combining S-DES encryption with PVD-based steganography for protecting sensitive medical information while preserving the quality and structural characteristics of medical CT images. The proposed framework therefore represents a potential approach for secure medical data storage and transmission under the experimental conditions investigated in this study.

Future work should extend the evaluation to larger and more diverse medical-image datasets and additional modalities, including MRI and ultrasound. Further investigations should also consider higher payload capacities, computational complexity, advanced cryptographic algorithms, and comprehensive robustness testing against compression, filtering, noise, geometric transformations, and other relevant attacks. Comparative experiments with state-of-the-art medical image steganography and reversible data-hiding techniques are also recommended.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[2] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. CRC Press, 2020.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding—A survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[4] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[5] ISO 27799, Health Informatics—Information Security Management in Health Using ISO/IEC 27002. International Organization for Standardization, 2016.

[6] W. R. Hendee and E. R. Ritenour, Medical Imaging Physics. John Wiley & Sons, 2002.

[7] D. L. Pham, C. Xu, and J. L. Prince, “Current methods in medical image segmentation,” Annual Review of Biomedical Engineering, vol. 2, no. 1, pp. 315–337, 2000.

[8] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding using histogram shifting,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

“Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License”

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

[9] W. C. Kuo et al., "Joint data hiding and lossless compression scheme for medical images using Run-Length Encoding," Computers in Biology and Medicine, vol. 41, no. 4, pp. 210–218, 2011.

[10] S. Aharon et al., "A high-capacity reversible data hiding scheme for e-healthcare applications using non-linear chaos dynamics and ISB substitution," Journal of Medical Systems, vol. 43, no. 8, Art. no. 245, 2019.

[11] C. C. Chang et al., "A high-capacity data hiding scheme based on 3D magic cube," Signal Processing, vol. 148, pp. 120–130, 2018.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"