International Journal of Cognitive Computing in Engineering 5 (2024) 379–397

Contents lists available at ScienceDirect

International Journal of Cognitive Computing in Engineering

journal homepage: http://www.keaipublishing.com/en/journals/international-journal-of-cognitive-computing-in-engineering/

A novel medical steganography technique based on Adversarial Neural Cryptography and digital signature using least significant bit replacement

Mohamed Abdel Hameed [a], M. Hassaballah [b,c,*], Riem Abdelazim [d], Aditya Kumar Sahu [e]

[a] Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor, 85951, Egypt
[b] Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, AlKharj, 16278, Saudi Arabia
[c] Department of Computer Science, Faculty of Computers and Information, South Valley University, Qena, Egypt
[d] Department of Information Systems, College of Information Technology, Misr University for Science and Technology, Giza, Egypt
[e] Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amaravati, Andhra Pradesh, 522503, India

ARTICLE INFO

Keywords:
Medical information
Multimedia security
Data hiding
Steganography
LSB
HOG-LSB

ABSTRACT

With recent advances in technology protecting sensitive healthcare data is challenging. Particularly, one of the most serious issues with medical information security is protecting of medical content, such as the privacy of patients. As medical information becomes more widely available, security measures must be established to protect confidentiality, integrity, and availability. Image steganography was recently proposed as an extra data protection mechanism for medical records. This paper describes a data-hiding approach for DICOM medical pictures. To ensure secrecy, we use Adversarial Neural Cryptography with SHA-256 (ANC-SHA-256) to encrypt and conceal the RGB patient picture within the medical image's Region of Non-Interest (RONI). To ensure anonymity, we use ANC-SHA-256 to encrypt the RGB patient image before embedding. We employ a secure hash method with 256bit (SHA-256) to produce a digital signature from the information linked to the DICOM file to validate the authenticity and integrity of medical pictures. Many tests were conducted to assess visual quality using diverse medical datasets, including MRI, CT, X-ray, and ultrasound cover pictures. The LFW dataset was chosen as a patient hidden picture. The proposed method performs well in visual quality measures including the PSNR average of 67.55, the NCC average of 0.9959, the SSIM average of 0.9887, the UQI average of 0.9859, and the APE average of 3.83. It outperforms the most current techniques in these visual quality measures (PSNR, MSE, and SSIM) across six medical assessment categories. Furthermore, the proposed method offers great visual quality while being resilient to physical adjustments, histogram analysis, and other geometrical threats such as cropping, rotation, and scaling. Finally, it is particularly efficient in telemedicine applications with high achieving security with a ratio of 99% during remote transmission of Electronic Patient Records (EPR) over the Internet, which safeguards the patient's privacy and data integrity.

1. Introduction

The widespread use of the Internet to send massive amounts of information across unsecured networks and channels places private and confidential information at risk (Ding et al., 2023; Khan et al., 2020; Sangaiah, Javadpour, Ja'fari, Pinto, & Chuang, 2024). As more digital information is sent over the Internet, new technologies for safeguarding and securing critical communications must be created continuously (Hameed, Abdel-Aleem, & Hassaballah, 2023; Hameed, Hassaballah, Aly, & Awad, 2019). Additionally, confidentiality in the context of medical information is a crucial ethical and legal principle that protects patients' privacy and the security of their personal health information (Chowdhuri, Pal, & Si, 2023). Maintaining patient confidentiality is a legal and fundamental ethical obligation for health care professionals. Breaching patient confidentiality breaches trust and damages the patient–doctor relationship. Although patient confidentiality is paramount, there are exceptions when health authorities may need to share information for public health reasons, such as tracking the spread of infectious diseases (Hua et al., 2023; Rajaram et al., 2023). Thus, it is essential for both health care providers and patients to be aware of the laws and best practices surrounding medical confidentiality to ensure that patient privacy is respected and protected (Yan, Li, Iliyasu, Salama, & Hirota, 2023). Patients should feel comfortable discussing their medical concerns with their health care providers, knowing that

* Corresponding author at: Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, AlKharj, 16278, Saudi Arabia.
E-mail address: mah.ali@psau.edu.sa (M. Hassaballah).

https://doi.org/10.1016/j.ijcce.2024.08.002
Received 15 October 2023; Received in revised form 15 June 2024; Accepted 6 August 2024
Available online 17 August 2024
2666-3074/© 2024 The Authors. Publishing services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

their information will be handled with the utmost care and discretion (Al-Chaab et al., 2023; Durafe & Patidar, 2023). In the era of multimedia security assessments, an Ensemble Whale Optimized Recurrent Neural Network (EWO-RNN) is introduced to improve resilience, accuracy, generalization, and decision-making capabilities in a dynamic and evolving digital environment (Haripriya et al., 2024).

Moreover, steganographic framework based on Concomitantly shaRing generated Images and PrompTs (SCRIPT) achieves the importance of multimedia security. This framework ensures information security and robustness by identifying robust coefficients within the image for message embedding and synchronizing their positions (Zeng, Chen, Zhang, Zhang, & Yu, 2024). Similarly, the secret medical image containing the QR code for the patient diagnosis information (PDI) is hidden in a natural target image. A lossless compression technique, labeled soft technique, is introduced (Ping et al., 2024) to achieve hiding invisibility, recovery accuracy, and multimedia security.

By utilizing three techniques, steganography, cryptography, and watermarking, the data-concealing idea was established to preserve the integrity of secret data and keep unauthorized users away from transmitted data (Abdel Hameed, Aly, & Hassaballah, 2018; Hussain, Wahab, Idris, Ho, & Jung, 2018). Steganography is a technique of information concealment that may be used to solve communication security issues (Qin, Li, Tan, Tang, & Huang, 2022; Yang, Bai, Xue, Li, & Li, 2023). It is capable of hiding particular secret information in public media, such as photographs, documents, audio, and video, without raising suspicion. It may be divided into several categories, including spatial, transform, spread spectrum, statistical, and cover generation techniques (Sahoo & Sahoo, 2020; Shtayt, Zakaria, & Harun, 2021).

Image steganography and multimedia security are new fields in which data is embedded into an image so that it is visible or invisible. It has already been done in the spatial and frequency domains (Roy et al., 2022). The secret message is hidden by adjusting pixel values directly in the spatial domain. This domain has an advantage by achieving a higher payload and taking less time to embed secret data than the frequency domain. Mainly, the least significant bit (LSB) substitution scheme has become the most commonly used as a data hiding technique in which the LSBs of the cover image are used for embedding secret bits (Hameed et al., 2019; Shen & Huang, 2015).

There is always a trade-off between imperceptibility and embedding payload. In contrast, the stego-image will have a lower visual quality because of more bits embedded in the cover image. This is contrary to the main goal of the steganography technique of sending secret data without others knowing of their existence. Consequently, after embedding more data bits, the stego images should be indistinguishable from the matching cover images and imperceptible to human vision (Hassaballah, Hameed, Aly, & AbdelRady, 2020).

Most recent secure steganographic approaches for digital images represented in the spatial domain are content-adaptive. This means steganalysis can change the embedding process in complex regions of the cover image, which are difficult to detect. As a result, the multimedia security against steganalysis attackers will be increase (Denemark, Boroumand, & Fridrich, 2016; Li, Tan, Wang, & Huang, 2014). The spatial domain steganography techniques are very simple, and the secret information is directly embedded in pixel values (Singh & Attri, 2015).

Over time, steganographic techniques provided different LSBs of pixel or bit-planes for embedding secret data. Due to the simplicity of LSB embedding, several methods have been developed to improve capacity while enhancing imperceptibility. Adaptive LSB replacement based on the edges, texture, intensity level, and brightness of the cover pictures is one of them, and it is used to estimate the k number of LSBs for embedding data (Hameed et al., 2019; Shtayt et al., 2021).

Several key properties make HOG well-suited for feature extraction in medical imaging, such as being insensitive to geometric and photometric transformations, capturing edge/shape information, unsupervised feature extraction, noise tolerance, and being simple and efficient to compute histograms for image blocks (Gu et al., 2024; Iqbal et al., 2024; Taspinar & Ozkurt, 2024).

Using digital signatures in steganography makes it possible to verify that the hidden information has not been tampered with or altered during transmission or storage. A digital signature is a cryptographic technique that uses a private key to generate a unique identifier for a piece of data. This identifier, known as a signature, can be verified using a corresponding public key (Hua et al., 2023)

When applying steganography techniques, digital signatures can be used in several ways (Hua et al., 2023; Huang, Dong, Ye, Yap, & Goi, 2023; Yang et al., 2023):

1. Integrity verification: The digital signature can be applied to the original data before it is concealed within another file. When the hidden data is extracted later on, the digital signature can be checked against the extracted data to ensure that it has not been modified or corrupted.
2. Authenticity verification: Digital signatures can also be used to verify the authenticity of the hidden data. By associating a digital signature with the original data before hiding it, recipients can verify that the extracted data originated from the expected source.
3. Non-repudiation: Digital signatures provide non-repudiation, meaning that once a sender has signed their message with their private key, they cannot later deny having sent it. This helps establish trust and accountability in steganographic communication.

In most techniques (Ch et al., 2024; Hegde & Maddikunta, 2023; Hua et al., 2023; Ping et al., 2024) that are used for medical steganography, we can provide some limitations that might be associated with our proposed technique as follows:

1. Capacity vs. Imperceptibility Trade-off: There is often a trade-off between the amount of data that can be hidden (capacity) and the imperceptibility of the modifications (how noticeable they are). LSB replacement may affect the quality of medical images if too much data is embedded.
2. Robustness to Image Processing: Medical images might undergo various processing steps such as compression, scaling, or format conversion, which can potentially disrupt the hidden information.
3. Detection by Steganalysis: Advanced steganalysis tools are capable of detecting alterations in images, including those made by LSB replacement methods, potentially exposing the hidden data.
4. System Complexity: Implementing a system that combines adversarial neural cryptography with steganography and digital signatures can be complex, which may lead to difficulties in deployment and maintenance.
5. Computational Resources: The training and execution of neural cryptography models require significant computational power, which might be a constraint in some medical environments.
6. Error Propagation: Errors in embedding or extraction processes can lead to loss or corruption of both the image and the hidden data, which is particularly critical when dealing with sensitive medical information.

Overall, by incorporating digital signatures into steganography techniques, users can have confidence in both the integrity and authenticity of hidden information while maintaining privacy and security.

This paper proposes a novel medical steganography technique with two authentication factors encryption and digital signature using the HOG-LSB approach for hiding metadata. In this technique, the medical image is split into two regions: the Regions of interest (ROIs) and the Regions of non-interest (RONIs). To find RONIs, we calculate the gradient magnitude using the threshold value (T). Furthermore, the embedding areas may be enlarged or lowered by the size of EPR by

modifying the threshold value T. In other words, the embedding rate can be determined in the medical image by adjusting the two key parameters (K, T) to satisfy the regions that can be selected adaptively for hiding EPR. In the specified set of RONIs, the patient's image is encrypted using ANC SHA-256 to be embedded in the LSB. On the sender side, the proposed technique is used to convert metadata from the DICOM file to its corresponding digital signature using the Secure Hash Algorithm (SHA-256) and a private key. On the recipient side, the digital signature is extracted using the public key to obtain a hash value $Hash_1$. At the same time, get a copy from the same DICOM file and use metadata to obtain the hash value $Hash_2$ using SHA-256. Then, compare two hash values $Hash_1$ and $Hash_2$ if they are identical; thus, we can ensure that no modification has been altered on the secret image or DICOM file. By incorporating digital signatures into steganography techniques, we can have confidence in both the integrity and authenticity of hidden information while maintaining privacy and multimedia security.

Experimental results demonstrate that the proposed HOG-LSB technique is resistant to standard uniform affine transformations such as cropping, rotation, and scaling. In addition, the performance of the proposed technique is compared to other information-hiding methods according to the physical measure of change inside the medical image, including three metrics PSNR, MSE, and SSIM values. Moreover, the segmentation of medical images to differentiate between the region of interest and other regions will be beneficial to the embedding process to avoid any effects on the region of interest.

The paper is structured as follows: Section 2 gives an overview of the telemedicine steganography techniques. Then, both embedding and extraction procedures of the proposed HOG-LSB scheme are illustrated in Section 5. Moreover, experimental results and discussion along with analysis and comparisons are provided in Section 6. Finally, the conclusion is given in Section 7.

2. Literature review

Telemedicine has benefits like improving access to medical information, accessing care, and determining the most cost-effective diagnosis (Al-Chaab et al., 2023; Ramasamy et al., 2022). Although telemedicine has previous advantages, it has some disadvantages such as multimedia security level of the medical information transmitted (Zain & Clarke, 2011) and the poor quality of received medical images. In DICOM image formats, the EPR is present as metadata consisting of a set of pixels with metadata at the header linking the image to its corresponding EPR. In this way, advances in the telecom technologies have led to the expansion of services based on DICOM files for the transmission of medical images through Picture Archiving and Communication Systems (PACS), a technology that follows the DICOM standard. PACS also enables the development of various applications, including telemedicine, and the ability to remotely diagnose, among others, opening the possibility of providing a better clinical analysis or treatment, in the interest of the plan of care. A medical image can therefore be transmitted multiple times inside hospitals or even outside of them during every moment of its existence (Olvera-Martinez, Cedillo-Hernandez, Diaz-Rodriguez, & Jimenez-Borgonio, 2022). This scenario may introduce some management and information security risks that must be prevented because medical data are confidential and traditional informatics security tools such as anti-virus, cryptography tools, or firewalls, to name a few, cannot solve all medical data security issues. As a result, data hiding is a research subject that has been widely recommended for enhancing the management and information security of medical imaging by concealing primarily binary data to create a trustworthy relationship between these data and the image (Cedillo-Hernandez, Cedillo-Hernandez, Nakano-Miyatake, & Perez-Meana, 2020; Olvera-Martinez et al., 2022; Qasim, Meziane, & Aspin, 2018).

For multimedia security assessments with watermarking, an Ensemble Whale Optimized Recurrent Neural Network (EWO-RNN) is used in order to enhance generalization, robustness, and accuracy in a dynamic and changing digital environment (Haripriya et al., 2024). Also, Zeng et al. (2024) suggests the steganographic system based on concurrently shaRing-produced images and prompts (SCRIPT). This system provides acceptable security and resilience by finding resilient coefficients inside the image for message embedding and synchronizing their locations. Similarly, Ping et al. (2024) proposed the soft lossless compression technology for recovery precision, and hiding invisibility by utilizing a natural target image for concealing the secret medical image with the QR code for the patient diagnosis information (PDI).

In the same manner, Ch et al. (2024) proposed a robust digital watermarking approach tailored to brain medical images, combining hashing, the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Integer Wavelet Transform-Discrete Cosine Transform (IWT-DCT). This achieved an integrated blockchain technology to enhance data security and integrity verification. Prabhavathi, Anandaraju, and Ravi (2023) proposed the region-based medical image encryption using a 2D logistic sine map (2DLSM) and an advanced zigzag transform for securing medical images. So, the suggested approach is strong in defending against diverse attacks and can get an acceptable, secure ROI for different medical photos according to various sizes and types. Singh, Singh, Singh, and Agrawal (2024) suggested an approach for safe watermarking based on multi-modal medical image fusion called WatMIF. The suggested approach has three stages: embedding and extracting the fused mark, fusing multi-modal medical photos, and encrypting the host media to achieve invisibility, robustness, and multimedia security.

Unauthorized individuals who try to access patient information can discover EPR regardless of the digital signature and encryption measures used in DICOM images (Karakus & Avci, 2020; McEvoy & Svalastoga, 2009; Memon & Gilani, 2008). A critical role in telemedicine applications has been played using the steganography technique by providing privacy, integrity, and originality. The Internet and other recent cloud computing technologies have been used significantly in telemedicine to provide different medical services for patients in remote places. Telemedicine has been using more technologies to deliver different medical services to patients in remote locations. When these applications are used, there are certain benefits, such as improved access to medical information, developed care delivery, and cost-effective diagnostics. Despite the benefits listed above, telemedicine has significant drawbacks, such as the security level of medical information transferred and the quality of medical images received (McEvoy & Svalastoga, 2009; Memon & Gilani, 2008). The patient's data should be kept private, and medical information should be transmitted safely.

Different adaptive steganographic methods come up to improve the embedding capacity. Amirtharajan and Rayappan (2012) presented an adaptive LSB method, where the random k-bit embedding approach is utilized. Later, Goel, Gupta, and Kaushik (2015) provided a method for comparing the quality of stego-images to original cover images using the LSB approach and a set of image quality measures such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structure Similarity Index Measure (SSIM). Nguyen, Arch-Int, and Arch-Int (2016) presented an adaptive data-hiding method based on LSB substitution and multi-bit planes for Region data-hiding (MPBDH) that used multiple image regions. Yuan (2014) introduced a technique that uses multi-cover adaptive steganography. A different scheme was illustrated by Hussain et al. (2018) that fused based on different lower and upper texture sections of the cover image, the adaptive LSB with the rightmost digit replacement (RMDR) technique. Muhammad, Ahmad, Farman, and Zubair (2015) introduced a method for RGB images with better imperceptibility and acceptable embedding payload. Chang, Tsai, and Lin (2004)introduced an adaptive technique for determining the degree of smoothness with high embedding capacity using the LSB substitution method that makes use of the correlation between surrounding pixels. Singla and Juneja (2014) proposed a new technique

for RGB images that adaptively uses the host image's features to hide more information than in other areas. The LSB replacement approach was used to incorporate secret information. The capacity has been enhanced, and an unnoticeable stego-image quality has been achieved, however, there is a considerable drawback in terms of computational complexity and running time. Recently, Vanmathi and Prabu (2018) proposed a high payload and good imperceptibility using the fuzzy logic approach to hide secret bits. The main principle is to find edge areas that tolerate more number embedding bits than the smooth areas according to HVS.

Various techniques are proposed to improve the security of medical images. For instance, Yang, Xiao, Cai, and Zhang (2019) presented a secure and high visual-quality framework for medical images. They suggested a reversible data hiding (RDH) method based on lesion extraction that embeds secret data into medical images for privacy protection and image quality improvement. In addition, images are encrypted using homomorphic encryption to achieve multimedia security. A pixel similarity-based LSB method proposed by Karakus and Avci (2020) based on optimum pixel selection for hiding confidential medical information of the patients. The medical images have hidden capacities, including 5,000 and 10,000 characters to maintain robustness and visual quality according to MSE, RMSE, PSNR, and SSIM. Recently, Abdul (2022) demonstrated the proposed approach known as zero-steganography for medical image transmission in insecure communication channels. It achieves effective robustness against attacks like filtering, compression, and the addition of noise. Magdy, Hosny, Ghali, and Ghoniemy (2022) introduced different security techniques such as steganography, cryptography, and watermarking. They used four types of medical images Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-rays, and ultrasound to perform robustness against several attacks. Moreover, Ahmad et al. (2022) proposed a new data-hiding method to maintain robustness using medical DICOM images. First, an integer wavelet transform filter is decomposed for the medical image. Then, the patient's confidential information is processed using the Arithmetic Coding (AC) and Data Encryption Standard (DES) algorithms to be compressed and encrypted before the embedding process. In the same domain, Hussain and Khodher (2024) proposed a method for securing medical images using chaotic map encryption and LSB. They combine the Triple Data Encryption Algorithm (3DES) and AES methods with three chaotic maps to enhance security and visual quality. Hameed, Hassaballah, Bekhet, Narmatha, and Kenk (2023) proposed a high-quality secure technique using LSB substitution to hide secret bits inside medical images to improve capacity while maintaining security.

With the development of medical steganography, the proposed technique can enhance the performance of balancing between capacity, visual quality, and security. So, this paper assembled the following contributions:

1. A combination of HOG-LSB and ANC SHA-256 approaches is proposed to verify two authentication factors encryption and digital signature using the HOG-LSB approach for hiding metadata and improving the security of medical images.
2. Incorporating digital signatures into steganography techniques increases confidence in both the integrity and authenticity of hidden information while maintaining privacy and medical information security.
3. Extensive experiments have been conducted on medical images, which indicate that the proposed method is feasible and effective because of its robustness against standard uniform affine transformations, such as cropping, rotation, and scaling. Moreover, the performance of the proposed method outperforms other medical steganography methods according to the physical measure of change including three metrics PSNR, MSE, and SSIM.

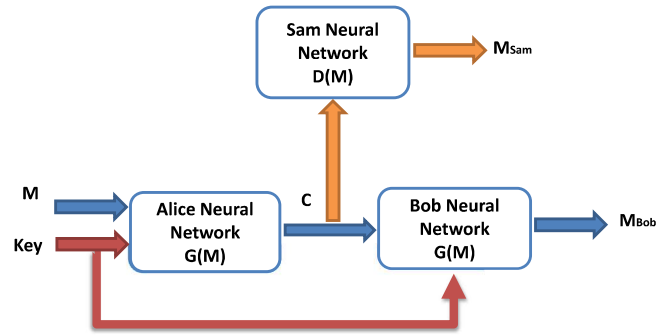


Fig. 1. The framework of the Adversarial Neural Cryptography.

3. Adversarial neural cryptography with SHA-256 encryption

A highly nonlinear image encryption method known as Adversarial Neural Cryptography with combining SHA-256 is used in our proposed technique to resist typical attacks like differential attacks against the patient image (Wu et al., 2021) if the attacker succeeds in extraction. This method integrates antagonistic neural cryptography (ANC) and chaotic systems controlled by SHA-256. As demonstrated in Fig. 1, the system of ANC designed with the classical scenario in security involves three parties: Alice, Bob, and Sam. Typically, Alice and Bob share the secret key K and wish to communicate Message M confidentially.

In the framework of the ANC, the network formed by Alice and Bob neural networks is regarded as the generator in GAN denoted as $G(M)$, while the Sam neural network is regarded as the discriminator in GAN denoted as $D(M)$. The Alice Network is mostly utilized for encryption, whereas the Bob network is used for decryption. At the same time, Sam is unable to complete the decryption task without the key. Moreover, the image encryption and decryption procedures are shown in Figs. 2,3 respectively. While the parameters α, β, and the hash value are used as cipher keys. α is equal to the initial value x_0 in Eq. (1) and β is equal to the initial value x_0 in Eq. (2).

In addition, a logistic map is a popular classical chaotic dynamic system that produces chaotic sequences with stable properties. It can be described as follows (Wu et al., 2021):

$$x_{n+1} = \mu x_n \left(x_n + 1\right), x_0 \in (0, 1) \tag{1}$$

Where x_n is the value of the nth element, x_0 is the initial value and μ is the control parameter, the system is in a chaotic state if $\mu \in [3.57, 4]$.

Similarly, a logistic-sine map consists of a logistic map and a sine map and can be expressed as:

$$x_{n+1} = \left[\mu x_n \left(1 - x_n\right) + (4 - \mu) \sin\left(\pi x_n\right)/4\right] \bmod 1 \tag{2}$$

where $\mu \in [0, 4]$ is the control parameter.

The proposed technique encrypts the secret image during the preprocessing phase. Subsequently, it can be embedded into a carrier image in the embedding procedure.

4. Region of non-interset RONI in medical images

An ROI is a significant part of the medical image that can be used for diagnosis. This region of the image is susceptible; thus, any little changes should be avoided. To locate the ROI in the medical image, the maximum value of the cumulative gradient magnitude histogram is used to determine the gradient magnitude for each Region. Furthermore, the number of K LSBs and threshold value T are calculated adaptively according to the size of the given EPR, including all secret bits in the candidate Regions of the medical image. RONI is defined as a block with an accumulated gradient magnitude value less than the selected threshold parameter T. This RONI element of the medical

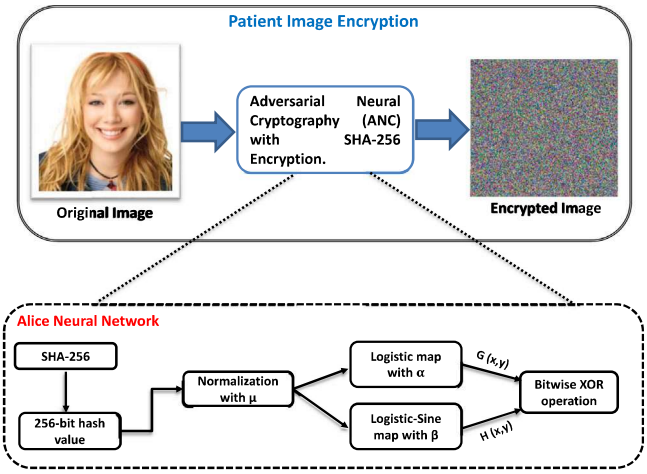


Fig. 2. Encryption procedure of the patient image using ANC and SHA-256.

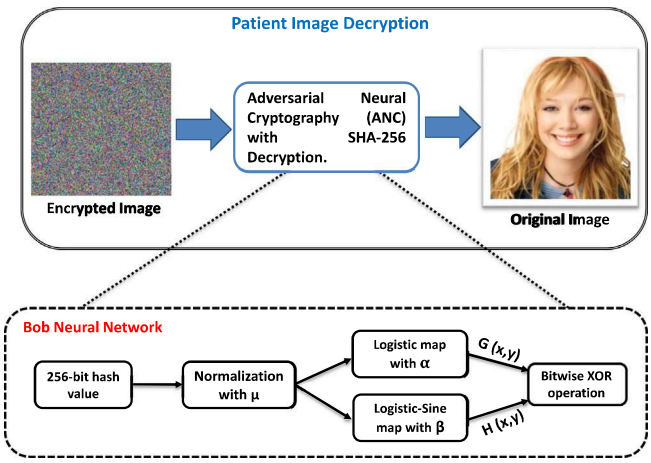


Fig. 3. Decryption procedure of the patient image using ANC and SHA-256.

image includes the Electronic Patient Record (EPR), as it does not affect the diagnosis. Furthermore, one method employed in medical image processing is edge detection to distinguish the ROI from the RONI. So, RONIs had poor edge information or were located in smooth regions (Thiyagarajan & Aghila, 2013) as shown in Fig. 4.

5. Proposed medical steganography technique

The LSB approach is the most often utilized spatial domain technique and has the greatest potential for medical images. Compared to other approaches, it can give more hiding payload and is easier to perform. This approach changes the LSB of the host image's selected pixels with the required values. Because changes to LSBs are not perceptible to the Human Visual System (HVS), the visual degradation induced is substantially less with the LSB replacement (Hameed, Abdel-Aleem, & Hassaballah, 2023; Hassaballah, Hameed, Awad, & Muhammad, 2021).

The proposed medical technique is applied to the 2×2 pixel block adaptively. It is composed of two algorithms, one for embedding and the other for extracting the EPR, which consists of ID number, name, doctor's name, date of birth, and address. The embedding algorithm relies on the LSB substitution technique to choose a group of Regions of non-interest (RONI) by applying the Histogram of Oriented Gradient (HOG) algorithm to hide EPR in medical images. These Regions contained weak edges of medical information or fell into the smooth

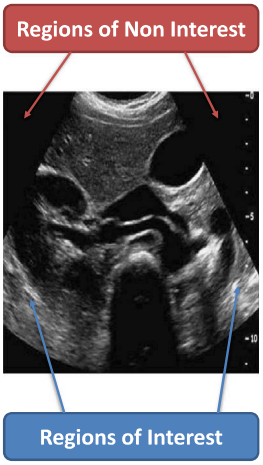


Fig. 4. ROIs and RONIs of the Kidney medical image.

regions. Thus, using the LSB technique for embedding in each block is very useful for increasing the embedding payload while maintaining the visual quality and security of the DICOM file, assuming that the top-left pixel in each RONI is a base pixel that can store positions selected by RONIs. The other three adjacent pixel pairs are used to hide secret bits (EPR).

5.1. Histogram of oriented gradients (HOG)

HOG algorithm (Dalal & Triggs, 2005) or Histogram of Oriented Gradients, is a feature descriptor similar to the Canny Edge Detector and SIFT (Scale Invariant and Feature Transform). It is used to detect objects in computer vision and image processing. The approach counts the number of times a gradient orientation appears in a limited image region. This technique is comparable to Edge Orientation Histograms and SIFT. The HOG description focuses on an object's structure or form. It outperforms all other edge descriptors because it computes features using both the magnitude and angle of the gradient. It creates histograms for the picture areas based on the magnitude and orientation of the gradient. This gradient magnitude is calculated from the input medical image's x and y gradient images. Then, normalize the gradient magnitude value to be in the range $\{0-1\}$. Based on these criteria, the steps of the algorithm used to extract and collect HOGs for all blocks over the detection window are shown in Fig. 5.

Thus, to collect HOG descriptors for all blocks over a detection window in a medical image:

1. Preprocessing: Medical images often require pre-processing to enhance features, remove noise, or standardize intensity values. Different preprocessing techniques may be applied depending on the type of medical image (e.g., MRI, CT, X-ray).
2. Define detection window: Determine the size and location of the detection window within the medical image. This may be the entire image or ROI where you expect to find the object of interest.
3. Divide into Cells and Blocks: The detection window is divided into small, spatial regions called cells, which are grouped into larger blocks. The organization of cells into blocks allows for local contrast normalization, which is beneficial for handling variations in illumination and shadowing.
4. Calculate gradients: Compute the gradient magnitude and direction at each pixel within the cells. This step is sensitive to the textural and edge information.
5. Create HOG: Compile a histogram based on gradient orientations for each cell. The number of bins in the histogram typically corresponds to the number of orientation angles.

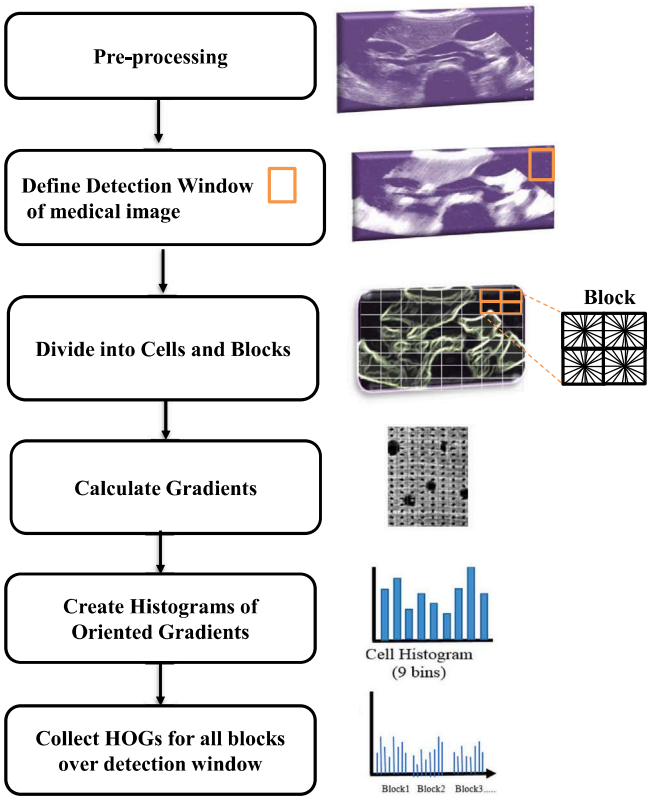


Fig. 5. Illustration of Histogram of Oriented Gradients in the medical image.

6. Normalization is applied to account for changes in illumination and contrast. This is important in medical images, which can vary widely in terms of lighting and contrast due to different imaging modalities and patient anatomy.

5.2. Allocating digital signature

As displayed in Fig. 6, the DICOM file must be checked enmake sure it has not been altered or modified after being retrieved. It is suggested that the Secure Hash Algorithm (SHA-256) (Wu et al., 2021) for the given metadata attached to the DICOM file to check the precision of the contents. On the sender side, we generate a digital signature for the metadata of the DICOM file using a private key with a hash value of 256 bits size which is calculated independently. At the recipient, the SHA-256 of the received file is computed and checked with the signature of the key file as part of the receiver's reconstruction of the DICOM file. If the results of comparing the two hashes match, it may be concluded that the DICOM file sent and the one received by the recipient are identical, ensuring that a third party did not alter the retrieved file. On the other hand, the received file should be rejected if a function comparison mismatch occurs since it indicates that the DICOM file has been modified.

5.3. Embedding procedure

The medical image and meta-data are separated in the DICOM file. During the embedding procedure, the encryption scheme is performed using Adversarial Neural Cryptography with SHA-256 for the patient's secret image. Also, a digital signature is generated for the metadata of the DICOM file using the Secure Hash Algorithm (SHA-256) and a private key as illustrated in Fig. 6. After that, we can get the digital signature and the encrypted image in the form of a key. Moreover, this key is concealed in the selected RONIs. Finally, the metadata is concealed inside the medical image and the stego-image is obtained as displayed in Fig. 7. Usually, in this phase, we initialize the threshold value $T_i = 0$ and number of LSBs $K_i = 1$ to get the actual size of selected RONIs for hiding metadata, including the patient's secret image and the digital signature, can be exploited using the following formula:

$$T_i = \lfloor \frac{t_{min} + t_{max}}{2} \rfloor \tag{3}$$

where $t_{min} = 0$, $t_{max} = 1$ and $K_i = [1 - 4]$

While the T_i and K_i are not appropriate to the metadata size, we can change these values adaptively until all RONIs become available to hide the DICOM file. On the other hand, to validate the integrity of the DICOM file, it is retrieved in the extraction procedure to acquire its hash value and add it to the key.

5.4. Extraction procedure

As shown in Fig. 8, the second stage of the proposed HOG-LSB technique is the extraction phase where the hidden patient image and DICOM file are extracted. When the recipient receives the medical image, the process of extracting the DICOM file, and the patient's secret image starts. Fig. 8 defines the extraction strategy with the following steps:

1. When the stego medical image is received, find the total number of pixels that fall in RONIs using the base pixel where the positions of selected RONIs are stored.
2. For each RONI, apply the LSB extraction algorithm until the metadata of the DICOM file is extracted.
3. Once the metadata is extracted from the stego-image, we calculate the hash value using the SHA-256 algorithm.
4. At the same time, the patient image was extracted using the ANC-SHA-256 decryption algorithm.
5. When the hash value has been calculated using the public key, it is compared to the received hash.
6. Finally, the DICOM file is reconstructed with the metadata and the resulting medical image.

6. Experimental results and analysis

This section introduces experimental outcomes and analysis to show the viability and efficiency of the suggested HOG-LSB strategy. Imperceptibility, capacity, and security are the primary factors for image steganography, so we tested and evaluated the model from these three perspectives. Various datasets are also employed to test the proposed HOG-LSB for the generalization capability.

6.1. Developmental environment and datasets

All tests and outcomes are run on Matlab *R*2020*b* using Intel(R) Core(TM) i7-7400, with CPU 3.0 GHz, 16 GB RAM, and Windows 10 operating system. The performance evaluation of the proposed technique is done in terms of visual quality, robustness, and physical change measurement. This technique is tested with four medical datasets including an MRI medical dataset[1], brain CT dataset[2], X-ray dataset[3] and US-4 Ultrasound dataset[4]. All images assumed for the experiment were considered uncompressed in DICOM format and selected randomly. As illustrated in Figs. 9, 10, 11, and 12 for MRI, brain CT, X-ray, and Ultrasound datasets respectively, the proposed technique is tested and

[1] https://www.kaggle.com/datasets/kmader/siim-medical-images
[2] https://www.kaggle.com/datasets/vbookshelf/computed-tomography-ct-images
[3] https://www.kaggle.com/datasets/paultimothymooney/xray-pneumonia
[4] https://paperswithcode.com/dataset/us-4

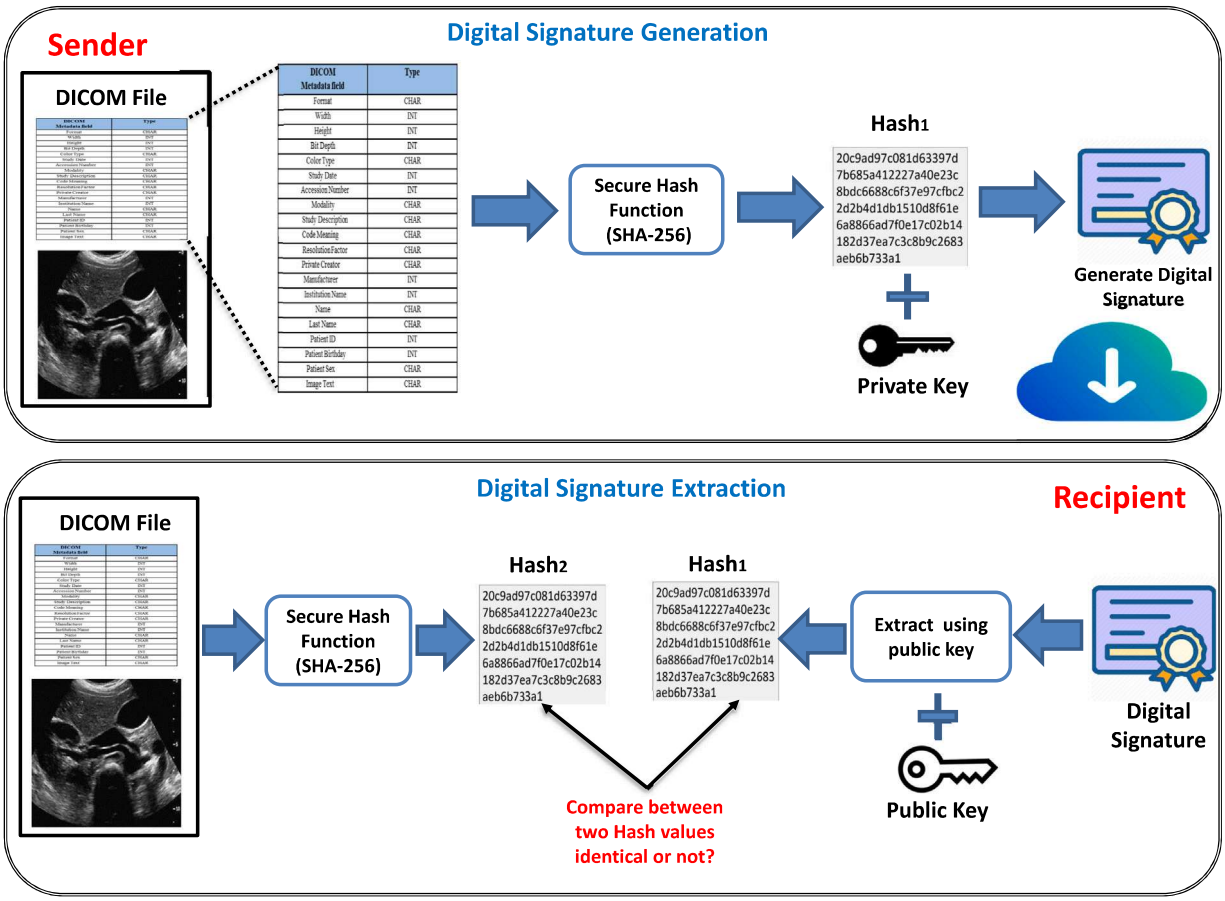


Fig. 6. Digital signature generation and extraction using secure hash algorithm SHA-256.

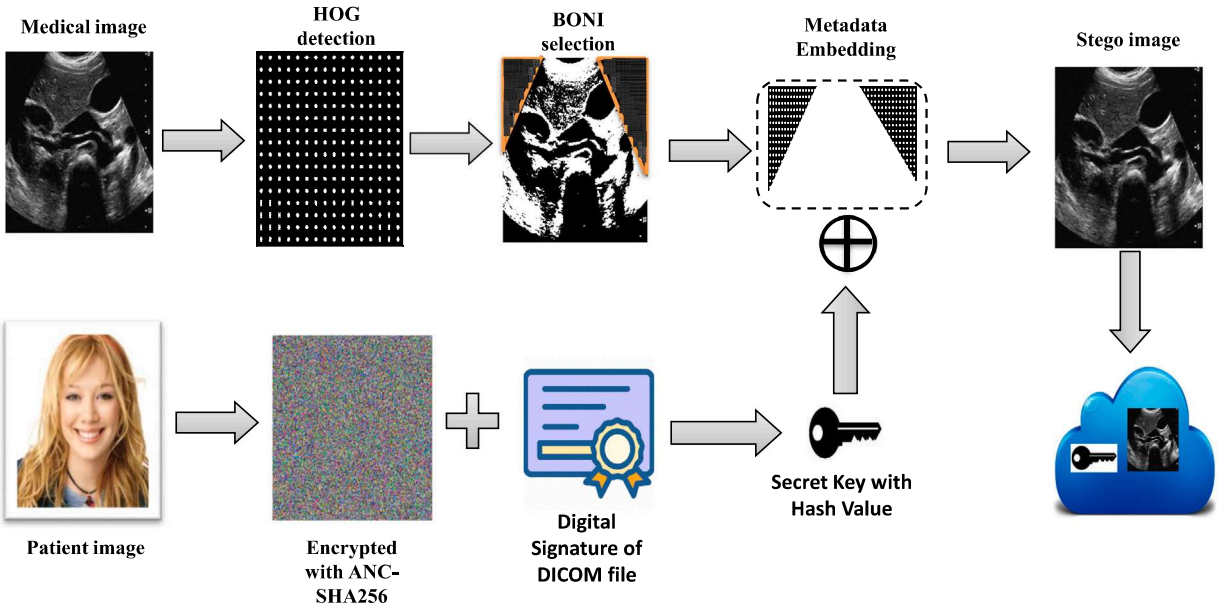


Fig. 7. Flow chart of embedding procedure to hide the patient image and digital signature of the DICOM file in the medical image.

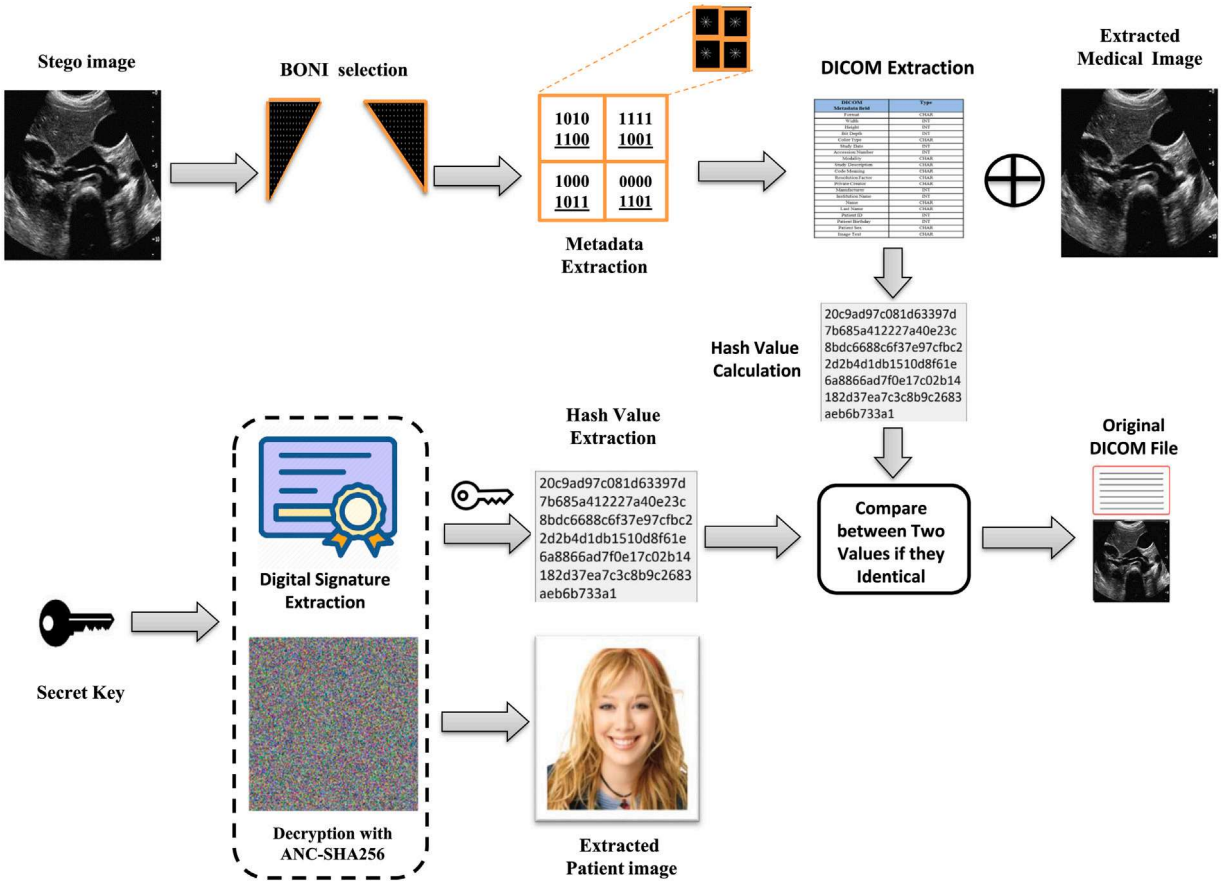


Fig. 8. Flow chart of extraction procedure to retrieve patient image and original DICOM file.

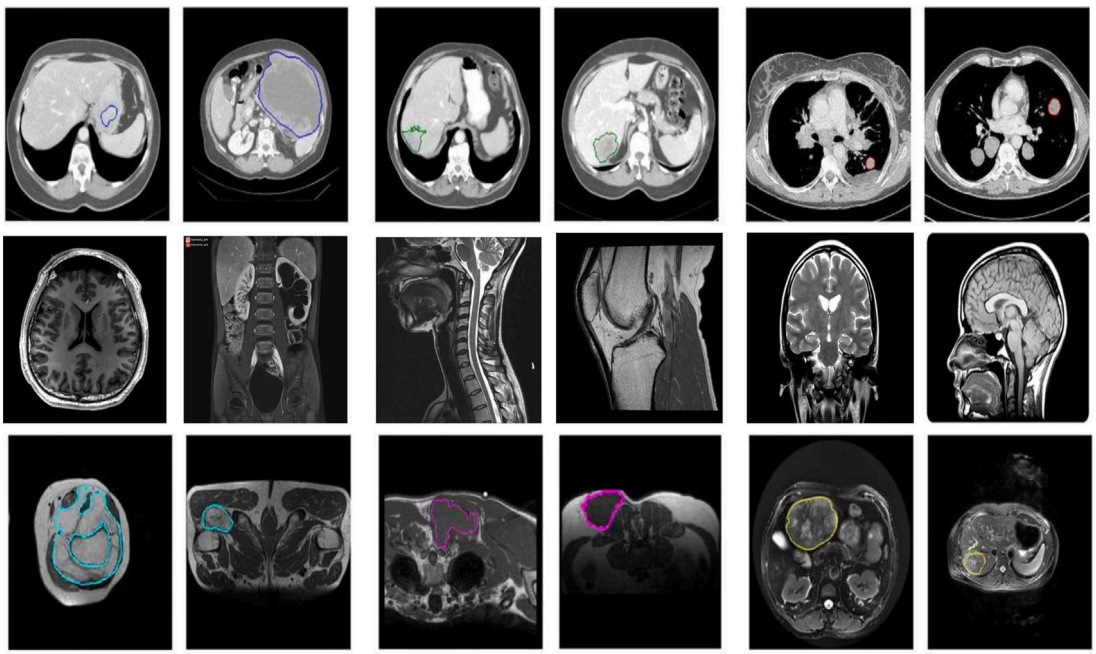


Fig. 9. Sample test images from MRI medical dataset.

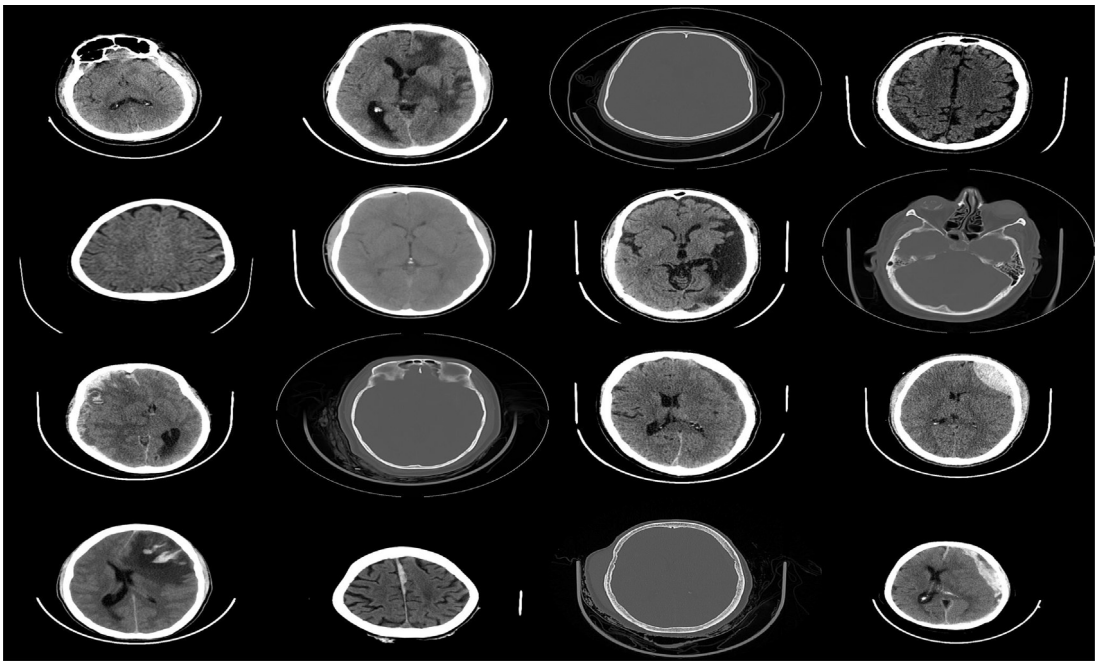


Fig. 10. Sample test images from brain CT medical dataset.

Fig. 11. Sample test images from X-ray medical dataset.

investigated using hundreds of medical images, and a sample of RGB images with size 56 is selected randomly from the LFW dataset (Huang, Mattar, Berg, & Learned-Miller, 2008) as displayed in Fig. 13 to evaluate our approach's efficiency and effectiveness. Here's a clear rationale for selecting medical image datasets focusing on specific features:

- Redundancy: Medical images often contain redundant information, especially in areas with uniform intensity or textures. This redundancy provides hiding spaces for embedding secret data without significantly altering the original image, like X-rays with large homogeneous regions or specific MRI sequences with predictable patterns.
- Modality-specific features: As demonstrated in CT scans, the inherent noise level in CT scans can be exploited for steganography. Also, the proposed method can modify specific noise patterns to embed data while maintaining a visually unchanged image. Moreover, ultrasound images have dynamic sequences that can be used for steganography by manipulating subtle variations in pixels between frames without affecting the diagnostic quality.
- Embedding capacity: The datasets should have enough redundancy to embed the secret data without introducing perceptible artifacts. Consider the trade-off between embedding capacity and the potential impact on image quality. Datasets with higher redundancy can hide more data with a lower risk of detection.

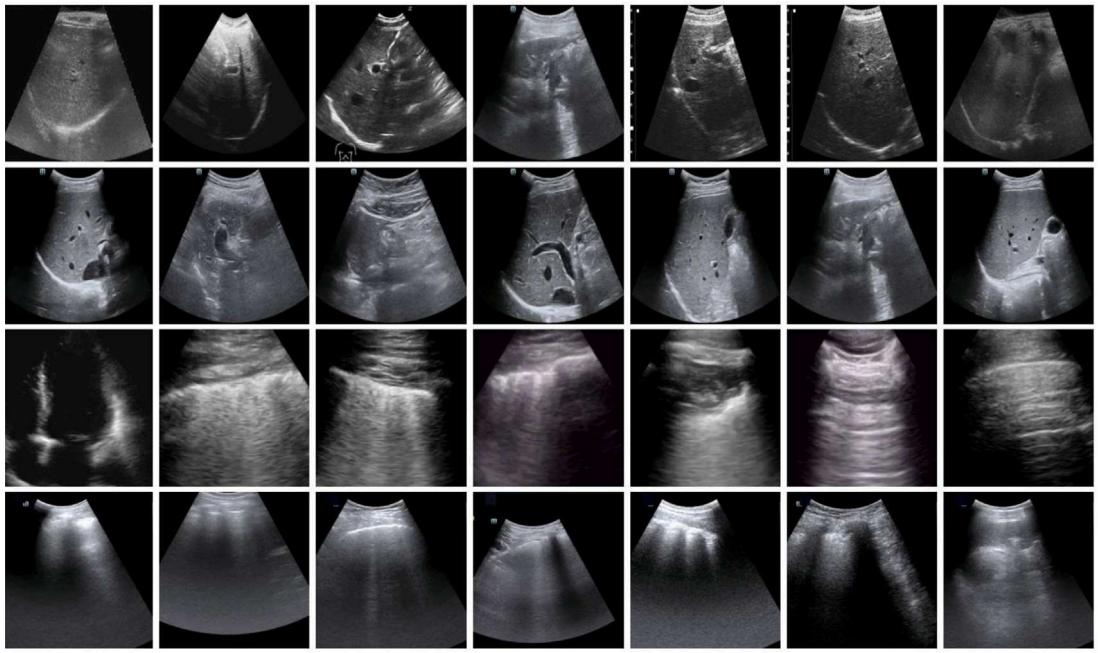


Fig. 12. Sample test images from Ultrasound medical dataset.

Fig. 13. Sample test images from LFW dataset.

6.2. Visual quality assessment

As the payload embedding secret images inside the cover image adjusts the details by changing the values of pixels, which influences the perceptual quality of the stego-image (image after embedding) and the cover medical (image before embedding), we tested the visual quality of the stego medical and cover images. This involves a subjective evaluation by steganalyst observers who assess whether any noticeable changes are present in the stego media compared with the original cover media. In this context, five benchmark criteria are used to assess the visual quality of the stego-image as a result of the embedding of patient image and digital signature inside the RONIs: mean square error (MSE), peak signal-to-noise ratio (PSNR) (Yang et al., 2023), universal quality index (UQI) (Hameed et al., 2019), structural similarity index measure (SSIM) (Zhu, Lai, Liang, Xiong, & Wu, 2022), and average absolute pixel error (APE) (Zhu et al., 2022). The PSNR and MSE are defined as:

$$PSNR = 10\ log_{10} \frac{(256-1)^2}{MSE} \tag{4}$$

Where MSE is the mean square error and can be calculated using Eq. (5)

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (P_{x,y} - P'_{x,y})^2 \tag{5}$$

where $P_{x,y}$ refers to the pixel value of the cover medical image before embedding, $P'_{x,y}$ is the corresponding pixel value of the stego medical image after embedding, and $M \times N$ represents the height and width of the cover image respectively.

Another visual quality metric known as UQI is also evaluated to measure the statistical similarity between the cover medial image and stego or extracted image. It is depicted by the next formula (Hameed et al., 2019):

$$UQI = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2 + \sigma_y^2)[(\bar{x})^2 + (\bar{y})^2]} \tag{6}$$

Moreover, SSIM estimates the visual quality of the image by comparing the structural similarity of the input image and the stego or

Table 1
Obtained results of the proposed HOG-LSB technique in terms of PSNR, SSIM, UQI, and APE for stego and cover medical images.

Image dataset	Stego image vs. Cover image			
	Average PSNR	Average SSIM	Average UQI	Average APE of RONIs
MRI	67.82	0.9985	0.9989	3.75
Brain-CT	69.89	0.9989	0.9995	3.59
X-ray	68.95	0.9988	0.9983	3.67
Ultrasound	67.45	0.9968	0.9985	3.98
Average	68.53	0.9983	0.9988	3.75

Table 2
Obtained results of the proposed HOG-LSB technique in terms of PSNR, SSIM, UQI, and APE for extracted and secret patient images.

Image dataset	Extracted image vs. Secret image			
	Average PSNR	Average SSIM	Average UQI	Average APE R, G, B
MRI	42.93	0.9998	0.9980	3.56, 3.85, 3.61
Brain-CT	44.09	0.9989	0.9992	3.49, 3.52, 3.39
X-ray	43.96	0.9978	0.9984	3.52, 3.68, 3.46
Ultrasound	42.76	0.9987	0.9974	3.74, 3.89, 3.56
Average	43.44	0.9988	0.9983	3.58, 3,74, 3,51

extracted image. The expressions are defined as follows:

$$SSIM = \frac{(2\mu_C\mu_S + c_1) * (2\sigma_{CS} + c_2)}{(\mu_C^2 + \mu_S^2 + c_1) * (\sigma_C^2\sigma_S^2 + c_2)} \tag{7}$$

where,

μ_C is the average of the cover medical image C,
μ_S is the average of the stego medical image S;
σ_C^2 is the variance of C,
σ_S^2 is the variance of S; σ_{CS} is the co-variance of C and S.

Finally, the average absolute pixel error (APE) is often used to express the absolute pixel values of the errors between cover medical image x_{ij} and stego or extracted image y_{ij} is defined by the following formula:

$$APE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x_{ij} - y_{ij}) \tag{8}$$

Table 1 shows the obtained results by the proposed method for stego and covers medical images in terms of PSNR, SSIM, UQI, and APE on different medical datasets. The MRI dataset has four averages of PSNR, SSIM, UQI, and APE with values of 67.82, 0.9985, 0.9989, and 3.75 respectively. The Brain-CT dataset has averages of PSNR, SSIM, UQI, and APE with values of 69.89, 0.9989, 0.9995, and 3.59 respectively. The X-ray dataset has averages of PSNR, SSIM, UQI, and APE with values of 68.95, 0.9988, 0.9983, and 3.67 respectively. The Ultrasound dataset has four averages of PSNR, SSIM, UQI, and APE with values of 67.45, 0.9968, 0.9985, and 3.98 respectively. As a result, the obtained results show that our approach can be used to generate high-quality stego-images free of visual artifacts induced by embedding $56 \times 56 \times 3$ patient image plus 6000 bits of metadata. As a result, our method is very effective in maintaining medical image diagnosis without any changes while we use only the RONIs for hidden secret bits. Furthermore, we achieve that our approach is indistinguishable and highly efficient with various datasets with averages of PSNR, SSIM, UQI, and APE with values of 68.53, 0.9983, 0.9988, and 3.75, respectively.

In contrast, Table 2 demonstrates the obtained results of the proposed HOG-LSB technique in terms of PSNR, SSIM, and UQI for extracted and secret patient images with the average values of 43.44, 0.9988, 0.9983 respectively. Moreover, the APE of Red, Green, and Blue of the extracted image has average values of 3.58, 3.74, and 3,51 respectively. Therefore, the proposed approach provides acceptable imperceptibility to the HVS while we retrieve the patient's secret image after the extraction procedure. Furthermore, the retrieved secret image is of good quality with no noticeable differences between it and the associated secret image. As a result, our approach is very effective in retaining RGB patient images with very little of undetectable changes.

6.3. Protection against geometric attacks

As shown in Table 3, typical attacks such as rotation, scaling, and cropping have been used as testing on some samples in Fig. 14 that are divided into six categories including (Chest, Eye, Kidney, Hand, Foot, and Brain) selected randomly from four datasets to demonstrate the robustness against geometric attacks (Ma et al., 2021). The NCC metric shows how strongly the stego-image is matched to the cover image after hidden secret bits. The NCC value varies from 0 to 1. If the NCC values are actually equivalent to 1, the stego images are completely immune to image processing assaults (Hassaballah et al., 2020, 2021). The results of the NCC values against various attacks are obtained from the stego images and attacked stego images. This is done to determine whether the secret bits EPR embedded in the image withstand the attack or not. It is given by the Eq. (9):

$$NCC = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[P_{x,y} * P'_{x,y} \right]}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[P_{x,y} \right]^2} \tag{9}$$

The most common geometrical digital image assault is the rotational attack. Rotation assaults were conducted using the stego-image created by the proposed method. Table 3 shows the obtained stego-image with rotation rates of 45°, 90° and 180°. The NCC is then computed between the stego-image and its rotated equivalent. The NCC value varied between 0.9121 and 1 within every case. The outcomes show that the proposed approach is capable of resisting rotating attacks. Moreover, the stego-image created by our technique was scaled. So, we found that NCC values range between 0.8726 and 1 in the obtained results provided in Table 3, indicating that the stego-image created by the proposed approach sensibly resists scaling attacks. Furthermore, stego images generated from the proposed technique were exposed to cropping attacks. It is described as the process of eliminating the outside portions of the image (Thiyagarajan & Aghila, 2013). As indicated in Table 3, the NCC value for all of the images used in the experiment was over 0.9067, indicating that the proposed technique can tolerate cropping assaults to some extent.

6.4. Protection against physical change

In steganography, the physical measure of change refers to the amount of alteration or distortion introduced to the cover media (such as an image or audio file) when embedding medical information. The main goal is to minimize any noticeable changes that could potentially raise suspicion (Hua et al., 2023). There are several metrics to quantify the physical measure of change in steganography, including the following:

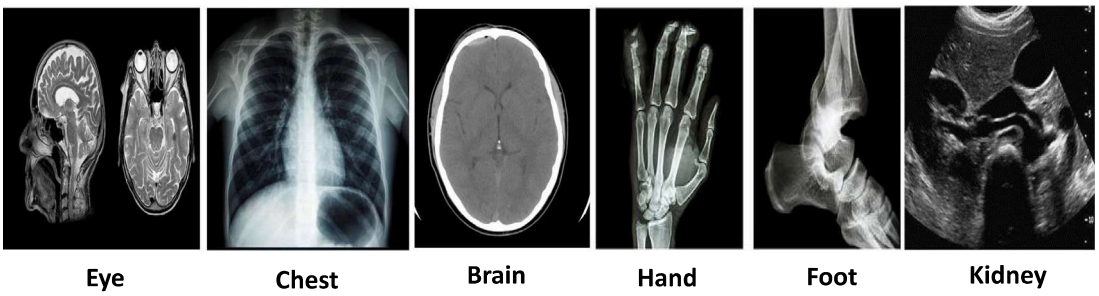


Fig. 14. Sample test images selected from four datasets including six categories.

Table 3
Obtained results of NCC values against different geometric attacks.

Attacks	Rate	Brain	Eye	Kidney	Chest	Hand	Foot
Rotation	45°	0.9121	0.9321	0.9491	0.9321	0.9347	0.9144
	90°	0.9205	0.9589	0.9562	0.9769	0.9577	0.9562
	180°	1.000	1.000	1.000	0.9826	1.000	0.9988
Scaling	0.5	0.9725	1.000	1.000	1.000	1.000	0.9987
	1.5	0.9295	0.9671	0.9647	0.9769	0.9554	0.9672
	2	0.8894	0.8826	0.8738	0.8726	0.8587	0.8921
Cropping	10%	0.9981	0.9999	0.9959	0.9893	0.9851	0.9860
	20%	0.9647	0.9725	0.9628	0.9751	0.9532	0.9541
	30%	0.9354	0.9204	0.9159	0.9067	0.9252	0.9174

1. Peak signal-to-noise ratio (PSNR): PSNR measures the difference between the original cover media and the stego media after embedding. A higher PSNR indicates a smaller change in the cover media.
2. Structural Similarity Index (SSIM): SSIM compares the structural medical information between the original and stego media. A higher SSIM indicates a smaller perceptual change.
3. Universal Quality Index (UQI): is a metric used to measure the quality of an image after steganographic embedding. It compares the original image with the stego-image and calculates a score that represents how similar they are. A higher UQI indicates a better quality stego-image.
4. Absolute Pixel Error (APE): APE is used to measure the difference between the original and stego-image. It calculates the average absolute difference between corresponding pixels in both images. A lower APE indicates a smaller difference and therefore a better quality stego-image.

Obviously, both UQI and APE are commonly used to evaluate the performance of different steganographic algorithms or techniques, helping researchers and practitioners assess how well an algorithm preserves image quality while hiding medical information. It is important for steganographic techniques to balance the amount of hidden information and minimize detectability (a physical measure of change).

In Table 4, the size of metadata in bits is taken in four ranges (2000–3000), (3000–4000), (4000–5000) and (5000–6000) respectively. Similarly, the six patient images at random selected from the LFW dataset with the same size 56×56 are employed in all ranges. The obtained results of the proposed HOG-LSB technique show that the PSNR has averaged with 67.55 dB This implies that the stego-images generated by the proposed technique are highly robust to HVS which leads to high visual quality after embedding $56 \times 56 \times 3$ plus 6000 bits of metadata. In addition, NCC, SSIM, UQI, and APE values are averaged to 0.9959, 0.9887, 0.9859, and 3.83 respectively, which concludes that the differences between the cover and stego-images are extremely small. Therefore, the obtained results prove that we have an accepted payload for secret bits while maintaining the imperceptibility of stego medical images.

6.5. Protection against histogram analysis

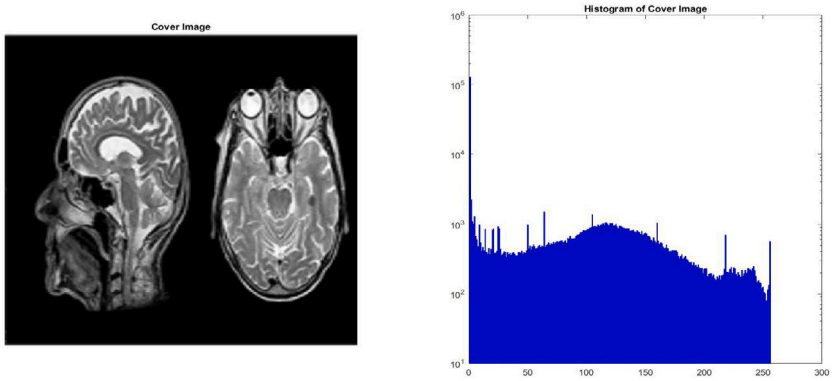
The histogram analysis is mainly performed to catch and evaluate secret data relics caused in the cover image after embedding. It is possible to calculate the size of the secret message, mainly when embedding has been very high, which means that steganalyst can detect any changes easily using HVS (Hameed et al., 2019). Consequently, we can perform this histogram analysis in terms of the proposed method between cover and stego images for the medical images mentioned earlier in Fig. 14.

In Figs. 15–20, there are six tested medical images, eye, chest, brain, hand, foot, and kidney, including histograms of cover images and their corresponding stego images after using the proposed technique HOG-LSB. By contrast, there is no variation between the histograms indicating that stego-images have superior imperceptibility and security. Therefore, the embedding procedure has a superior ability to hide color images and digital signatures without being detected by histogram analysis.

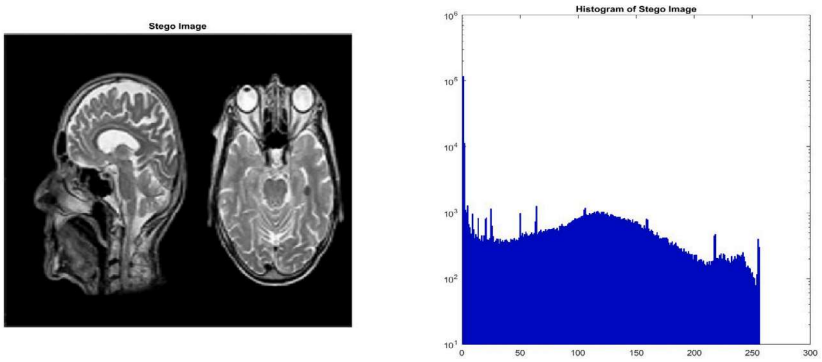
6.6. Comparative analysis with existing hiding techniques

Tables 5, 6 show a comparison between the experimental results of the proposed HOG-LSB technique and the prior work of Ahmad et al. (2022), Hameed, Hassaballah, et al. (2023), Hussain and Khodher (2024), Karakus and Avci (2020) and Thiyagarajan and Aghila (2013), according to three metrics, PSNR, MSE, and SSIM values for measuring the stego-image quality after embedding different EPR (metadata) size. The PSNR values should be as high as possible for the distortions to be undetected by the HVS (Abdel Hameed et al., 2018). Also, the MSE should be as low as possible to prove that no changes between cover and stego images which leads to high imperceptibility (Hassaballah et al., 2021).

As displayed in Tables 5, 6 In all cases of hidden metadata bits only, the obtained results of the proposed HOG-LSB technique outperforms recent methods including, (Ahmad et al., 2022; Hameed, Hassaballah, et al., 2023; Hussain & Khodher, 2024; Karakus & Avci, 2020; Thiyagarajan & Aghila, 2013) in terms of the PSNR value which is greater than 66.63 dB. Moreover, the MSE values of the proposed technique are given to be in the range 0 to 0.004 which is lower than (Ahmad et al., 2022; Hameed, Hassaballah, et al., 2023; Hussain & Khodher, 2024; Karakus & Avci, 2020; Thiyagarajan & Aghila, 2013). Besides, the SSIM values of the proposed technique are given in the range 0.9999 to 1 which is better than other methods, (Ahmad et al., 2022; Hameed, Hassaballah, et al., 2023; Hussain & Khodher, 2024; Karakus & Avci, 2020; Thiyagarajan & Aghila, 2013). So, the proposed technique achieved better results according to imperceptibility and visual quality to ensure that there is very little change between the cover and stego medical image after embedding secret metadata within the range of (650–1850) bits. Hence, this leads to high effectiveness in concealing secret bits of our approach as compared to state-of-the-art medical steganography according to the human visual system (HVS).

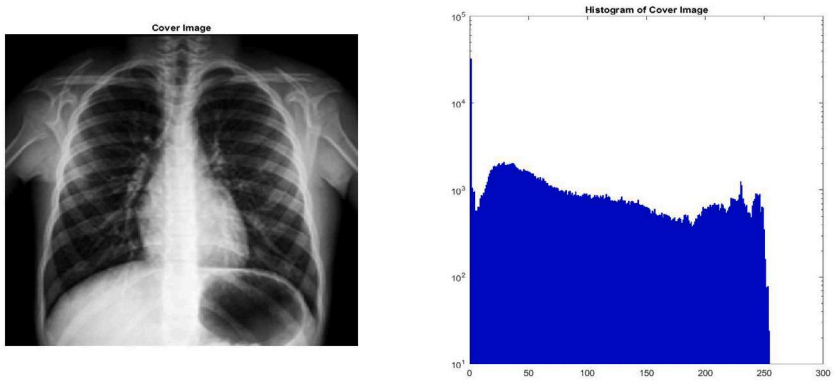


(a) Eye Cover

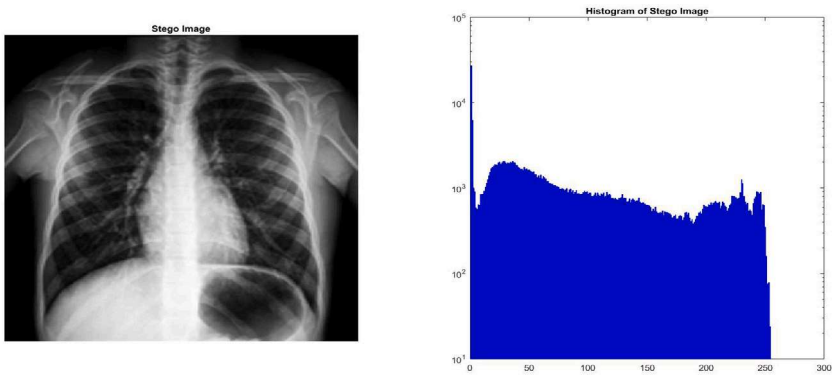


(b) Eye Stego

Fig. 15. Histogram analysis of the proposed HOG-LSB technique for the Eye cover and its stego-image.

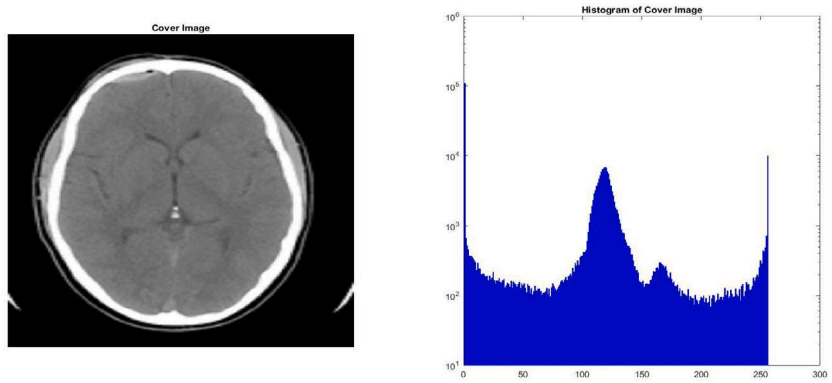


(a) Chest Cover

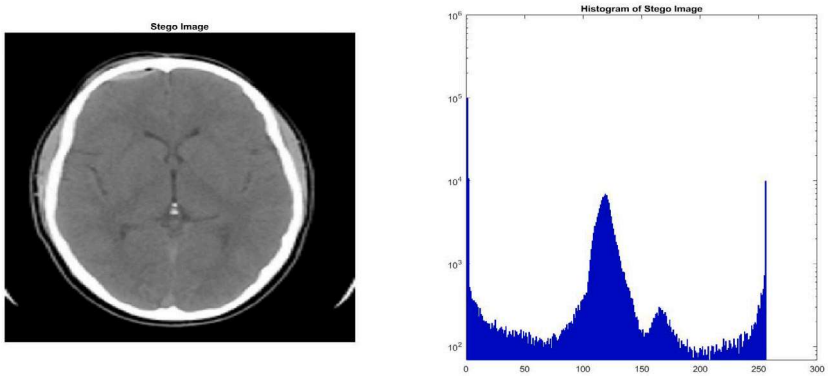


(b) Chest Stego

Fig. 16. Histogram analysis of the proposed HOG-LSB technique for the Chest cover and its stego-image.

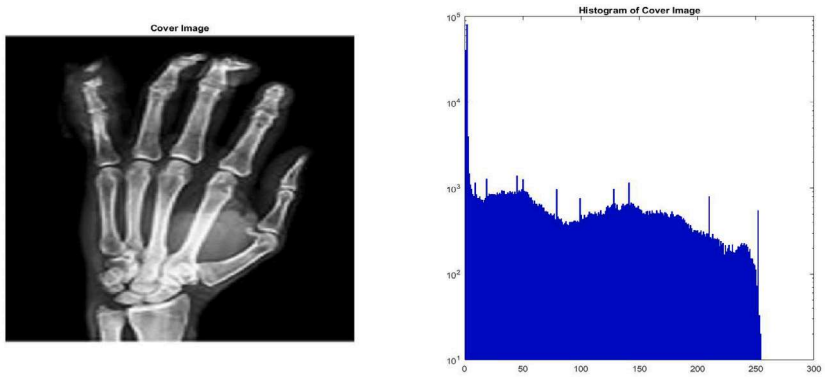


(a) Brain Cover

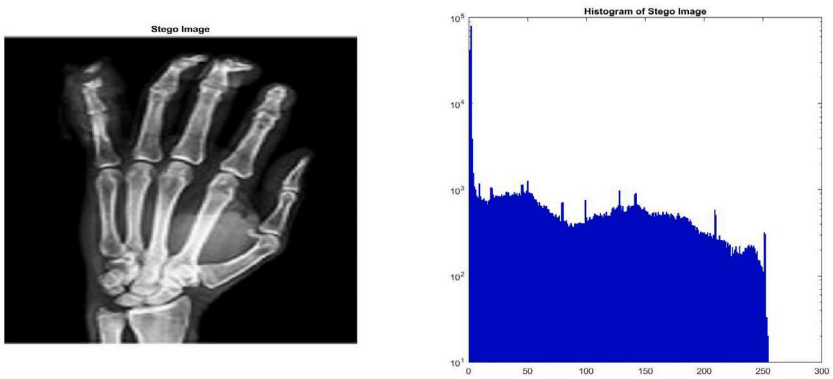


(b) Brain Stego

Fig. 17. Histogram analysis of the proposed HOG-LSB technique for the Brain cover and its stego image.



(a) Hand Cover

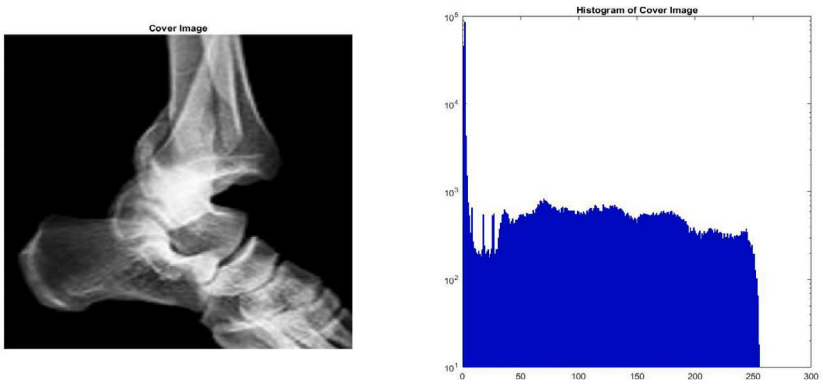


(b) Hand Stego

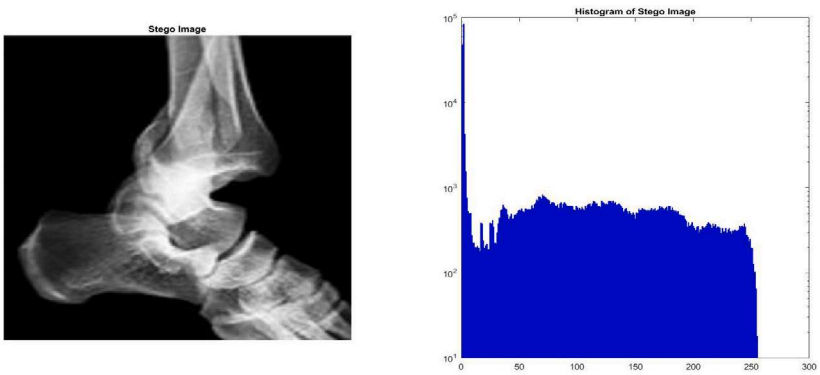
Fig. 18. Histogram analysis of the proposed HOG-LSB technique for the Hand cover and its stego-image.

Table 4
Obtained results of PSNR, NCC, SSIM, UQI, and APE of the proposed technique HOG-LSB at different metadata sizes of bits.

Medical Image	Patient Image (bits)	Metadata Size (bits)	PSNR (dB)	NCC	SSIM	UQI	APE
Brain	$56 \times 56 \times 3$	2000–3000	69.82	0.9988	0.9899	0.9799	3.25
		3000–4000	69.37	0.9986	0.9896	0.9789	3.54
		4000–5000	68.92	0.9980	0.9893	0.9779	3.83
		5000–6000	68.47	0.9960	0.9890	0.9769	4.12
Eye	$56 \times 56 \times 3$	2000–3000	69.87	0.9978	0.9898	0.9798	3.44
		3000–4000	69.22	0.9948	0.9885	0.9888	3.65
		4000–5000	68.57	0.9918	0.9882	0.9887	3.86
		5000–6000	67.92	0.9915	0.9879	0.9868	4.07
Kidney	$56 \times 56 \times 3$	2000–3000	65.49	0.9989	0.9875	0.9869	3.51
		3000–4000	65.04	0.9974	0.9881	0.9853	3.77
		4000–5000	64.59	0.9952	0.9877	0.9831	4.03
		5000–6000	64.14	0.9950	0.9873	0.9809	4.29
Chest	$56 \times 56 \times 3$	2000–3000	66.27	0.9981	0.9878	0.9868	3.68
		3000–4000	65.62	0.9951	0.9878	0.9876	3.95
		4000–5000	64.97	0.9921	0.9874	0.9874	4.22
		5000–6000	64.32	0.9891	0.9860	0.9872	4.49
Foot	$56 \times 56 \times 3$	2000–3000	69.49	0.9977	0.9889	0.9889	3.44
		3000–4000	69.04	0.9975	0.9896	0.9887	3.69
		4000–5000	68.59	0.9971	0.9893	0.9885	3.94
		5000–6000	68.14	0.9967	0.9890	0.9883	4.19
Hand	$56 \times 56 \times 3$	2000–3000	68.72	0.9978	0.9898	0.9788	3.14
		3000–4000	68.47	0.9975	0.9896	0.9887	3.55
		4000–5000	68.22	0.9952	0.9893	0.9876	3.96
		5000–6000	67.97	0.9929	0.9890	0.9865	4.37
Average			67.55	0.9959	0.9887	0.9859	3.83

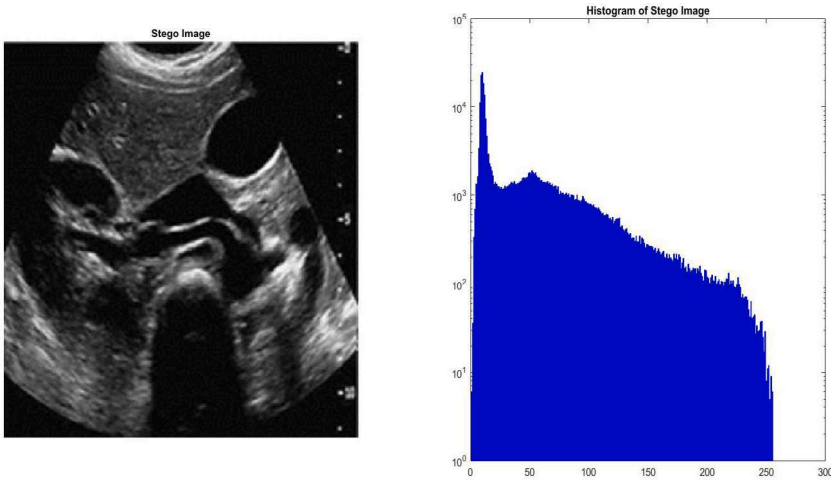


(a) Foot Cover

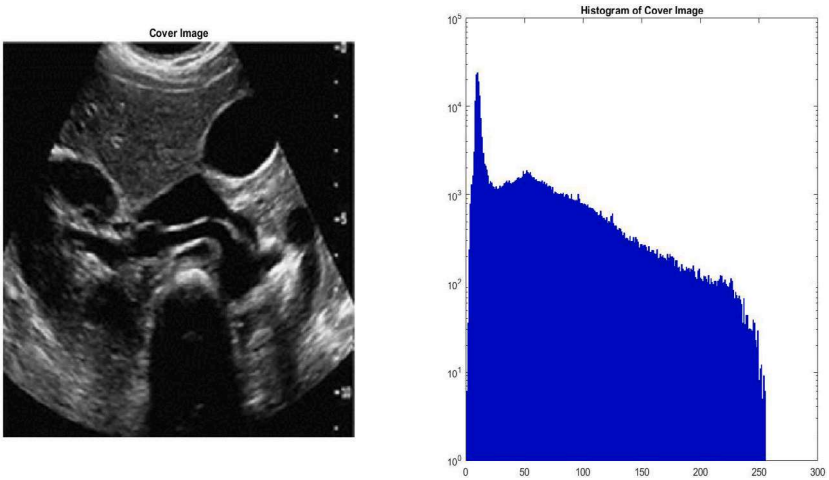


(b) Foot Stego

Fig. 19. Histogram analysis of the proposed HOG-LSB technique for the Foot cover and its stego-image.



(a) Kidney Cover



(b) Kidney Stego

Fig. 20. Histogram analysis of the proposed HOG-LSB technique for the Kidney cover and its stego-image.

Table 5
Comparison of the proposed technique with the state-of-the-art data hiding techniques in terms of various metadata sizes.

Image	Metadata size	Thiyagarajan and Aghila (2013)			Karakus and Avci (2020)			Ahmad et al. (2022)		
	(bits)	PSNR (dB)	MSE	SSIM	PSNR (dB)	MSE	SSIM	PSNR (dB)	MSE	SSIM
Brain	650–950	74.36	0	0.9844	75.55	0.01	0.9988	75.84	0.005	0.9998
	950–1250	73.22	0	0.9832	73.47	0.01	0.9988	73.67	0.005	0.9997
	1250–1550	72.14	0	0.9712	72.21	0.01	0.9988	72.61	0.005	0.9996
	1550–1850	71.58	0	0.9614	71.68	0.01	0.9888	71.74	0.005	0.9995
Eye	650–950	68.65	0.01	0.9862	69.41	0.01	0.9885	69.76	0.005	0.9997
	950–1250	67.21	0.01	0.9744	68.65	0.01	0.9888	69.35	0.005	0.9996
	1250–1550	66.17	0.02	0.9957	67.59	0.01	0.9888	68.57	0.005	0.9994
	1550–1850	65.53	0.02	0.9882	66.87	0.01	0.9888	67.37	0.005	0.9992
Kidney	650–950	68.32	0.01	0.9896	68.35	0.01	0.9888	68.35	0.005	0.9998
	950–1250	67.08	0.01	0.9832	66.47	0.01	0.9888	66.47	0.005	0.9997
	1250–1550	66.07	0.02	0.9832	66.18	0.01	0.9888	66.18	0.005	0.9996
	1550–1850	65.57	0.02	0.9832	66.04	0.01	0.9888	66.04	0.005	0.9995
Chest	650–950	72.84	0.01	0.9832	72.56	0.01	0.9888	72.56	0.005	0.9995
	950–1250	71.24	0.01	0.9832	71.39	0.01	0.9888	71.39	0.005	0.9994
	1250–1550	69.84	0.02	0.9832	69.89	0.01	0.9888	69.89	0.005	0.9993
	1550–1850	68.14	0.02	0.9832	68.44	0.01	0.9854	68.44	0.005	0.9992
Foot	650–950	72.84	0.01	0.9832	72.56	0.01	0.9888	72.56	0.005	0.9995
	950–1250	71.24	0.01	0.9832	71.39	0.01	0.9888	71.39	0.005	0.9994
	1250–1550	69.84	0.02	0.9832	69.89	0.01	0.9888	69.89	0.005	0.9993
	1550–1850	68.14	0.02	0.9832	68.44	0.01	0.9854	68.44	0.005	0.9992
Hand	650–950	68.65	0.01	0.9862	69.41	0.01	0.9885	69.76	0.005	0.9997
	950–1250	67.21	0.01	0.9744	68.65	0.01	0.9888	69.35	0.005	0.9996
	1250–1550	66.17	0.02	0.9957	67.59	0.01	0.9888	68.57	0.005	0.9994
	1550–1850	65.53	0.02	0.9882	66.87	0.01	0.9888	67.37	0.005	0.9992

Table 6
Comparison of the proposed technique with the state-of-the-art data hiding techniques in terms of various metadata sizes.

Image	Metadata size	Hameed, Hassaballah, et al. (2023)			Hussain and Khodher (2024)			Proposed HOG-LSB Technique		
	(bits)	PSNR (dB)	MSE	SSIM	PSNR (dB)	MSE	SSIM	PSNR (dB)	MSE	SSIM
Brain	650–950	69.82	0	0.9899	72.36	0.01	0.9877	**76.79**	0	**1.000**
	950–1250	69.37	0	0.9896	71.22	0.02	0.9865	**74.03**	0	**1.000**
	1250–1550	68.92	0	0.9893	70.08	0.02	0.9853	**73.29**	0	**1.000**
	1550–1850	68.47	0	0.989	68.94	0.03	0.9841	**71.82**	0	**1.000**
Eye	650–950	69.87	0.002	0.9888	69.95	0.01	0.9885	**76.57**	**0.001**	**0.9999**
	950–1250	69.22	0.003	0.9885	69.21	0.03	0.9848	**74.74**	**0.002**	**0.9999**
	1250–1550	68.57	0.004	0.9882	68.47	0.05	0.9811	**73.75**	**0.003**	**0.9998**
	1550–1850	67.52	0.005	0.9879	67.73	0.07	0.9774	**72.75**	**0.004**	**0.9999**
Kidney	650–950	65.49	0.002	0.9885	68.32	0.02	0.9877	**68.39**	**0.001**	**0.9997**
	950–1250	65.04	0.003	0.9881	67.08	0.03	0.9865	**67.94**	**0.002**	**0.9999**
	1250–1550	64.59	0.004	0.9877	66.07	0.04	0.9853	**66.96**	**0.003**	**0.9998**
	1550–1850	64.14	0.005	0.9873	65.57	0.05	0.9841	**66.63**	**0.004**	**0.9997**
Chest	650–950	66.27	0.002	0.9882	72.84	0.02	0.9765	**75.88**	**0.001**	**0.9999**
	950–1250	65.62	0.004	0.9878	71.24	0.03	0.9748	**71.85**	**0.002**	**0.9999**
	1250–1550	64.97	0.006	0.9874	69.84	0.04	0.9731	**69.95**	**0.003**	**0.9998**
	1550–1850	64.32	0.008	0.9866	68.14	0.05	0.9714	**68.93**	**0.004**	**0.9997**
Foot	650–950	69.49	0.003	0.9899	72.84	0.01	0.9877	**75.88**	**0.001**	**0.9999**
	950–1250	69.04	0.005	0.9896	71.24	0.01	0.9865	**71.85**	**0.002**	**0.9999**
	1250–1550	68.59	0.007	0.9893	69.84	0.03	0.9853	**69.95**	**0.003**	**0.9998**
	1550–1850	68.14	0.009	0.9897	68.44	0.03	0.9841	**68.93**	**0.004**	**0.9997**
Hand	650–950	68.72	0.002	0.9899	68.75	0.02	0.9765	**76.57**	**0.001**	**0.9999**
	950–1250	68.47	0.004	0.9896	67.21	0.03	0.9748	**74.74**	**0.002**	**0.9999**
	1250–1550	67.22	0.006	0.9893	67.47	0.03	0.9731	**73.75**	**0.003**	**0.9998**
	1550–1850	67.57	0.008	0.9895	67.63	0.04	0.9754	**72.75**	**0.004**	**0.9999**

7. Conclusion

In this paper, a data-hiding technique based on the HOG-LSB method to embed Electronic Patient Records (EPR) inside Digital Imaging and Communications in Medicine (DICOM) medical images is demonstrated. Using the HOG edge detector, a collection of regions of non-interest (RONI) is selected to hide a secret image and metadata from the DICOM file using the LSB replacement approach. The patient RGB image is encrypted using ANC-SHA-256. Then, we allocate a digital signature for each DICOM file using the SHA-256 algorithm to verify the precision of the contents using a private key. Many experiments were conducted to test visual quality assessment with various medical datasets containing, MRI, CT, X-ray, and ultrasound as cover images. While the LFW dataset is selected to be patient secret images. It can be conclude that the PSNR average of 67.55, the NCC average is 0.9959, the SSIM average is 0.9887, the UQI average is 0.9859 and the APE average is 3.83. Further, it concludes the robustness and the physical measure of change in the stego-images generated by the method. Moreover, the proposed technique achieves robustness against various geometric attacks and histogram analysis. Besides, the proposed method outperforms the state-of-the-art approaches in visual quality metrics PSNR, MSE, and SSIM with respect to six categories of testing medical images. Finally, the proposed method is very effective in telemedicine applications as it can increase the security of the EPR

during its transmission over the Internet from different remote places while maintaining visual quality images.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This study is supported via funding from Prince sattam bin Abdulaziz University project number (PSAU/2024/R/1445).

Appendix

Table 7 lists the abbreviations and their explanations, which have been used throughout the paper.

Table 7
Abbreviations that have used throughout the paper.

Abbreviation	Explanation
APE	Average Absolute Pixel Error
ANC	Adversarial Neural Cryptography
CT images	Computed Tomography images
DICOM	Digital Imaging and Communications in Medicine
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
EPR	Electronic Patient Record
ECDSA	Elliptic Curve Digital Signature Algorithm
HOGs	Histogram of Oriented Gradients
HVS	Human Visual System
IWT-DCT	Integer Wavelet Transform-Discrete Cosine Transform
LSB	Least Significant Bit
MSE	Mean Square Error
PSNR	Peak Signal-To-Noise Ratio
PACS	Picture Archiving and Communication Systems
PDI	Patient Diagnosis Information
RONIs	Regions of Non-Interest
RONs	Regions of Interest
SHA-256	Secure Hash Algorithm with 256-bit
SSIM	Structural Similarity Index
UQI	Universal Quality Index

References

Abdel Hameed, M., Aly, S., & Hassaballah, M. (2018). An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). *Multimedia Tools and Applications*, *77*(12), 14705–14723.

Abdul, W. (2022). Security of medical images over insecure communication channels using zero-steganography. *International Journal of Distributed Sensor Networks*, *18*(2), Article 15501477211006347.

Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., et al. (2022). Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal*, *61*(12), 10577–10592.

Al-Chaab, W., Abduljabbar, Z. A., Abood, E. W., Nyangaresi, V. O., Mohammed, H. M., & Ma, J. (2023). Secure and low-complexity medical image exchange based on compressive sensing and LSB audio steganography. *Informatica*, *47*(6), 65–74.

Amirtharajan, R., & Rayappan, J. B. (2012). An intelligent chaotic embedding approach to enhance stego-image quality. *Information Sciences*, *193*, 115–124.

Cedillo-Hernandez, M., Cedillo-Hernandez, A., Nakano-Miyatake, M., & Perez-Meana, H. (2020). Improving the management of medical imaging by using robust and secure dual watermarking. *Biomedical Signal Processing and Control*, *56*, Article 101695.

Ch, R., Srivastava, G., Gadekallu, R., et al. (2024). ECDSA-based tamper detection in medical data using a watermarking technique. *International Journal of Cognitive Computing in Engineering*, *5*, 78–87.

Chang, C.-C., Tsai, P., & Lin, M.-H. (2004). An adaptive steganography for index-based images using codeword grouping. In *Pacific-rim conference on multimedia* (pp. 731–738). Springer.

Chowdhuri, P., Pal, P., & Si, T. (2023). A novel steganographic technique for medical image using SVM and IWT. *Multimedia Tools and Applications*, *82*(13), 20497–20516.

Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. In *IEEE computer vision and pattern recognition*: *vol. 1*, (pp. 886–893). IEEE.

Denemark, T. D., Boroumand, M., & Fridrich, J. (2016). Steganalysis features for content-adaptive JPEG steganography. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1736–1746.

Ding, Y., Wang, Z., Qin, Z., Zhou, E., Zhu, G., Qin, Z., et al. (2023). Backdoor attack on deep learning-based medical image encryption and decryption network. *IEEE Transactions on Information Forensics and Security*, *19*, 280–292.

Durafe, A., & Patidar, V. (2023). An insight into image steganography for medical informatics. In *Cloud computing in medical imaging* (pp. 217–241). Auerbach Publications.

Goel, S., Gupta, S., & Kaushik, N. (2015). Image steganography–least significant bit with multiple progressions. In *3rd international conference on frontiers of intelligent computing: theory and applications* (pp. 105–112). Springer.

Gu, Q., Xiao, Y., Yuan, L., Shen, M., Zhang, F., Liao, H., et al. (2024). Image retrieval of colored spun fabrics based on variable weight and semantic features. *The Journal of the Textile Institute*, 1–7. http://dx.doi.org/10.1080/00405000.2024.2318683.

Hameed, M. A., Abdel-Aleem, O. A., & Hassaballah, M. (2023). A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. *Journal of Ambient Intelligence and Humanized Computing*, *14*, 4639–4657.

Hameed, M. A., Hassaballah, M., Aly, S., & Awad, A. I. (2019). An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. *IEEE Access*, *7*, 185189–185204.

Hameed, M. A., Hassaballah, M., Bekhet, S., Narmatha, C., & Kenk, M. A. (2023). A high quality secure medical image steganography method. In *3rd international conference on computing and information technology* (pp. 465–470). IEEE.

Haripriya, V., Vishal Gupta, M., Nadkarni, N., Malik, S., Yadav, A., & Joshi, A. (2024). Enhanced radial base deep learning algorithm for predicting multimedia security issues. *Journal of Intelligent & Fuzzy Systems*, *46*(2), 4829–4840.

Hassaballah, M., Hameed, M. A., Aly, S., & AbdelRady, A. (2020). A color image steganography method based on ADPVD and HOG techniques. In *Digital media steganography: principles, algorithms, and advances* (pp. 17–40). Academic Press, ISBN: 978-0-12-819438-6.

Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A novel image steganography method for industrial internet of things security. *IEEE Transactions on Industrial Informatics*, *17*(11), 7743–7751.

Hegde, P., & Maddikunta, P. K. R. (2023). Amalgamation of blockchain with resource-constrained IoT devices for healthcare applications–State of art, challenges and future directions. *International Journal of Cognitive Computing in Engineering*, *4*, 220–239.

Hua, C., Wu, Y., Shi, Y., Hu, M., Xie, R., Zhai, G., et al. (2023). Steganography for medical record image. *Computers in Biology and Medicine*, *165*, Article 107344.

Huang, X., Dong, Y., Ye, G., Yap, W.-S., & Goi, B.-M. (2023). Visually meaningful image encryption algorithm based on digital signature. *Digital Communications and Networks*, *9*(1), 159–165.

Huang, G. B., Mattar, M., Berg, T., & Learned-Miller, E. (2008). Labeled faces in the wild: A database for studying face recognition in unconstrained environments. In *Workshop on faces in real-life'images: detection, alignment, and recognition* (pp. 1–12).

Hussain, A. Z., & Khodher, M. A. A. (2024). Securing medical images using chaotic map encryption and LSB steganography.. *Revue d'Intelligence Artificielle*, *38*(1), p313.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K.-H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46–66.

Iqbal, S., Qureshi, A. N., Aurangzeb, K., Alhussein, M., Wang, S., Anwar, M. S., et al. (2024). Hybrid parallel fuzzy CNN paradigm: Unmasking intricacies for accurate brain MRI insights. *IEEE Transactions on Fuzzy Systems*, http://dx.doi.org/10.1109/TFUZZ.2024.3372608.

Karakus, S., & Avci, E. (2020). A new image steganography method with optimum pixel similarity for data hiding in medical images. *Medical Hypotheses*, *139*, Article 109691.

Khan, J., Li, J. P., Ahamad, B., Parveen, S., Haq, A. U., Khan, G. A., et al. (2020). SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. *IEEE Access*, *8*, 15747–15767.

Li, B., Tan, S., Wang, M., & Huang, J. (2014). Investigation on cost assignment in spatial image steganography. *IEEE Transactions on Information Forensics and Security*, *9*(8), 1264–1277.

Ma, Z., Zhang, W., Fang, H., Dong, X., Geng, L., & Yu, N. (2021). Local geometric distortions resilient watermarking scheme based on symmetry. *IEEE Transactions on Circuits and Systems for Video Technology*, *31*(12), 4826–4839.

Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. *Multimedia Tools and Applications*, 1–45.

McEvoy, F. J., & Svalastoga, E. (2009). Security of patient and study data associated with DICOM images when transferred using compact disc media. *Journal of Digital Imaging*, *22*(1), 65–70.

Memon, N. A., & Gilani, S. (2008). NROI watermarking of medical images for content authentication. In *IEEE international multitopic conference* (pp. 106–110). IEEE.

Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. arXiv preprint arXiv:1503.00388.

Nguyen, T. D., Arch-Int, S., & Arch-Int, N. (2016). An adaptive multi bit-plane image steganography using block data-hiding. *Multimedia Tools and Applications*, *75*(14), 8319–8345.

Olvera-Martinez, L. A., Cedillo-Hernandez, M., Diaz-Rodriguez, C. A., & Jimenez-Borgonio, E. T. (2022). Secure exchange of medical images via extended visual cryptography. *Revista Mexicana de Ingeniería Biomédica*, *43*(2).

Ping, P., Wei, P., Fu, D., Guo, B., Bloh, O. T., & Xu, F. (2024). IMIH: Imperceptible medical image hiding for secure healthcare. *IEEE Transactions on Dependable and Secure Computing*, http://dx.doi.org/10.1109/TDSC.2024.3355165.

Prabhavathi, K., Anandaraju, M., & Ravi, V. (2023). Region based medical image encryption using advanced zigzag transform and 2D logistic sine map (2DLSM). *International Journal of Cognitive Computing in Engineering*, *4*, 349–362.

Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, *27*, 45–60.

Qin, X., Li, B., Tan, S., Tang, W., & Huang, J. (2022). Gradually enhanced adversarial perturbations on color pixel vectors for image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, *32*(8), 5110–5123.

Rajaram, G., Dash, S., Arslan, F., Venu, D., Ahmed, M. A., & Lydia, E. L. (2023). Polynomial cryptographic optical steganography substitution model for the telehealth system with multimedia data. *Optical and Quantum Electronics*, *55*(9), 819.

Ramasamy, M. D., Periasamy, K., Periasamy, S., Muthusamy, S., Panchal, H., Solanki, P. A., et al. (2022). Design of adaptive hybrid classification model using genetic-based linear adaptive skipping training (GLAST) algorithm for health-care dataset. *Advances in Computational Intelligence*, *2*(2), 1–10.

Roy, S., Islam, M., et al. (2022). A hybrid secured approach combining LSB steganography and AES using mosaic images for ensuring data security. *SN Computer Science*, *3*(2), 1–12.

Sahoo, S., & Sahoo, S. S. (2020). A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans. In *17th India council international conference* (pp. 1–6). IEEE.

Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., & Chuang, H.-M. (2024). Privacy-aware and AI techniques for healthcare based on *k*-anonymity model in internet of things. *IEEE Transactions on Engineering Management*, *71*, 12448–12462.

Shen, S.-Y., & Huang, L.-H. (2015). A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Computers & Security*, *48*, 131–141.

Shtayt, B. A., Zakaria, N. H., & Harun, N. H. (2021). A comprehensive review on medical image steganography based on LSB technique and potential challenges. *Baghdad Science Journal*, *18*(2), 0957.

Singh, S., & Attri, V. K. (2015). State-of-the-art review on steganographic techniques. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *8*(7), 161–170.

Singh, K. N., Singh, O. P., Singh, A. K., & Agrawal, A. K. (2024). Watmif: Multimodal medical image fusion-based watermarking for telehealth applications. *Cognitive Computation*, *16*(4), 1947–1963.

Singla, D., & Juneja, M. (2014). New information hiding technique using features of image. *Journal of Emerging Technologies in Web Intelligence*, *6*(2), 237–242.

Taspinar, G., & Ozkurt, N. (2024). A review of ADHD detection studies with machine learning methods using rsfMRI data. *NMR in Biomedicine*, *37*(8), 1–23, Article e5138.

Thiyagarajan, P., & Aghila, G. (2013). Reversible dynamic secure steganography for medical image using graph coloring. *Health Policy and Technology*, *2*(3), 151–161.

Vanmathi, C., & Prabu, S. (2018). Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility. *International Journal of Fuzzy Systems*, *20*(2), 460–473.

Wu, J., Xia, W., Zhu, G., Liu, H., Ma, L., & Xiong, J. (2021). Image encryption based on adversarial neural cryptography and SHA controlled chaos. *Journal of Modern Optics*, *68*(8), 409–418.

Yan, F., Li, N., Iliyasu, A. M., Salama, A. S., & Hirota, K. (2023). Insights into security and privacy issues in smart healthcare systems based on medical images. *Journal of Information Security and Applications*, *78*, Article 103621.

Yang, A., Bai, Y., Xue, T., Li, Y., & Li, J. (2023). A novel image steganography algorithm based on hybrid machine learning and its application in cyberspace security. *Future Generation Computer Systems*, *145*, 293–302.

Yang, Y., Xiao, X., Cai, X., & Zhang, W. (2019). A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access*, *7*, 96900–96911.

Yuan, H.-D. (2014). Secret sharing with multi-cover adaptive steganography. *Information Sciences*, *254*, 197–212.

Zain, J. M., & Clarke, M. (2011). Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. arXiv preprint arXiv:1101.1603.

Zeng, K., Chen, K., Zhang, J., Zhang, W., & Yu, N. (2024). Towards secure and robust steganography for black-box generated images. *IEEE Transactions on Information Forensics and Security*, *19*, 3237–3250.

Zhu, X., Lai, Z., Liang, Y., Xiong, J., & Wu, J. (2022). Generative high-capacity image hiding based on residual CNN in wavelet domain. *Applied Soft Computing*, *115*, Article 108170.