Computers and Electrical Engineering 126 (2025) 110443

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Hybrid medical image encryption with compression framework for Internet of Medical Things

Anandbabu Gopatoti [a,*], James Stephen Meka [b], Poornaiah Billa [c]

[a] Department of Electronics and Communication Engineering, Wellfare Institute of Science, Technology and Management, Pinagadi, Andhra Pradesh, India
[b] Dr. BR Ambedkar Chair, Andhra University, Visakhapatnam, Andhra Pradesh, India
[c] Department of Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, Andhra Pradesh, India

ARTICLE INFO

Keywords:
Discrete Karhunen–Loève transform
Gray wolf optimization
Hybrid medical image encryption
Improved Henon Chaotic Map Encryption
Medical image compression
Watermarking

ABSTRACT

Patient medical data's security, storage, and transmission are critical challenges in healthcare systems, especially in the Internet of Medical Things (IoMT) environments. The vulnerability to attacks, higher computational costs, and loss of diagnostic quality are most often failures of the conventional encryption methods due to an imbalance between security and imperceptibility. This work focuses on developing a hybrid medical image encryption and compression (HMIEC) framework that uniquely integrates encryption, compression, and watermarking to address these issues. Initially, Improved Henon Chaotic Map Encryption (IHCME) was applied on the source image, which provides higher security. Then, the preprocessing operation is performed on the cover image, which converts the color space of the cover image. Further, the Discrete Karhunen–Loève Transform (DKLT) is applied to preprocessed and encrypted images. Moreover, a naturally inspired gray wolf optimization (GWO) algorithm selects the optimal embedding coefficients. Further, medical image embedding is performed using a GWO-based optimal embedding strength factor, where the preprocessed image hides the encrypted image and generates a watermarked image. Finally, a post-processing operation is performed on the watermarked image to generate a smoother watermarked image. The proposed HMIEC system resulted in improved peak signal-to-noise ratio (PSNR) by 77.04 dB, entropy of 41.923, mean square error (MSE) of 0.001283, structural similarity index metric (SSIM) of 0.991, normalizer correlation coefficient (NCC) of 0.992, compression ratio (CR) of 21.955%, the unified average change in intensity (UACI) of 99.60%, and the number of pixels change rate (NPCR) of 33.46% as compared to existing watermarking and security systems.

1. Introduction

Hospitals rely heavily on the internet of medical things (IoMT), which has recently grown in popularity. The global spread of COVID-19 has coincided with the rise in popularity of contactless medical treatment [1]. Through the IoMT platform, users transmit massive volumes of medical images. The block diagram of the IoMT environment is shown in Fig. 1. The IoMT collects data from the human body and relies on wireless connections and the internet to transmit it to a medical server, making it vulnerable to cyber-attacks due to its reliance on these technologies. This could compromise patient privacy rights and put their lives at risk. To effectively stop, identify, and counter these attacks in real-time, adhering to the necessary security standards is crucial [2,3].

* Corresponding author.
E-mail address: anandbabu.gopathoti@gmail.com (A. Gopatoti).

https://doi.org/10.1016/j.compeleceng.2025.110443
Received 20 December 2024; Received in revised form 9 May 2025; Accepted 10 May 2025
Available online 5 June 2025

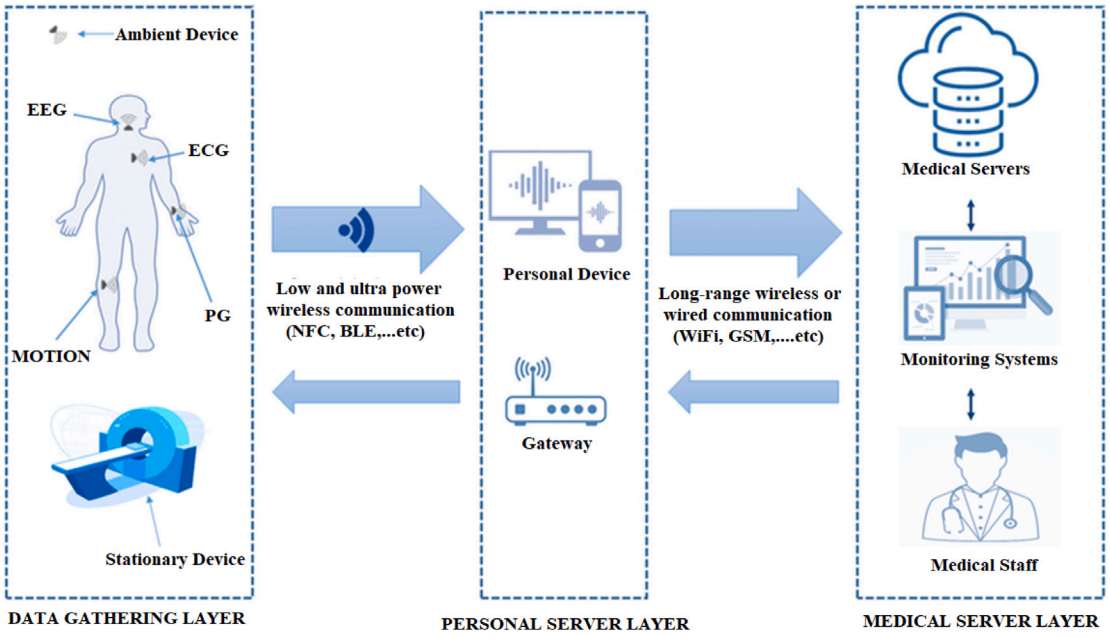

Fig. 1. Environment for IoMT applications.

IoMT healthcare systems have a data integrity feature to guarantee that data transported to its intended destination has not been tampered with in any way. It was being communicated wirelessly at the same time [4]. Maintaining the data integrity allows us to achieve this goal [5]. Medical data is sensitive and will be at risk if the unauthorized person gains access to the IoMT environment. It is more vulnerable as it has limited processing power and storage with different architectures, protocols, and security capabilities making it difficult to implement strong encryption and security measures. The IoMT devices that are connected to medical record storage data systems in the open network fail to update their firewalls, leading to vulnerability due to privilege elevation attacks [6]. Regularly updating the firewall can prevent these threats [7]. The centralized architectures are utilized to provide smart healthcare services to the patients by the healthcare systems through hospitals. The scalability is a significant challenge in these architectures as they use centralized servers, which are more vulnerable, causing considerable security risks, data confidentiality, and privacy challenges in maintaining patient records [8]. Data integrity is another significant challenge in IoMT, as these devices are often rely on wireless communication to exchange data, making them vulnerable to attacks [9]. Against these vulnerabilities, strong mechanisms of encryption are required essential when it comes to maintaining the confidentiality and integrity of medical data. Implementing encryption in the IoMT system is difficult due to resource constraints, making it impossible to implement traditional security protocols. Additionally, compliance with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) imposes mandatory strong encryption, security and access control to the sensitive medical data of the patient [10].

Numerous imagine encryption techniques can be used to guarantee the security of these images, according to existing research. Image encryption is the process of converting an unencrypted image into an encrypted one using a private key [11]. The decryption process restores the original image from the encrypted ones created using the cypher with the help of the private key. There is a significant degree of similarity between the encryption approach and the decryption process, even if the steps are applied in a different order [12]. The use of secret keys is crucial to encryption. Encryption makes use of both public and private keys.

A private key component utilized in both encryption and decryption processes is significantly responsible for the protection provided by the encryption approach [13]. Two keys are required in order to use a public key: one for encryption and another for decryption. The decryption key is always kept private and protected as secret information, even though the encryption key is revealed to the public in this case [14]. Current medical image security solutions often struggle with high computational costs, limited compatibility with low-power IoMT devices, weak resistance to differential attacks, and a lack of adaptability to image quality preservation. The proposed HMIEC framework addresses these limitations by uniquely integrating encryption, compression, and watermarking. The IHCME ensures lower correlation values, higher entropy, and strong encryption. The DKLT is employed for efficient compression and transformation, which reduces the data size without significant loss of diagnostic quality and is suitable for resource-constrained IoMT environments. The GWO also dynamically identifies optimal embedding strength factors to ensure a balanced trade-off between imperceptibility and robustness. Together, these components deliver enhanced resistance to statistical and differential attacks, reduced computational time, and compliance with data integrity and privacy requirements such as HIPAA and GDPR.

Medical image security is therefore one of the primary issues with this IoMT. Still, there is a potential that higher security, robustness, and imperceptibility would have been achieved with the traditional methods. The following list outlines the significant contributions of this work:

- Implementation of a novel HMIEC system with encryption, compression, and watermarking approaches.
- Implementation of IHCME for encryption of source image and development of DKLT for compression of encrypted images.
- Perform the cover image and encrypted image watermarking using DKLT using GWO-based embedding strength factor.
- The proposed HMIEC method improved PSNR, SSIM, MSE-based watermarking performance and entropy, NCC, UACI, NPCR based encryption performance compared to state-of-art recent works.
- When compared to conventional coding techniques, the suggested technique also enhanced compression performance.

The remaining sections in this paper are structured as follows: Section 2 provides a review of the literature on several watermarking and encryption techniques. Section 3 describes the proposed HMIEC system in detail, along with the results and discussions in Section 4 and research challenges and future work in Section 5. Finally, Section 6 provides a conclusion, discussing potential areas for future exploration.

2. Literature survey

This section gives a detailed analysis of related works with respect to watermarking, encryption or cryptography, and joint watermarking with encryption methods [15]. The authors have presented a unique watermarking approach for medical image watermarking that makes use of lifting (LWT) and discrete wavelet transform (DWT), which are employed here to embed the watermark information to create watermarked images of high quality [16]. These approaches are being investigated in further depth to establish a more solid system for copyright protection. However, the proposed methods are non-blind medical image watermarking schemes where there exists storage overhead, and computational complexity. The researchers developed a new effective and secure watermarking system based on DCT–DWT [17]. Firstly, the DCT technique was used to insert the cover image's watermark. However, the discrete cosine transform (DCT) technique was ineffective in lossless compression and attack-free environment. The association rules mining and texture analysis are utilized to overcome challenges with blind spatial domain-based image watermarking suffering from watermark distortions and computational overheads [18]. The concept is to locate the areas of the host images that are heavily textured to place the watermark. The texture is associated with human visual system (HVS). A new scheme that uses a mix of the least significant bit (LSB) and DWT-Singular Value Decomposition (SVD) domains, with the primary emphasis on providing appropriate solutions for limiting the impact of geometric attacks on the system [19]. To achieve this aim, the cover image is separated into four non-overlapping rectangular components known as sub-images. Then the hybrid technique is used to embed a watermark into each segment individually. However, these methods suffer from computational complexity and increased processing time. The utilization of Harris hawk's optimization (HHO) in the context of blind watermarking applications is proposed with the deep learning (DL) [20]. Compared to previous DL convolution neural network (DLCNN)-based methods, this approach eliminates most of the issues often encountered while simultaneously improving performance in terms of resilience and imperceptibility. However, these methods required more power, storage, loss of image quality and suffering from the computational complexity.

The following survey is focused on different medical image encryption methods. The steganography and cryptography are combined to safeguard the information in the medical images [21]. Initially, the message was encrypted using revised content-aware deoxyribonucleic acid (CA-DNA) algorithm to transform the message into a secret image. However, this DNA-based encryption methods suffers from the processing overhead with high computational complexity. A sharp frequency localized contourlet transform with a memristive ring neural network (MRNN) is implanted to tackle the false positive issue in the encryption strategy [22]. In addition, this technique is robust against ambiguity-based attacks, but there are energy efficiency concerns and hardware complexity. The lightweight cryptosystems based on Henon's chaotic map, Chen's chaotic approach, and Brownian motion for medical image encryption exist [23]. It is determined that the blocks with the lowest entropy values and the edges with the lowest entropy values are the optimal places to put the encrypted. However, the selection of the parameters is more sensitive. The tests were conducted on various images to evaluate the consistency of encryption findings using a V-Net CNN with a hyperchaotic system [24]. This CNN approach produced findings that were quite comparable with minimal variance across a variety of test images, but it is more computationally complex approach. An effective encryption model that includes the matrix transformation technique combined with Henon, Gaussian, and Logistic map (HGL) is developed to encrypt medical images [25]. Further, the HGL matrix factorization and LSB replacement were exploited to embed the watermark. Finally, the Q learning technique was employed for selecting the best host blocks. This model requires more execution time and storage.

The following sections are focused on joint watermarking and encryption methods. The watermarking process is divided into: an encoder, a decoder, and a detector sub-network [26]. The encoder sub-network utilizes the watermarking encryption method to encode data. It is also responsible for decoding the image watermarking embedding and extraction network. The normalized correlation (NC) reported greater than 0.55 in this watermarking process indicating the low watermarking capability. An accelerated-KAZE DCT (AKAZE-DCT) that embeds the watermarks superiorly by varying the mean value of the pixels is developed [27]. However, the proposed method introduces more computational complexity due to the DCT and KAZE feature extraction process. The multiplicative watermarks were considered, and then the AKAZE-DCT technique was utilized to change the pixel's variance. At the same time, the detection functions were also used to find the thresholds adaptively. A watermarking technique called multi-modal medical image fusion (WatMIF) in transform domain that utilizes low-frequency coefficients of the image is proposed [28]. As an

Table 1
Summary of literature with their key approaches and weaknesses.

Reference	Technique	Weaknesses
Vaidya SP [16]	Lifting wavelet transform and discrete wavelet transform	Storage overhead with more computational time
Amine K et al. [17]	Discrete cosine transform and Discrete Wavelet Transform	Ineffective in lossless compression and attack-free environment
Moad MS et al. [18]	Discrete Wavelet Transform	Watermark distortions and computational overheads
Singh P et al. [19]	LSB-DWT-SVD transforms	Significantly increased processing time
Chacko A et al. [20]	Harris hawk's optimization	Increased computational complexity and potential loss of image quality
Wu Y et al. [21]	DNA-based encryption	Processing overhead with high computational complexity
Lin H et al. [22]	Frequency localized contourlet transform and memristive ring neural network	Energy efficiency concerns and hardware complexity
Masood F et al. [23]	Lightweight cryptosystem	Sensitivity to small parameter variations
Wang X et al. [24]	V-Net CNN with a hyperchaotic system	Training overhead with lack of scalability
Abdelfatah RI et al. [25]	Matrix transformation technique combined with Henon, Gaussian, and Logistic map	More execution time and storage
Liu Z et al. [26]	Ridgelet-DCT transform along with Tent-Henon-Map	Limited effectiveness against attacks
Li D et al. [27]	Accelerated-KAZE DCT	Substantial computational overhead
Singh KN et al. [28]	Multi-modal medical image fusion	High computational complexity with lack of scalability
Balasamy K et al. [29]	Adaptive neuro-fuzzy region-based selection	More false positive rate
Gong C et al. [30]	Residual-DenseNet	Lack of generalization
Almaiah MA et al. [31]	Neural watermarking technique	High latency with more energy consumption

output, the trained WatMIF generates 1024-real numbers normalized according to N(0,1). Scalability is the major limitation of WatMIF.

Hybridizing an adaptive neuro-fuzzy region-based selection (ANFRS) with geometric invariance features of shape invariant exponents can be an initial approach for a reliable watermarking approach for color images. The technique of embedding the watermarks within the audio stream itself is designed to increase security while maintaining the original media, and thus, it is also appropriate for usage in copyright protection, digital rights management, and secure communications [29]. However, the false positive rate affects the diagnostic accuracy. A hybrid watermarking encryption approach based on Residual-DenseNet is proposed as universal and practicable based on the assessments obtained from subjective and objective aspects [30]. The performance of the DenseNet depends on the high training dataset; this dependency creates generalization problems. To demonstrate the resilience of the broad neural watermarking technique, regularly utilized attacks are made on encrypted–watermarked images to study the associated extracted watermarks, which in some cases still maintain sufficient identifiable characteristics [31]. The high latency with more energy consumption is the major problem in the neural watermarking technique. Table 1 provides an overview of the literature, the methodology, and the weaknesses.

3. Proposed method

Insecure watermarking systems are inadequate for copyright protection, fingerprinting, data authentication, and monitoring of digital information. Security is a significant challenge in medical imaging security measures. Different encryption techniques can be employed to ensure security, with the key being the factor that determines the amount of protection. The use of security measures can have advantageous effects on various industries such as telemedicine, digital imaging, telecommunications, multimedia data, and other related domains. Fig. 2 shows the block diagram of the proposed HMIEC. The use of the compression technique to carry out data compression and watermarking is a unique aspect of the HMIEC. In the beginning, IHCME was applied to the original image, giving a better security level. The cover picture must next go through the preprocessing step, which involves converting an image color space. In addition, the DKLT should be applied to both the preprocessed and the encrypted images. Both images are compressed using DKLT, which is also used for watermarking medical images. In addition, the GWO method, inspired by nature, is utilized to choose the best embedding coefficients. In addition, the operation of medical image embedding is carried out using a GWO-based optimum embedding strength factor. This hides the encrypted images inside the preprocessed image and creates a watermarked image. In the end, a post-processing procedure is conducted on the image that has been watermarked to obtain a watermarked image that is smoother. The extraction process is precisely in a reverse manner and restores the source medical image.

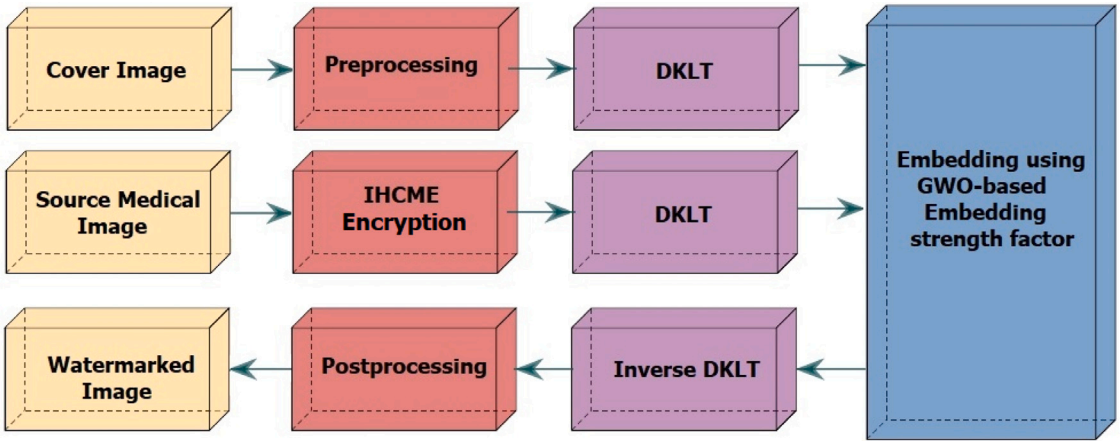

Fig. 2. Proposed Hybrid Medical Image Encryption and Compression (HMIEC) approach.

3.1. Preprocessing

Preprocessing is converting the original image's color space into brighter color space. Practically, the YC_bC_r color space is commonly used to take advantage of the HVS's low-resolution capacity for color and luminance. The perceptual quality of the encoded image is important for medical image security. The human eye is more sensitive to the changes in the luminance (Y) component than the changes in the chrominance (C_bC_r) components. For better separation of these components, YC_bC_r color space is utilized in the preprocessing compared to other color spaces, ensuring that the modifications in color information do not significantly degrade the perceptual quality of the encoded image. By working in the YC_bC_r, our preprocessing also aligns with the HVS properties to maintain high security. As a result, image processing approaches need this translation, which is becoming more popular for converting HVS color space. The following Eqs. (1)–(3) are used for converting RGB to YC_bC_r.

$$Y = 16 + (\frac{65.738 \times R}{256}) + (\frac{129.057 \times G}{256}) + (\frac{25.064 \times B}{256}) \tag{1}$$

$$C_b = 128 - (\frac{37.945 \times R}{256}) + (\frac{74.494 \times G}{256}) + (\frac{112.439 \times B}{256}) \tag{2}$$

$$C_r = 128 + (\frac{112.439 \times R}{256}) + (\frac{94.154 \times G}{256}) + (\frac{18.285 \times B}{256}) \tag{3}$$

3.2. Embedding algorithm

The medical image embedding is performed using a GWO-based optimal embedding strength factor (λ). The GWO algorithm for selection of embedding strength factor is visualized in Fig. 3. The population of gray wolves represents the different embedding strength factor values (λ), which are initialized randomly in GWO algorithm for selection of embedding strength factor. This factor adjusts the pixels adaptively to keep the encryption process secure (entropy and correlation), as well as imperceptibility (PSNR and SSIM). The objective function $f(\lambda)$ is formulated based on entropy, correlation coefficients, PSNR, and SSIM. Each wolf in GWO represents the possible λ-value. The wolves follow a social leadership hierarchy while hunting in GWO. The same hunting behavior is considered for selecting the best λ-value based on evaluating the fitness or objective functions $f(\lambda)$ using Eq. (4).

$$f(\lambda) = w_1 * \text{Entropy} + w_2 * \text{NCC} + w_3 * \text{SSIM} + w_4 * \text{PSNR} \tag{4}$$

where, w_1, w_2, w_3, and w_4 are weights to control the trade-off between security and quality. The GWO is used to find the best λ factor by maximizing $f(\lambda)$ with hunting strategy of gray wolves where the candidate solutions (λ-values) are adjusted iteratively. The best three candidate solutions, which are the top three candidate solutions in GWO based on the hunting behavior of the wolves, are assigned as α, β, and δ. In contrast, the remaining solutions are considered as omega (ω). These three solutions represent the best values for the λ. The wolves present in the hunting change their position adaptively by changing the control coefficients parameters such as A and C. As the best wolf is selected as the best candidate solution in GWO, the best λ-values are selected as the optimal value for watermarking. The highest fitness wolf indicates the best λ value obtained upon algorithm converging.

The position update for λ is obtained by calculating the distance (D) between the current position of the gray wolf (X_g), which is the candidate solution, and the position of the prey (X_p), which is the best-known solution so far. The distance D is formulated in Eqs. (5)–(6).

$$D = \left| C \cdot X_p - X_g \right| \tag{5}$$

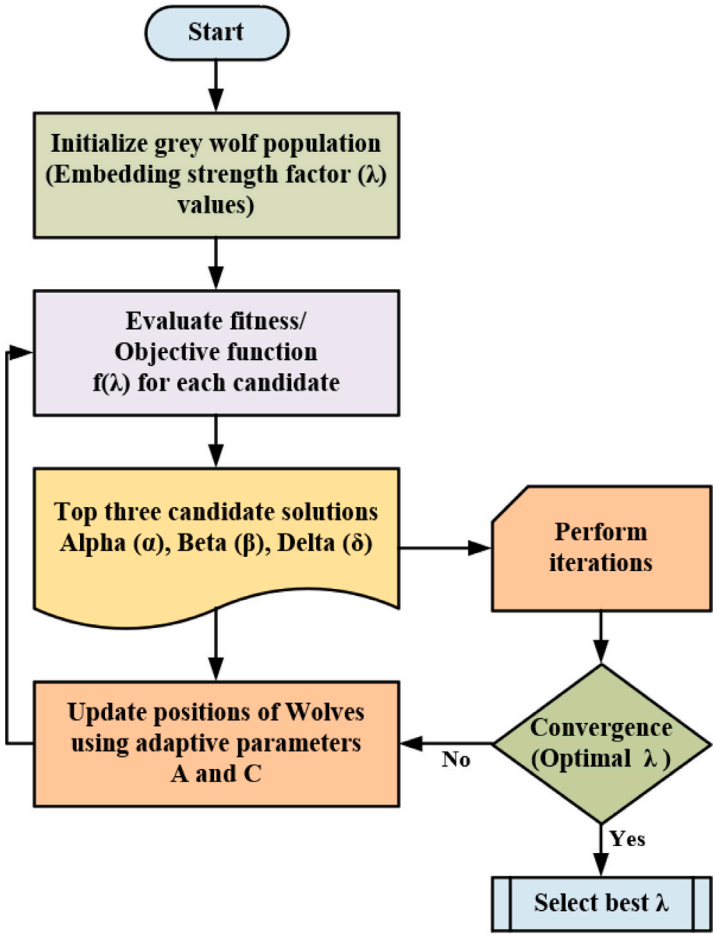

Fig. 3. GWO algorithm for selection of embedding strength factor.

$$\lambda_{\text{new}} = \lambda_p - A \cdot D \tag{6}$$

where, λ_p best-known solution, X_g is current solution, λ_{new} is the new updated position of the candidate solution, and A and C are adaptive control coefficients. Different λ values are evaluated by the fitness function and select the one that provides the best trade-off between security and image quality. The GWO is computationally efficient as it contains fewer control parameters than the particle swarm optimization (PSO) and genetic algorithm (GA). GWO adjusts exploration and exploitation dynamically with its leadership hierarchy and reduces local optima trapping. However, PSO may fall into diverse search space exploration, and GA requires fine-tuned mutation rates for better optimal results. A thorough analysis of the embedding procedure is provided as step by step as follow:

Step 1: First, choose and read the medical image and cover or host color image, that is watermarking image.

Step 2: Use color space transformation called YC_bC_r to convert the given watermarking (cover) image as shown in Eqs. (1)–(3), where it comprises the components such as luminance, chroma red, and chroma blue. In practical terms, chroma red and chroma blue include low-intensity elements. Hence, it will be easy to embed the watermark image into watermarking image precisely.

Step 3: Use DKLT [32] to transform the obtained three YCbCr color spaces to return their unitary versions cited as $DKLT_u$. Here, DKLT also compresses the source image and reduces the cover image size.

Step 4: Now, isolate the *R*, *G*, and *B*-channels from the obtained $DKLT_u$ and represent them with $DKLT_{u_r}$, $DKLT_{u_g}$, and $DKLT_{u_b}$, respectively.

Step 5: Implement a meta-heuristic optimization technique inspired by the wolves called GWO [33] for obtaining the optimal embedding strength coefficients from $DKLT_{u_r}$, $DKLT_{u_g}$, and $DKLT_{u_b}$ with enhanced embedding strength.

Step 6: In addition, use the IHCME algorithm illustrated in Table 2 to obtain an encrypted medical image (W_{HE}). $DKLT_{W_r}$

Table 2
IHCME algorithm.

Phase 1: Logistic function development with confusion
Step 1: Introduce the various metrics such as probabilities (p), array index (x), and range (r). Step 2: Estimate the number of elements (s) from the source image. Step 3: Develop the logistic analysis as follows: for $n = 1 : (s-1)$ $x(n+1) = r \star x(n) \star (1 - x(n))$; end Step 4: Perform sorting operation between resultant array elements based on their indexes. Step 5: Based on index properties, develop the confusion.
Phase 2: Henon chaotic approach based key generation
The Lorenz map is simplified using the advanced properties of the 2D-Dynamic map of the Henon chaotic approach and is derived as follows. $x_{i+1} = 1 - (a * x)_i^2 + y_i$ $y_{i+1} = b * (x_i), i = 1, 2, \ldots$ Here, a and b are the fundamental initialization metrics, x_0 and y_0 represents the initial point. Further, x_{i+1} and y_{i+1} represent the new points generated from the present x_n and y_n points. In addition, all these points are interconnected by a Henon map and generate the synchronized key. Finally, diffusion of key points is formed, which generates the new pixels as follows: $\begin{bmatrix} x(i+1) \\ y(i+1) \end{bmatrix} = \begin{bmatrix} 1 - 1.4x^2(i) + y(i) \\ 0.3x(i) \end{bmatrix}, i = 0, 1, 2...$ Here, new pair values are generated from $\overline{x}\ \overline{y}$ resulting in $(x(i+1), y(i+1))$ Further, the scrambled image is generated by a diffusion process based on image size for iterations.
Phase 3: Final encryption
Step 1: Perform the transpose operation on Phase 1 output. Step 2: Perform logical XOR formulation between the Phase 2 generated key and the step 1 outcome. Step 3: Finally, reconstruct and generate the encrypted image.

Step 7: Use $DKLT$ to transform the obtained W_{HE} to return their unitary versions cited as $DKLT_W$. Now, isolate the R, G, and B-channels from the obtained $DKLT_W$ and represent them with $DKLT_{W_r}$, $DKLT_{W_g}$, and $DKLT_{W_b}$, respectively. Here, $DKLT$ compresses the source image and reduces the watermark image size.

Step 8: Use the embedding strength formulation to embed the $DKLT_{W_r}$, $DKLT_{W_g}$, and $DKLT_{W_b}$ into optimized $DKLT_{u_r}$, $DKLT_{u_g}$, and $DKLT_{u_b}$, respectively, and returns the modified $DKLT_{E_r}$, $DKLT_{E_g}$, and $DKLT_{E_b}$.

Step 9: Reconstruct the decomposed image by applying $IDKLT$ on $DKLT_{E_r}$, $DKLT_{E_g}$, and $DKLT_{E_b}$.

Step 10: Finally, apply the inverse transformation of YC_bC_r to RGB color format to obtain the watermarked output image from the inverse $DKLT$ outcome.

The IHCME algorithm integrates dual maps, such as a logistic map (for confusion) and a Henon chaotic map (for key generation and diffusion). This dual map integration strengthens randomness and unpredictability, making it more secure than other chaotic maps. The IHCME shows lower correlation values and higher entropy, ensuring strong encryption compared to the conventional chaotic maps such as lorenz, tent, and arnold. The IHCME algorithm is implemented by carefully selecting the key parameters to ensure strong security and chaotic behavior. The initial conditions in the Henon chaotic map for the initial point (x_0, y_0) are set at (0.1, 0.1). The fundamental initialization metrics, such as a and b, are the control parameters set at a = 1.4 and b = 0.3. The encryption key provides a 128-bit key space comprised (x_0, y_0, a, b) along with a logistic map to enhance the resistance against brute-force attacks. The number of iterations is tuned to MxN for each input image of the size MxN to maximize the randomness of the encryption sequence. The interaction between the IHCME, DKLT, and GWO is carefully designed and is performed sequentially to build an efficient, robust, and secured medical image encryption and compression framework that is suitable for IoMT. This sequential interaction begins with generating dual maps, such as a logistic map (for confusion) and a chaotic map (for key generation and diffusion), using the proposed IHCME algorithm to encrypt the original medical source image. Simultaneously, the DKLT is applied on both the encrypted and the preprocessed cover image, achieving compression and dimensionality reduction while preserving essential image features by transforming the images into unitary forms suitable for embedding. Following DKLT, GWO finds the optimal embedding strength factor (λ) that controls how strongly the encrypted image is embedded into the cover image in the DKLT domain. Thus, IHCME improves security by securing the content in the image, DKLT compresses and prepares the encrypted images for embedding, and GWO ensures that embedding is performed with optimal strength, maintaining a trade-off between security and visual quality.

3.3. Extraction process

An extensive study of the extraction procedure is provided in this section. Here, the original source image is extracted from the encrypted–watermarked image. Fig. 4 shows the extraction process of HMIEC. The IHCME decryption minimizes the potential data loss during the decryption process by strictly following the inverse transformation of the IHCME encryption algorithm, ensuring the

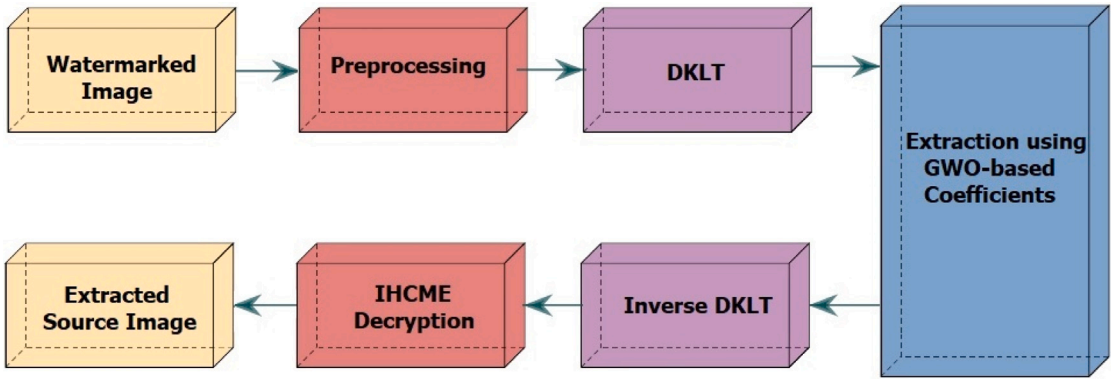

Fig. 4. Proposed HMIEC-based extraction approach.

lossless reconstruction of the original medical image. The DKLT and inverse DKLT transformations used in the extraction process will provide better compression and transformation without introducing the artifacts further. Furthermore, the optimized embedding strength factor (λ) reduces the potential distortions by maintaining the balance between imperceptibility and recoverability.

DKLT preserves more important medical information in the image due to its lower compression ratio compared to traditional compression techniques such as Joint Photographic Experts Group 2000 (JPEG2000) and Set Partitioning in Hierarchical Trees (SPIHT). The reconstruction quality of the DKLT lossless compression technique is higher due to the high values of PSNR and SSIM compared to the traditional JPEG2000 and SPIHT compression techniques. The following steps give a detailed analysis of extraction approach.

Step 1: First, read the outcome of embedding that is watermarked image and apply the color space transformation that is YC_bC_r.

Step 2: Use $DKLT$ to transform the obtained three YC_bC_r color spaces to return their unitary versions cited as $DKLT_u$.

Step 3: Now, isolate the R, G, and B-channels from the obtained $DKLT_u$ and represent them with $DKLT_{u_r}$, $DKLT_{u_g}$, and $DKLT_{u_b}$, respectively.

Step 4: Implement GWO to obtain optimal coefficients from $DKLT_{u_r}$, $DKLT_{u_g}$, and $DKLT_{u_b}$.

Step 5: Implement the extraction process to extract the (W_{HE}) from step 4 and apply IDKLT to reconstruct the modified $DKLT_u$.

Step 6: Use the IHCME decryption algorithm (reverse to the algorithm presented in Table 2) to obtain the decrypted original color medical image W_{DE}.

Step 7: Final medical image is generated by performing YC_bC_r to RGB color space conversion.

The proposed HMIEC framework uniquely combines compression and watermarking using the Discrete Karhunen–Loève Transform (DKLT), improving transmission efficiency and security while preserving diagnostic image quality. This makes it ideal for IoMT applications.

4. Results and discussions

A comprehensive evaluation of the simulation results produced using Matlab R2021a is provided in this section. Compared to existing approaches, the simulation results show that the proposed HMIEC method increased PSNR, SSIM, MSE-based watermarking performance and entropy, NCC, UACI, and NPCR-based encryption performance with CR-based compression performance. Additionally, the performance of the proposed approach is evaluated by comparing it to other ways that utilize the same dataset.

4.1. Datasets

A collection of different images from a variety of popular medical image collections were investigated in this study. A small number of samples from the Indian Diabetic Retinopathy Image Dataset (IDRiD) [34] contain ocular retinal image such as diabetic retinopathy (DR) and diabetic macular edema (DME) are present in the dataset utilized in this work. In addition, an additional group of cover images from the COVIDX dataset [35], which are images based on chest x-rays (CXR) containing information on the COVID-19 disease, are considered. In addition, only a small number of samples from the International Skin Imaging Collaboration (ISIC) dataset [36] are considered. This dataset contains images of skin lesions caused by benign and malignant diseases. In this study, the proposed method is evaluated on the diverse medical images taken from these datasets to ensure variation in image modality and pathology. However, testing on a broader range of other high-resolution images, such as magnetic resonance imaging

(MRI) and computerized tomography (CT), was not explicitly considered in this study to further validate the robustness of our proposed method. However, the proposed framework is scalable for large-scale medical databases and high-resolution imaging formats, including digital imaging and communications in medicine (DICOM), MRI, and CT images. The use of DKLT and GWO ensures efficient compression, significantly reducing storage requirements and transmission bandwidth while maintaining diagnostic integrity. The integration of HMIEC with Picture Archiving and Communication Systems (PACS) enables encrypted storage and retrieval of large-scale medical databases.

4.2. Performance metrics

The mathematical analysis of the many performance measurements employed in this work is provided in depth in this section. The PSNR is the image quality metric, which shows the improvement of the outcome by measuring the extracted image concerning the original image. A higher value of PSNR indicates less distortion and better preservation of the image quality with good visual fidelity in diagnosis. The MSE indicates how closely the recovered image resembles the original and is required where precision is essential in medical applications. The PSNR and MSE are defined mathematically in Eqs. (7)–(8).

$$PSNR = 10\log_{10}[\frac{255^2}{MSE}] \tag{7}$$

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[I(x,y) - O(x-y)]^2 \tag{8}$$

Here, the number of rows and columns are represented by N, and M. Further, y and x are image spatial coordinates of the watermark image (I), and O represents the watermarked image output. The NCC metric quantifies recovery by measuring the similarity between the recovered and original images. Its range is about 0 to 1. A high NCC indicates better similarity and can be calculated using Eq. (9).

$$NCC = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I(x,y) \star O(x,y)}{\sqrt{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I(x,y)^2 \star \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} O(x,y)^2}} \tag{9}$$

The perceptual image quality depends on luminance, contrast, and structural information. The SSIM evaluates the perceptual quality using Eq. (10) in the range of 0 to 1. A higher value indicates that recovered and original images are identical, confirming that the recovered and original images have similar structural features.

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_{x^2} + \mu_{y^2} + c1)(\sigma x^2 + \sigma y^2 + c_2)} \tag{10}$$

Here, μ_y and μ_x are the means of $\{y, x\}$, σy^2 and σx^2 are the variances of $\{y, x\}$, σ_{xy} is the covariance between $\{y, x\}$, $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ are narrow band denominator metric. Further, L is the dynamic range and constant metrics such as $k_2 = 0.03$ and $k_1 = 0.01$. The average intensity change between encrypted and original images depends on the alteration of the pixel values ensuring the resistance to differential attacks. This average intensity is measured by the UACI in the range of 0% to 100% using Eq. (11). A higher value indicates that maximum possible change in pixel intensities, this makes it extremely difficult for attackers to retrieve the original image, thus enhancing security.

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\frac{|I(i,j) - O(i,j)|}{255}\right] \times 100\% \tag{11}$$

The entropy metric measures the randomness of the pixels distributed in the encrypted image. This randomness ranges from 0% to 100% and is calculated using Eq. (12). A higher value indicates better security, as an ideal encrypted image should exhibit near-uniform pixel distribution to resist statistical attacks.

$$Entropy = -sum(p. \star \log 2(p)) \tag{12}$$

Here, p contains the normalized histogram counts returned from image histogram. A strong security method against various attacks produces a moderate to higher value of NPCR ranging from 0% to 100%. It measures the difference in pixel values between the original and encrypted images using Eq. (13).

$$NPCR = \frac{1}{M \times N}\sum_{i,j} D(i,j) \times 100\% \tag{13}$$

Here, D(i,j) represents the difference between [(I(i,j),O(i,j))]. The image storage and transmission costs are the two essential factors to consider while maintaining image quality in medical image encryption and decryption. The CR metric measures compression efficiency using Eq. (14), which provides how much image size is reduced after compression.

$$CR = \frac{Uncompressed\ image\ size}{Compressed\ image\ size} \tag{14}$$

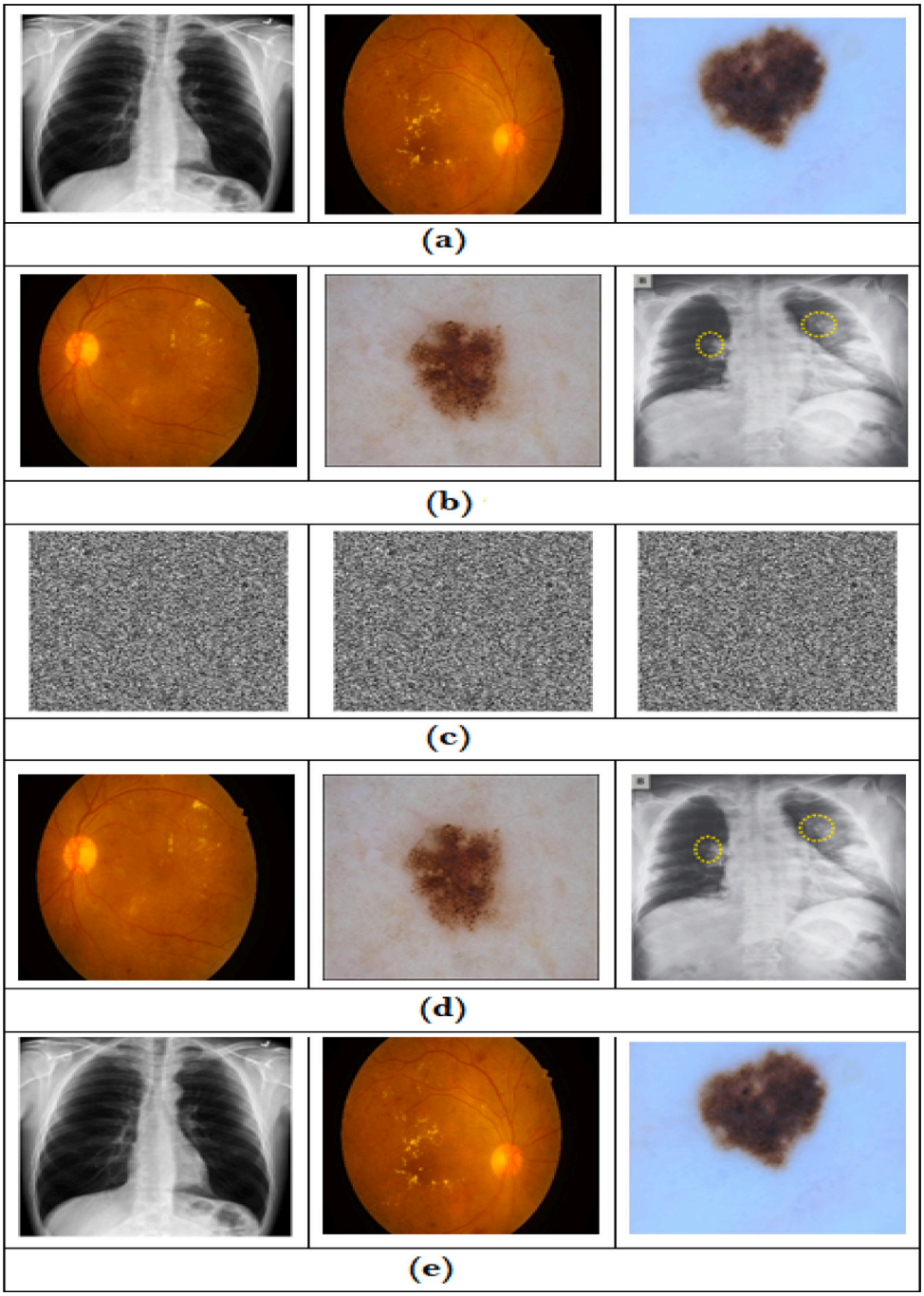

Fig. 5. Encryption and watermarking performance using proposed HMIEC framework: (a) Source medical images, (b) Cover medical images, (c) Encrypted source images, (d) Watermarked images, and (e) Extracted source medical images.

4.3. Subjective evaluation

An extensive study of the simulation results produced by the HMIEC approach is provided in this section. Fig. 5(a) shows the sample source medical images such as CXR, DR, and skin cancer images. Fig. 5(b) shows the cover medical images, such as DME, skin cancer, and CXR images. Fig. 5(c) depicts encrypted images produced by IHCME from CXR, DR, and skin cancer images. These encrypted images are in an unknown format, so an attacker cannot retrieve any information from that image in an IoMT environment. Further, the watermarking operation is also performed on encrypted images to provide more security. Fig. 5(d) shows

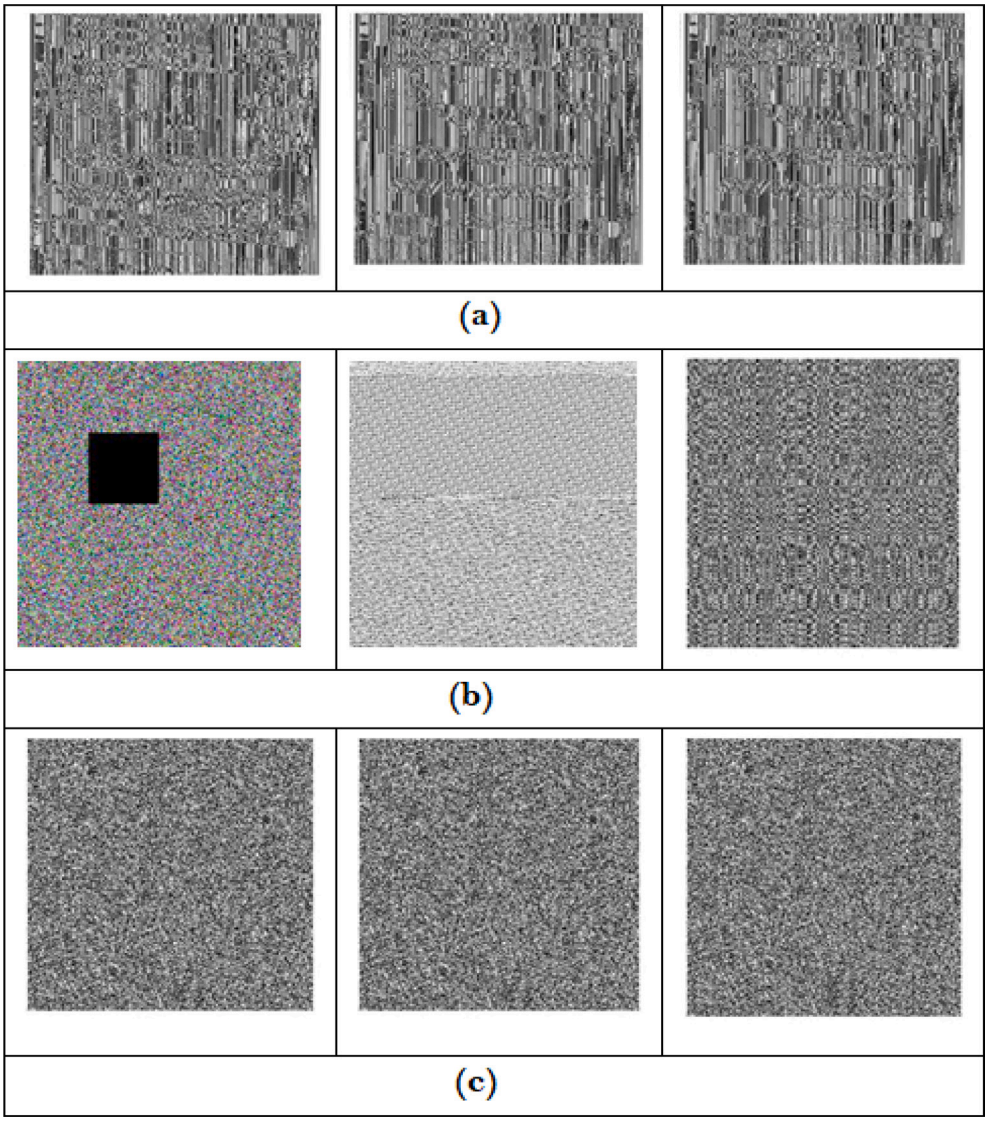

Fig. 6. Visual comparison of encrypted medical images: (a) CA-DNA-based encryption, (b) HGL-based encryption, and (c) Encryption using the proposed HMIEC method.

the watermarked images generated using IHCME, where cover images were overlaid on encrypted images. So, the attacker may think that the patient has a different disease due to this watermarking process. For example, patient one has COVID-19, but the watermarking process resulted in DME as the output image. In this case, the attacker may regard the DME as the original image and may not realize that another image exists within the DME image. Finally, the IHCME extraction process resulted in the original images shown in Fig. 5(e). The resultant extracted images look similar to the original images, which shows the proposed system resulted in superior performance.

Fig. 6 shows the visual comparison of encrypted medical images produced using various approaches. Here, the source images are presented in Fig. 5(a). The CA-DNA [21] approach resultant encrypted images were presented in Fig. 6(a). These encrypted images have higher losses due to uneven texture and border regions. Further, the HGL [25] approach resultant encrypted images were presented in Fig. 6(b). These resulting images have poor encryption results, such as a block box, white pixels, and inconsistent pixel location. Compared to these CA-DNA [21] and HGL [25] methods, the proposed HMIEC method resulted in superior subjective performance as shown in Fig. 6(c). Fig. 7 shows the watermarked images generated using various approaches. Here, the source images are presented in Fig. 5(a). The LSB-DWT-SVD [19] approach resultant watermarked images were presented in Fig. 7(a). These watermarked images suffer from higher color imbalance issues, so it is challenging to extract original medical images from these watermarked images. Further, the HHO-DLCNN [20] approach resultant watermarked images were presented in Fig. 7(b). These resulting images have higher contrast, saturation, and color balance issues, which causes reduced performance. Compared

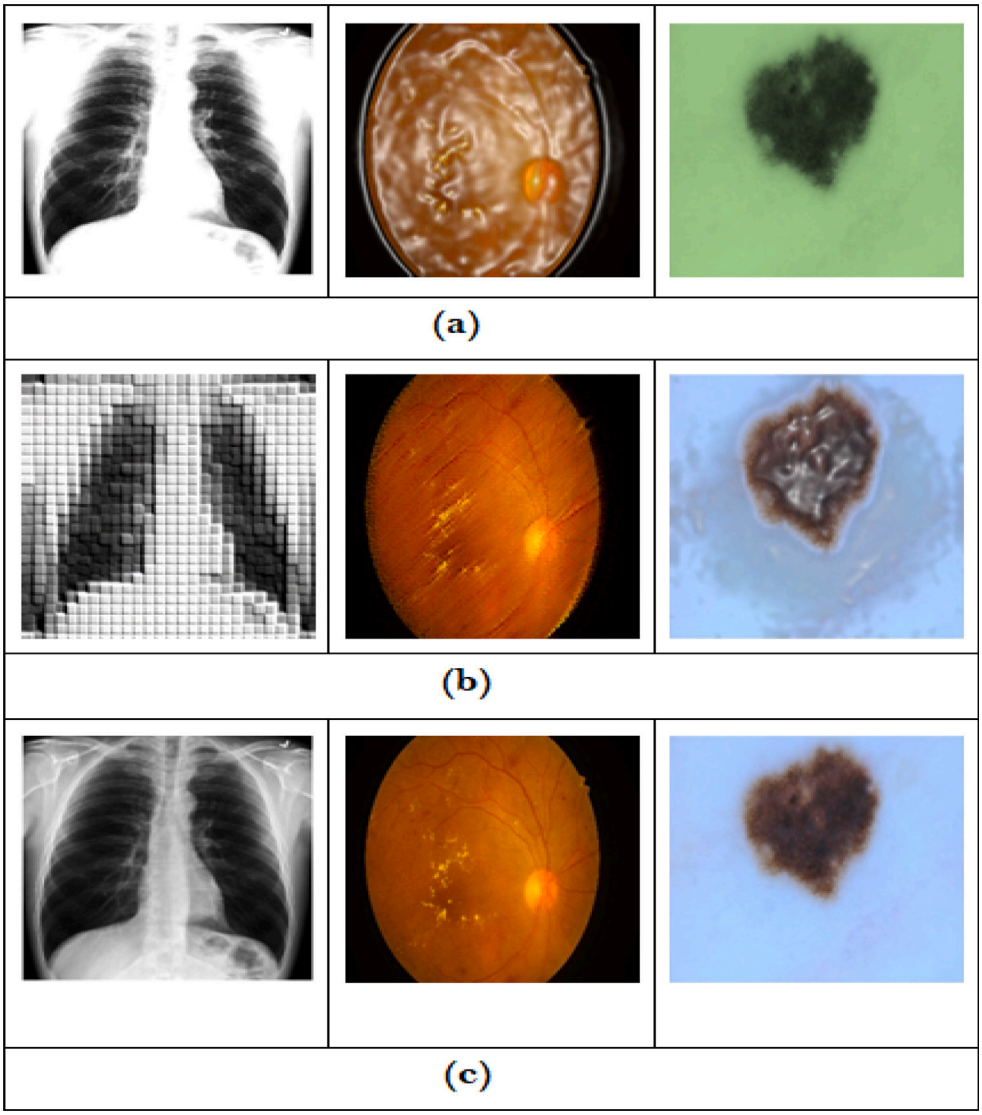

Fig. 7. Watermarked medical images generated using different methods: (a) LSB-DWT-SVD, (b) HHO-DLCNN, and (c) Proposed HMIEC.

to the LSB-DWT-SVD [19] and HHO-DLCNN [20] methods, the proposed HMIEC method resulted in better-watermarked images as shown in Fig. 7(c) and improved subjective outcomes.

4.4. Objective evaluation

This section evaluates the proposed HMIEC approach against other watermarking methods as compared in Table 3. Here, the proposed HMIEC method resulted in superior performance than existing methods such as LWT–DWT [16], DCT–DWT [17], Hybrid transformation [18], LSB-DWT-SVD [19], and HHO-DLCNN [20]. In this case, the performance of PSNR and SSIM resulted in higher and lower MSE values.

The highest PSNR (dB) value obtained by the proposed method after the watermarking is 77.04, indicating less distortion and better preservation of the image quality with good visual fidelity in diagnosis. The lower MSE value of 0.001283 indicates that the proposed method maintains high-quality image reconstruction. The higher value of 0.991 for the SSIM in the proposed approach indicates structural integrity with near-perfect preservation of visual details after watermarking, confirming that the recovered and original images have similar structural features. Table 4 compares the encryption performance comparison of the proposed HMIEC approach with existing approaches. Here, the proposed method resulted in increased entropy, NCC, NPCR (%), and UACI (%) as compared to other protocols like CA-DNA [21], MRNN [22], Henon chaotic map [23], V-Net CNN [24], HGL [25]. The numerical evaluated values of Table 4 are presented in Fig. 8 graphically. The entropy value obtained by the proposed method is 41.923, which

Table 3
Watermarking performance of various approaches.

Method	PSNR (dB)	MSE	SSIM
LWT–DWT [16]	65.24	0.01945	0.673
DCT–DWT [17]	65.74	0.01734	0.763
Hybrid transformation [18]	66.26	0.01538	0.782
LSB-DWT-SVD [19]	67.70	0.01103	0.81
HHO-DLCNN [20]	68.42	0.009338	0.88
Proposed HMIEC	**77.04**	**0.001283**	**0.991**

Table 4
Encryption performance comparison of various approaches.

Method	Entropy	NCC	NPCR (%)	UACI (%)
CA-DNA [21]	10.145	0.634	11.298	80.315
MRNN [22]	20.514	0.703	14.421	80.590
Henon chaotic map [23]	21.908	0.753	22.465	83.152
V-Net CNN [24]	23.331	0.771	24.981	83.549
HGL [25]	28.726	0.89	25.645	86.984
Proposed HMIEC	**41.923**	**0.992**	**33.46**	**99.60**

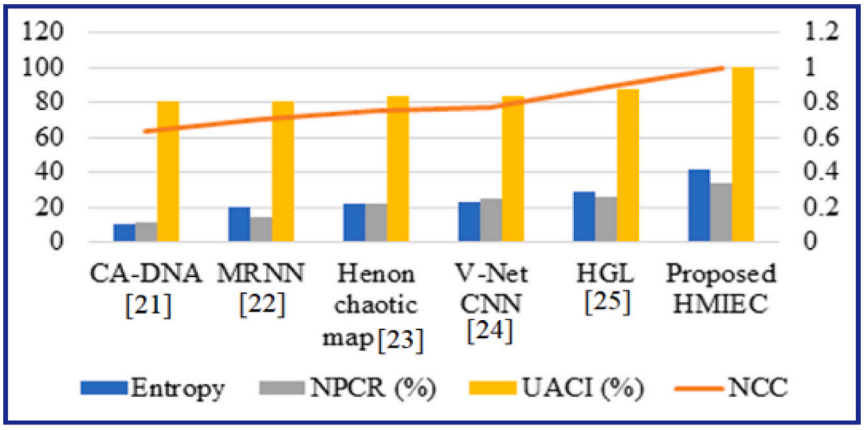

Fig. 8. Graphical representation of various encryption approaches performance.

ensures that the strong encryption watermarked image exhibits strong security properties in the proposed work. The increased high value of the entropy in the proposed work is due to increased randomness in pixel distribution due to the transformations, multi-channel contributions (RGB/YC_bC_r), and encryption process. This indicates the high resistance to differential and entropy-based attacks. The proposed work's high NCC value of 0.992 confirms the high similarity between the original and extracted watermark image. A high NCC value is necessary for applications where the embedded watermark image should be accurately retrievable without degradation. The NPCR (%) value of 33.46 indicates a difference in pixel values between the original and encrypted images, which confirms that the proposed work maintains a balance between security and image quality while keeping limited changes in pixel values. The proposed method obtains a high value of UACI (99.60%).

Due to this high value of UACI, the encrypted image is significantly different from the original image. This indicates the maximum possible change in pixel intensities, making it extremely difficult for attackers to retrieve the original image, thus enhancing security. The proposed method also avoids security vulnerabilities due to the high value of UACI.

Table 5 shows how different approaches compare in terms of compression performance. In this case, the suggested HMIEC method outperformed earlier methods such as LWT–DWT [16], DCT–DWT [17], Hybrid transformation [18], and LSB-DWT-SVD [19] regarding CR and calculation time. All these are wavelet-based methods, which compress the images by default.

The graphical representation of Table 5 is presented in Fig. 9. The proposed method significantly reduces the image size while preserving high-quality image reconstruction with a CR value of 21.955%. Transmission and extraction are required in healthcare systems for real-time quick encryption, and the proposed method shows a faster computation time of 6.535 s compared to the conventional Advanced Encryption Standard (AES) + JPEG2000+PSO, which is 12.351 s. This low computation time suggests the proposed method is suitable for real-time medical applications, particularly in IoMT, where telemedicine is required. Further, using DKLT and GWO in the proposed framework enhances efficiency, reducing the computational overhead. HMIEC can be seamlessly integrated into telemedicine applications by embedding it within cloud-based PACS and secure IoMT gateways, ensuring end-to-end encryption during remote diagnostics and consultations. Since the method achieves superior performance in all the metrics, it proves to be an optimal solution that balances both security and imperceptibility.

Table 5
Compression performance comparison of various approaches.

Method	CR (%)	Computation time (Seconds)
LWT–DWT [16]	8.192	29.128
DCT–DWT [17]	12.197	21.361
Hybrid transformation [18]	13.393	19.214
LSB-DWT-SVD [19]	15.992	16.385
Proposed HMIEC	**21.955**	**6.535**

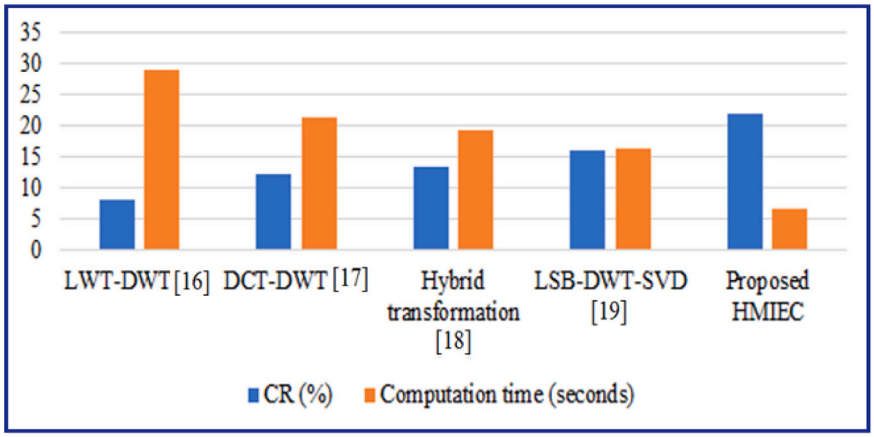

Fig. 9. Graphical representation of various compression approaches performance.

Table 6
Overall performance comparison of traditional approaches.

Metric	AKAZE-DCT [27]	ANFRS [29]	WatMIF [28]	Proposed HMIEC	Best competitor	p-value (HMIEC vs. WatMIF)
PSNR (dB)	37.942	47.280	54.867	**77.04**	WatMIF	1.7×10^{-6}
MSE	0.021208	0.00255	0.0022	**0.001283**	WatMIF	9.1×10^{-7}
SSIM	0.733	0.830	0.938	**0.991**	WatMIF	2.4×10^{-5}
Entropy	16.273	20.920	26.271	**41.923**	WatMIF	1.3×10^{-6}
NCC	0.663	0.709	0.857	**0.992**	WatMIF	3.5×10^{-5}
NPCR (%)	12.533	19.620	27.030	**33.46**	WatMIF	5.9×10^{-4}
UACI (%)	70.189	83.299	86.212	**99.60**	WatMIF	8.2×10^{-4}
CR (%)	8.440	10.608	15.428	**21.955**	WatMIF	6.8×10^{-5}
Computation time (s)	32.418	26.003	15.186	**6.535**	WatMIF	7.5×10^{-6}

Table 6 provides various approaches' overall performance (watermarking, compression, and encryption). Here, the proposed HMIEC method resulted in improved PSNR by 77.04 dB, MSE of 0.001283, SSIM of 0.991, entropy of 41.923, NCC of 0.992, NPCR of 33.46%, UACI of 99.60%, CR of 21.955%, and computation time of 6.535 s performance than existing methods such as AKAZE-DCT [27], ANFRS [29], WatMIF [28]. The graphical representation of Table 6 is presented in Fig. 10.

In addition to the traditional methods, a hybrid deep learning model based on DCT and CNN is tested on our dataset [37]. It exhibits a lower PSNR value of 55.32 dB, MSE of 0.0025, SSIM of 0.945, entropy of 28.231, NCC of 0.872, NPCR of 25.12%, UACI of 88.23%, CR of 14.923%, and computation time of 18.326 s. A DLEDNet which is a DL based image encryption and decryption network with Cycle-Generative adversarial network (GAN) for IoMT is evaluated on the dataset which is used in this research work [38]. This hybrid deep learning approach exhibits a lower PSNR value of 50.85 dB, MSE of 0.0038, SSIM of 0.902, entropy of 30.542, NCC of 0.899, NPCR of 29.65%, UACI of 92.45%, CR of 18.276%, and computation time of 24.215 s. A hybrid encryption scheme for the medical image with Autoencoder and AES is tested for its performance estimation [39]. This hybrid model exhibits a lower PSNR value of 48.92 dB, MSE of 0.0045, SSIM of 0.890, entropy of 27.812, NCC of 0.884, NPCR of 26.48%, UACI of 89.87%, CR of 16.562%, and computation time of 22.541 s. Additionally, a lightweight encryption technique that uses two permutation techniques to provide better security is analyzed to know its performance on the dataset utilized in this research work. Additionally, a lightweight encryption technique that uses two permutation techniques to provide better security is analyzed to know its performance on the dataset utilized in this research work [40]. The analysis concludes that the lightweight encryption technique is computationally efficient but exhibits higher MSE and lower PSNR, essential for more resistance to statistical attacks. The graphical representation of the overall performance of hybrid deep learning approaches with proposed HMIEC is shown in Fig. 11.

The proposed HMIEC exhibits superior performance than these hybrid models with balanced security and perceptual quality, making it a reliable solution for medical image protection in IoMT applications. Security, efficient transmission, and medical image

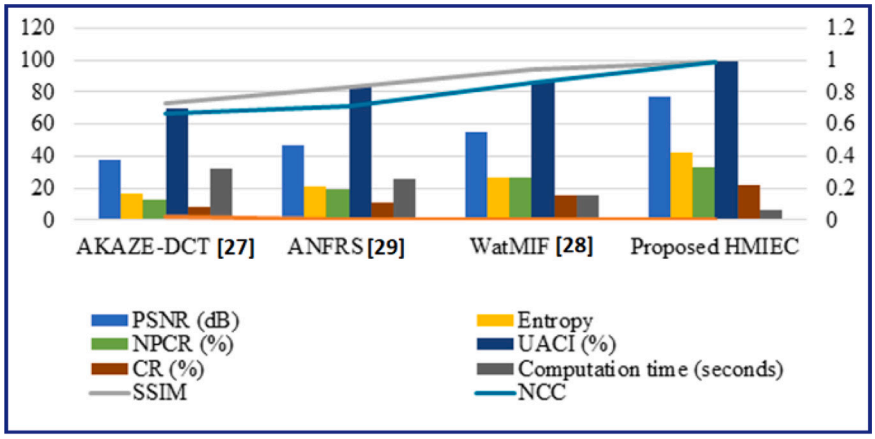

Fig. 10. Graphical representation of the overall performance of traditional approaches.

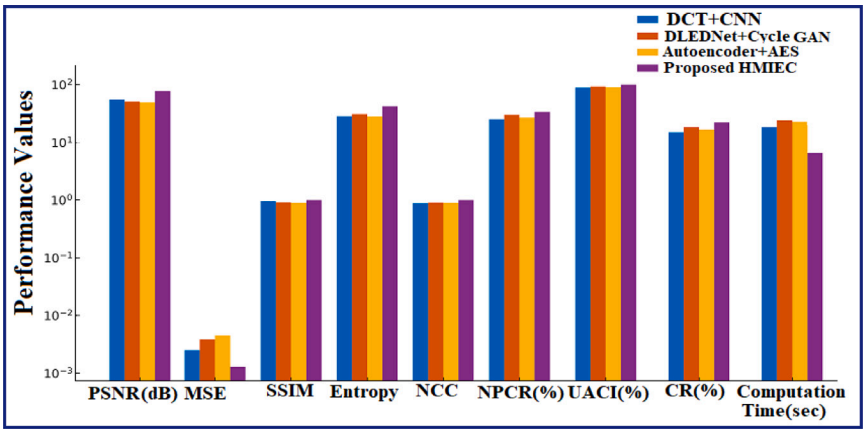

Fig. 11. Graphical representation of the overall performance of hybrid deep learning approaches.

analysis are essential in IoMT-based diagnostic applications. The proposed HMIEC framework is compatible with edge Artificial Intelligence (AI) and wearable healthcare devices. This compatibility makes the HMIEC secure and efficient in transmission and medical image analysis.

4.5. Statistical significance analysis

A statistical significance analysis was conducted using a paired t-test to validate the improvements achieved by the proposed HMIEC method. The test was conducted between the best competitor and the proposed HMIEC for each performance metric. From Table 6, the best competitor selected is WatMIF compared to other existing methods for paired t-tests. The p-values are computed to know the significant differences between the proposed method and the best competitor. The p-values calculated between the proposed HMIEC and WatMIF (best competitor existing approach) are provided in Table 6. It is found that the p-values for all key performance metrics are significantly lower than 0.05. The statistical tests confirm that the proposed HMIEC significantly improves PSNR, MSE, SSIM, Entropy, NCC, NPCR, UACI, CR, and Computation Time. These improvements are not due to random variations, and they confirm that the proposed method is an optimal and statistically validated approach for medical image encryption, compression, and watermarking.

4.6. Perceptual quality analysis

This study conducts a perceptual quality analysis to evaluate the effectiveness of the proposed encryption, watermarking, and extraction methods. This analysis is done by considering the histograms for the X-ray source image, including the diabetic retinopathy cover medical image, encrypted image of proposed HMIEC, watermarked image, and extracted image. The histograms computed for each of these images are shown in Fig. 12. This quality analysis confirms that the proposed encryption method provides strong security against statistical attacks by achieving a near uniform distribution in the histogram of the encrypted image and preserving

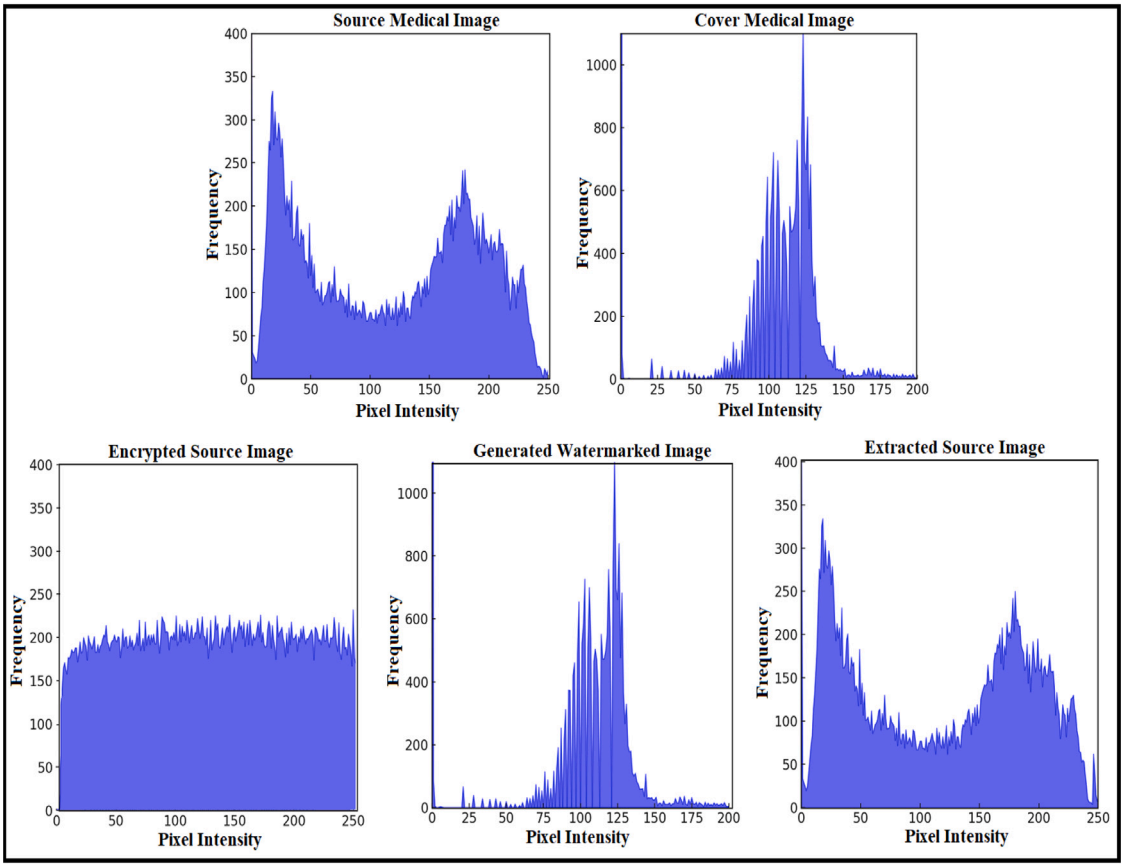

Fig. 12. Histograms evaluation for perceptual quality analysis.

the visual quality as the histogram for the watermarked image and cover image is approximately the same. The similarity between the original and extracted histograms confirms that the extraction process is reversible. Thus, the proposed HMIEC framework effectively balances security and perceptual quality, making it a reliable solution for medical image protection in IoMT applications.

The medical image should maintain good visual fidelity with the maximum possible compression to make it suitable for the IoMT environment. Fig. 13 shows the graphical representation of PSNR vs. CR. Image quality reduces as the compression increases; the suitable method maintains a balance between compression and image quality. The graphical representation of PSNR vs. CR of the proposed method with respect to existing methods confirms excellent quality retention at a good compression rate. The quality of the recovered images may be affected by the watermarking embedding strength and compression approach used. Similarly, Fig. 14 shows the graphical representation of SSIM vs. CR to provide trade-offs between compression performance and encryption quality of the proposed HMIEC. The SSIM value remains consistent and above 0.94 across varying compression levels, reaching a maximum of 0.967 at compression of 21%. This consistent performance is evidence of the method's robustness in preserving structural image quality, even at higher compression rates. A minor reduction in SSIM is observed at mid-level compression ratios (17%–18%). However, due to the SSIM above 0.94, the proposed framework achieves a balance between the compression performance and encryption quality. The watermark embedding effect on image quality using heatmaps in this research work is visualized in Fig. 15. The heatmaps comparing three distinct source images and their recovered images after watermarking embedding, along with their corresponding difference heatmaps, are presented in Fig. 15. The difference heatmaps show that the proposed HMIEC framework introduces minimal loss in image quality due to the watermarking embedding.

4.7. Key sensitivity and attack resistance analysis

The key sensitivity analysis is performed by the correct key (key-1) and a key with one-bit change (key-2) to ensure the robustness of the proposed HMIEC framework. It was found that key-1 decrypted the encrypted image correctly, while key-2 failed to decrypt the encrypted image. The proposed method is susceptible to key changes, preventing brute-force attacks and ensuring that only the correct key can decrypt the image. The proposed framework focuses on balancing security and image quality, preventing excessive changes in pixel values. The NPCR(%) of 33.46 is obtained by the proposed HMIEC, which creates fewer pixel changes with moderate differential attack resistance. However, the UACI (%) value of 99.60 indicates that the proposed method is robust against the

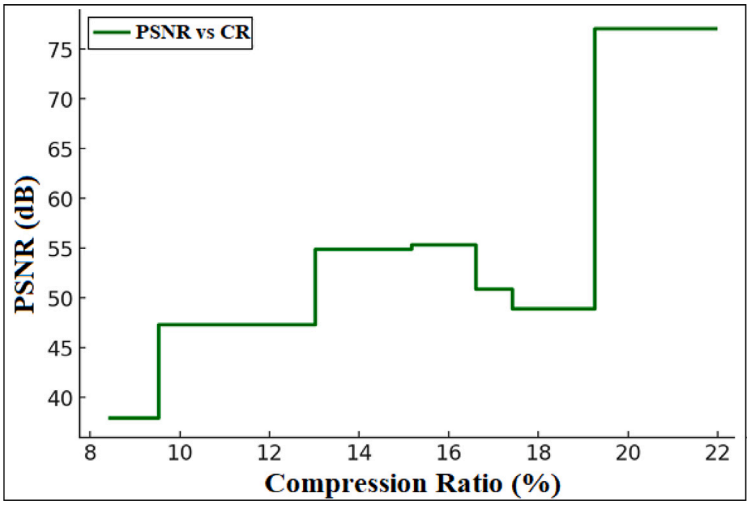

Fig. 13. Peak Signal-to-Noise Ratio (PSNR) vs. Compression Ratio (CR).

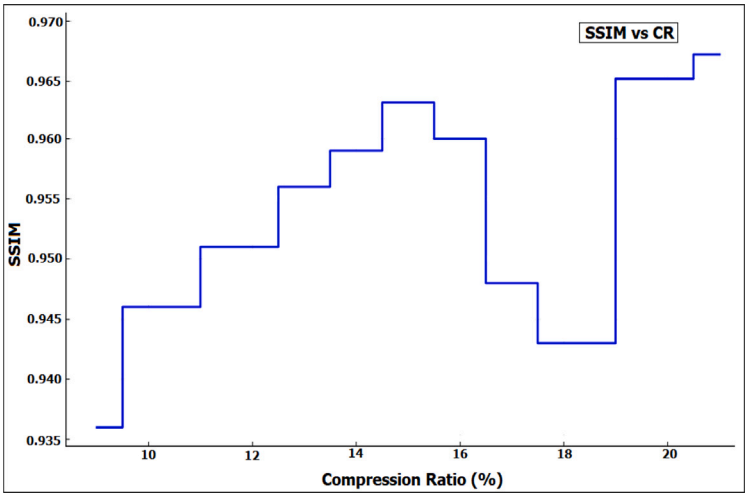

Fig. 14. Structural similarity index metric (SSIM) vs. Compression Ratio (CR).

differential attacks due to almost all pixel intensities changed significantly. The increased high value of the entropy in the proposed work is due to increased randomness in pixel distribution due to the transformations, multi-channel contributions (RGB/YC_bC_r), and encryption process. This indicates the high resistance of proposed method to differential and entropy-based attacks. The NCC value of 0.992 obtained by the proposed method confirms the high similarity between the extracted and original images, preventing watermark removal and forgery attempts. The redundant noise conditions, cropping, and geometric distortions affect the retrieval of the watermark image and encrypted image. Still, DKLT reduces these attack conditions, allowing the proposed HMIEC with GWO to retrieve the watermark and encrypted images.

The robustness of the proposed HMIEC framework against common attacks such as JPEG compression, Gaussian noise, salt and pepper noise, speckle noise, rotation, cropping, and scaling was evaluated and visualized in Fig. 16. Initially, the encrypted–watermarked image is subjected to the JPEG compression with quality factor (QF) of 50. The recovered image maintained a PSNR value of 69.959 dB and an NCC value of 0.993, indicating that the proposed framework strongly resists lossy compression and maintains the required image quality. The encrypted–watermarked image is subjected to noises such as Gaussian noise with variance $\sigma^2 = 0.0002$, salt and pepper noise with a density of 0.0002, and speckle noise with a variance of 0.0001 to evaluate the noise robustness of the proposed HMIEC. The recovered image maintained a PSNR value of 65.182 dB and an NCC value of 0.995 in case of Gaussian noise, a PSNR value of 71.372 dB and an NCC value of 0.987 in case of salt and pepper noise, and a PSNR value of 72.810 dB and an NCC value of 0.999 in case of speckle noise. These results demonstrate that the GWO-based embedding strategy effectively preserves visual quality even under noisy conditions. Further, the encrypted–watermarked image is subjected to geometric attacks by rotation at 10 degrees, image cropping at 10%, and scaling at 10% to evaluate the robustness of the proposed

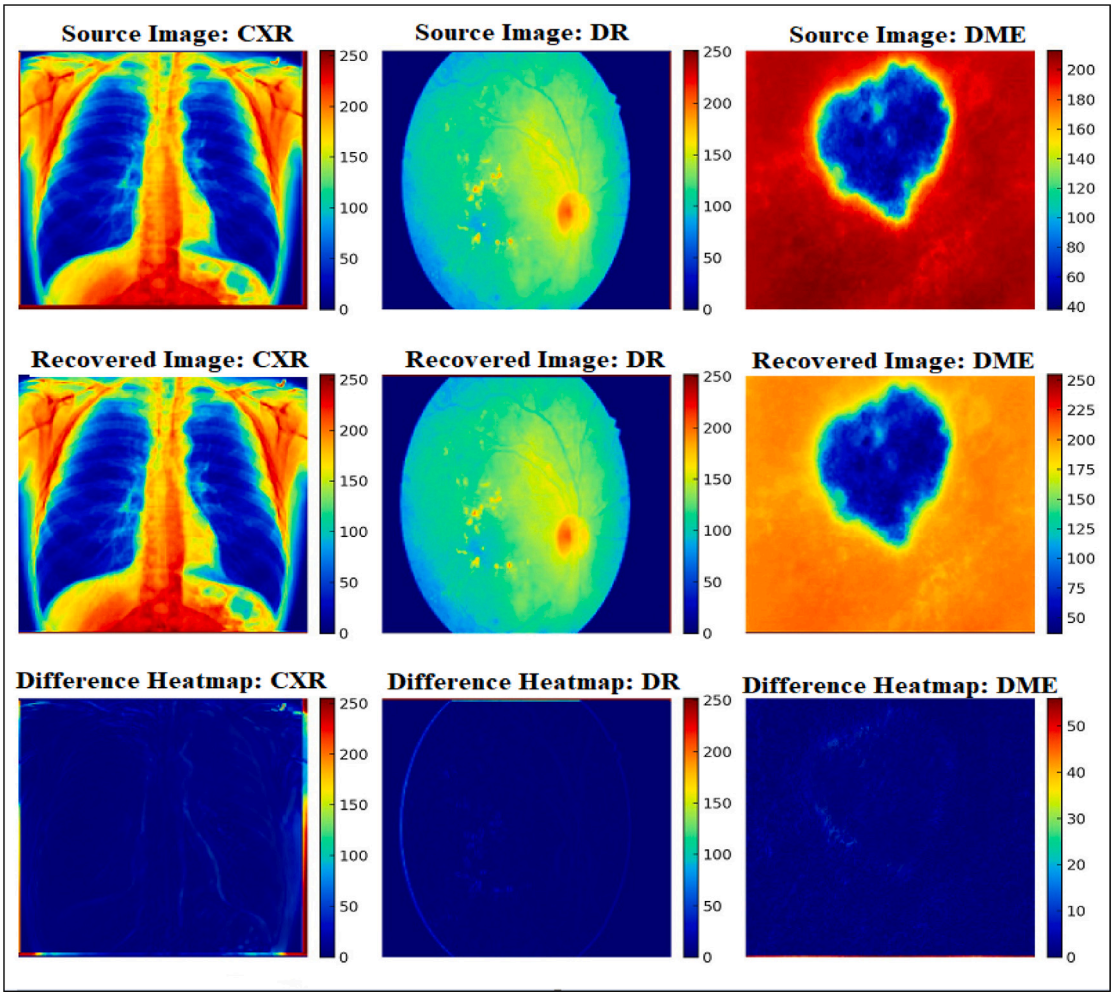

Fig. 15. Watermark embedding effect on image quality using heatmaps.

HMIEC against geometric attacks. The recovered image maintained a PSNR value of 68.521 dB and an NCC value of 0.984 in case of rotation with 10 degrees, the recovered image maintained a PSNR value of 67.513 dB and an NCC value of 0.982 in case of 10% image cropping, and the recovered image maintained a PSNR value of 66.252 dB and an NCC value of 0.983 in case of 10% image scaling. In all the cases, NCC is above 0.9, confirming the strong recoverability and minimal degradation of watermark integrity.

4.8. Computational efficiency

The graphical visualization of computational efficiency with individual processing times is shown in Fig. 17. The individual processing times of the encryption, compression, and watermarking are evaluated for the conventional methods such as AES + JPEG2000 + PSO and AES + DWT + GA along with the proposed HMIEC on the same dataset to know the scalability and feasibility of the proposed HMIEC framework in real-time IoMT environments. The AES + JPEG2000 + PSO requires encryption time of 7.210 s, compression time of 2.181 s, watermarking time of 2.960 s, and total time of 12.351 s. The AES + DWT + GA requires an encryption time of 6.920 s, compression time of 3.105 s, watermarking time of 4.120 s, and total time of 14.145 s. The proposed HMIEC framework requires an encryption time of 2.850 s, compression time of 1.750 s, watermarking time of 1.935 s, and total time of 6.535 s. These evaluated results confirm that the proposed HMIEC is scalable and feasible in IoMT environments compared to the conventional methods.

5. Research challenges and future work

The integration of encryption, compression, and watermarking with IHCME, DKLT, and GWO may increase the computational overhead, making real-time applications in IoMT and telemedicine difficult. Computationally efficient and optimized lightweight

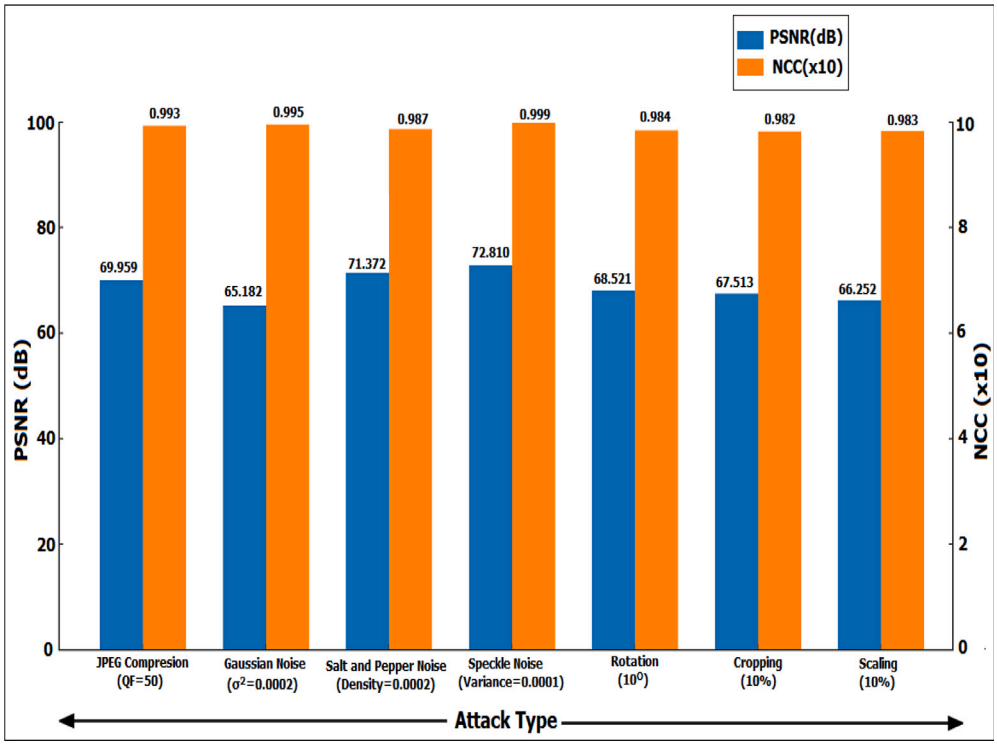

Fig. 16. Robustness evaluation of HMIEC under various attacks.

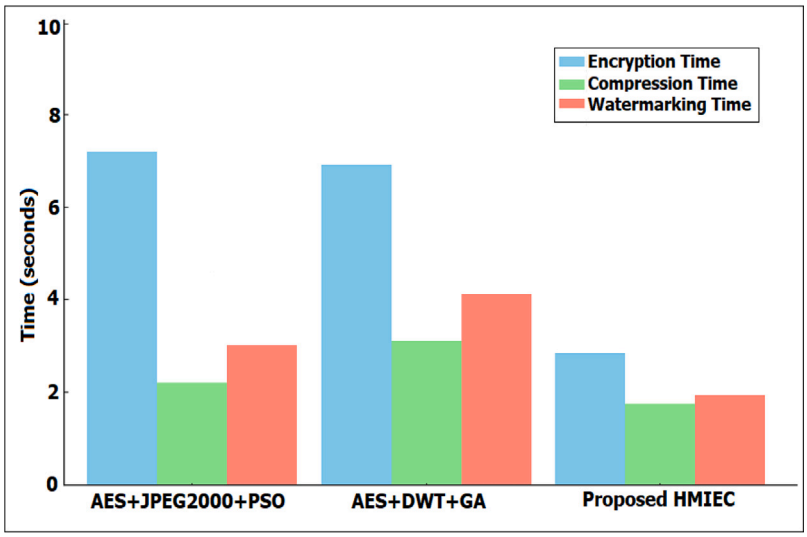

Fig. 17. Graphical visualization of computational efficiency with individual processing times.

versions of DKLT and IHCME are required to develop to overcome this challenge. Maintaining the balanced compression is another major challenge, as the high compression leads to the loss of medical information in the image. Adaptive compression techniques may address this challenge. The proposed HMIEC framework provides stronger encryption, high security, and a chance of image degradation. The Greylag Goose Optimization (GGO) algorithm is a swarm-based algorithm to solve the complex problems that can be used in the proposed framework to optimize computational efficiency with improved accuracy and robustness in image encryption and compression [41]. Advanced optimization algorithms such as deep learning and machine learning along with Adaptive Dynamic Dipper Throated Optimization can be utilized for encryption further to optimize the embedding strength factor [42]. Deep learning-based feature extraction can improve image retrieval and secure storage in cloud-based healthcare. Image restoration and secure

storage are important in healthcare systems and can be improved if we apply adaptive encryption levels based on the importance of the diagnosis using DL and ML [43]. Further, this work can be extended with hybrid deep learning methods for improved compression, watermarking, and encryption performance. Integrating quantum encryption and adaptive compression techniques with the proposed HMIEC framework is another future direction to enhance the security and efficient compression of medical images in the IoMT. Integrating the HMIEC framework with dynamic key generation based on chaotic sequences instead of a single key will significantly improve the resistance to brute-force, differential, and statistical attacks, making decryption difficult without a key. If dynamic key generation, adaptive compression, and decentralized key management are combined, medical image encryption becomes highly resistant to cybersecurity attacks, particularly in telemedicine and IoMT applications. The proposed HMIEC framework is developed with real-time applicability regarding computational time, memory, security, and robustness in a simulation environment. Integrating encryption, compression, and watermarking with IHCME, DKLT, and GWO will help handle the high-throughput in medical image processing, and it is required to be implemented and tested in a real-time IoMT environment in the future. Combining AI and blockchain technology in HMIEC enhances its robustness and security for next-generation healthcare applications and anomaly detection for cybersecurity threats. Also, AI-powered threat intelligence models will help adjust the strength of the encryption dynamically based on the severity of attacks. This adaptive encryption mechanism will further improve the robustness and security of HMIEC. The deployment of HMIEC in real-time telemedicine services is significantly enhanced through hardware acceleration using field programmable gate array (FPGA) and graphics processing unit (GPU) optimization to reduce computational overhead.

6. Conclusion

This work aims to develop an HMIEC framework that uniquely integrates encryption, compression, and watermarking as a scalable solution to the challenges of security, imperceptibility, and high-quality medical image transmission along with storage in an IoMT environment. The proposed work integrates the IHCME for strong image encryption, DKLT for effective compression and transformation, and GWO to identify optimal embedding strength for watermarking. This unique integration ensures high security, imperceptibility, and compression efficiency, making it more suitable for real-time healthcare applications. Extensive simulation results validate the superiority of the HMIEC, achieving a PSNR of 77.04 dB, entropy of 41.923, MSE of 0.001283, SSIM of 0.991, NCC of 0.992, CR of 21.955%, UACI of 99.60%, and NPCR of 33.46%, outperforming several existing approaches. Security evaluations with sensitivity and attack resistance analysis demonstrate high resistance to differential and brute-force attacks, while the perceptual quality analysis confirms minimal distortion in watermarked images. Additionally, the proposed framework maintains a low computational time, confirming its feasibility for real-time telemedicine and IoMT deployments. Future directions include combining AI and blockchain technology in HMIEC to enhance its robustness and security for next-generation healthcare applications and anomaly detection for cybersecurity threats. The deployment of HMIEC in real-time telemedicine services is significantly enhanced through hardware acceleration using FPGA and GPU optimization to reduce computational overhead.

CRediT authorship contribution statement

Anandbabu Gopatoti: Visualization, Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Writing – review & editing. **James Stephen Meka:** Resources, Supervision, Project administration, Conceptualization, Methodology. **Poornaiah Billa:** Investigation, Data curation, Formal analysis, Conceptualization.

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.

Data availability

Data will be made available on request.

References

[1] Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR. A review on security and privacy of internet of medical things. Intell Internet Things Heal Ind 2022;171–87.
[2] Hasan MK, Ghazal TM, Saeed RA, Pandey B, Gohel H, Eshmawi A, Abdel-Khalek S, Alkhassawneh HM. A review on security threats, vulnerabilities, and counter measures of 5G enabled internet-of-medical-things. IET Commun 2022;16(5):421–32.
[3] Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D. A survey on security threats and countermeasures in internet of medical things (IoMT). Trans Emerg Telecommun Technol 2022;33(6):e4049.
[4] Svandova K, Smutny Z. Internet of medical things security frameworks for risk assessment and management: A scoping review. J Multidiscip Heal 2024;2281–301.
[5] Hossen MN, Panneerselvam V, Koundal D, Ahmed K, Bui FM, Ibrahim SM. Federated machine learning for detection of skin diseases and enhancement of internet of medical things (IoMT) security. IEEE J Biomed Heal Inform 2022;27(2):835–41.
[6] He P, Huang D, Wu D, He H, Wei Y, Cui Y, Wang R, Peng L. A survey of internet of medical things: technology, application and future directions. Digit Commun Netw 2024.

[7] Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J Netw Comput Appl 2022;201:103332.

[8] Naeem F, Tariq M, Poor HV. SDN-enabled energy-efficient routing optimization framework for industrial internet of things. IEEE Trans Ind Inform 2020;17(8):5660–7.

[9] Huang C, Wang J, Wang S, Zhang Y. Internet of medical things: A systematic review. Neurocomputing 2023;557:126719.

[10] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet Things J 2020;8(11):8707–18.

[11] Al-Otaibi YD. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. Comput Electr Eng 2022;101:108129.

[12] Khan IA, Moustafa N, Razzak I, Tanveer M, Pi D, Pan Y, Ali BS. XSRU-IoMT: Explainable simple recurrent units for threat detection in internet of medical things networks. Future Gener Comput Syst 2022;127:181–93.

[13] Al Khatib I, Shamayleh A, Ndiaye M. Healthcare and the internet of medical things: applications, trends, key challenges, and proposed resolutions. In: Informatics. vol. 11, MDPI; 2024, p. 47.

[14] Annane B, Alti A, Lakehal A. Blockchain based context-aware CP-ABE schema for internet of medical things security. Array 2022;14:100150.

[15] Garg N, Wazid M, Singh J, Singh DP, Das AK. Security in iomt-driven smart healthcare: A comprehensive review and open challenges. Secur Priv 2022;5(5):e235.

[16] Vaidya SP. Fingerprint-based robust medical image watermarking in hybrid transform. Vis Comput 2023;39(6):2245–60.

[17] Amine K, Fares K, Redouane KM, Salah E. Medical image watermarking for telemedicine application security. J Circuits Syst Comput 2022;31(05):2250097.

[18] Moad MS, Kafi MR, Khaldi A. A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocess Microsyst 2022;90:104490.

[19] Singh P, Devi KJ, Thakkar HK, Kotecha K. Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. IEEE Access 2022;10:8974–93.

[20] Chacko A, Chacko S. Deep learning-based robust medical image watermarking exploiting DCT and Harris hawks optimization. Int J Intell Syst 2022;37(8):4810–44.

[21] Wu Y, Zhang L, Berretti S, Wan S. Medical image encryption by content-aware DNA computing for secure healthcare. IEEE Trans Ind Inform 2022;19(2):2089–98.

[22] Lin H, Wang C, Cui L, Sun Y, Zhang X, Yao W. Hyperchaotic memristive ring neural network and application in medical image encryption. Nonlinear Dynam 2022;110(1):841–55.

[23] Masood F, Driss M, Boulila W, Ahmad J, Rehman SU, Jan SU, Qayyum A, Buchanan WJ. A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wirel Pers Commun 2022;127(2):1405–32.

[24] Wang X, Yin S, Shafiq M, Laghari AA, Karim S, Cheikhrouhou O, Alhakami W, Hamam H. A new V-Net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption. Secur Commun Netw 2022;2022(1):4260804.

[25] Abdelfatah RI, Saqr HM, Nasr ME. An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map. Multimedia Tools Appl 2023;82(14):22213–27.

[26] Liu Z, Li J, Ai Y, Zheng Y, Liu J. A robust encryption watermarking algorithm for medical images based on ridgelet-DCT and THM double chaos. J Cloud Comput 2022;11(1):60.

[27] Li D, Chen Y-w, Li J, Cao L, Bhatti UA, Zhang P. Robust watermarking algorithm for medical images based on accelerated-KAZE discrete cosine transform. IET Biom 2022;11(6):534–46.

[28] Singh KN, Singh OP, Singh AK, Agrawal AK. Watmif: Multimodal medical image fusion-based watermarking for telehealth applications. Cogn Comput 2024;16(4):1947–63.

[29] Balasamy K, Krishnaraj N, Vijayalakshmi K. An adaptive neuro-fuzzy based region selection and authenticating medical image through watermarking for secure communication. Wirel Pers Commun 2022;122(3):2817–37.

[30] Gong C, Liu J, Gong M, Li J, Bhatti UA, Ma J. Robust medical zero-watermarking algorithm based on residual-DenseNet. IET Biom 2022;11(6):547–56.

[31] Almaiah MA, Ali A, Hajjej F, Pasha MF, Alohali MA. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors 2022;22(6):2112.

[32] Al-Saffar NFH, Al-Saiq IR. Symmetric text encryption scheme based Karhunen Loeve transform. J Discret Math Sci Cryptogr 2022;25(8):2773–81.

[33] Mirjalili S, Mirjalili SM, Lewis A. Grey wolf optimizer. Adv Eng Softw 2014;69:46–61.

[34] Kalpana Devi M, Mary Shanthi Rani M. Classification of diabetic retinopathy using ensemble of machine learning classifiers with IDRiD dataset. In: Evolutionary computing and mobile sustainable networks: proceedings of ICECMSN 2021. Springer; 2022, p. 291–303.

[35] Wang L, Lin ZQ, Wong A. COVID-Net: A tailored deep convolutional neural network design for detection of covid-19 cases from chest x-ray images. Sci Rep 2020;10(1):19549.

[36] Cassidy B, Kendrick C, Brodzicki A, Jaworek-Korjakowska J, Yap MH. Analysis of the ISIC image datasets: Usage, benchmarks and recommendations. Med Image Anal 2022;75:102305.

[37] Fan Y, Li J, Bhatti UA, Shao C, Gong C, Cheng J, Chen Y. A multi-watermarking algorithm for medical images using inception V3 and DCT. Comput Mater Contin 2023;74(1).

[38] Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, Qin Z. DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet Things J 2020;8(3):1504–18.

[39] Alslman Y, Alnagi E, Ahmad A, AbuHour Y, Younisse R, Abu Al-haija Q. Hybrid encryption scheme for medical imaging using autoencoder and advanced encryption standard. Electronics 2022;11(23):3967.

[40] Hasan MK, Islam S, Sulaiman R, Khan S, Hashim A-HA, Habib S, Islam M, Alyahya S, Ahmed MM, Kamil S, et al. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access 2021;9:47731–42.

[41] El-Kenawy E-SM, Khodadadi N, Mirjalili S, Abdelhamid AA, Eid MM, Ibrahim A. Greylag goose optimization: nature-inspired optimization algorithm. Expert Syst Appl 2024;238:122147.

[42] Atteia G, El-kenawy E-SM, Samee NA, Jamjoom MM, Ibrahim A, Abdelhamid AA, Azar AT, Khodadadi N, Ghanem RA, Shams MY. Adaptive dynamic dipper throated optimization for feature selection in medical data. Comput Mater Contin 2023;75(1):1883–900.

[43] El-kenawy E, Eid MM, Abualigah L. Machine learning in public health forecasting and monitoring the Zika virus. Metaheuristic Optim Rev 2024;72:01–11.

Dr. Anandbabu Gopatoti is a Professor and Head of the Department of Electronics and Communication Engineering at the Wellfare Institute of Science, Technology and Management, Pinagadi, Visakhapatnam, Andhra Pradesh, India. He holds a Ph.D. in Biomedical Image Processing from Anna University, ranked 383rd in the QS World University Rankings. Dr. Gopatoti has published extensively, over 48 research articles in high-impact national and international journals, authored six books and two book chapters, and holds over 50 patents/copyrights. With over 15 years of experience in teaching and research, his expertise includes computer vision, machine learning, deep learning, and biomedical image encryption and compression frameworks, and he is committed to advancing medical image processing techniques for healthcare applications.

Prof. James Stephen Meka is the National Chair Professor, Dr. B.R. Ambedkar Chair, Andhra University (Ministry of Social Justice & Empowerment, Govt. of India), and a Professor in Computer Science & Engineering with over 23 years of teaching and research experience and 11 years in administration. He served as Registrar (Adl. Charge), Dean of A.U. TDR-HUB, Principal of WISTM Engineering College, and Mentor of American Corner. Holding a Ph.D. and five postgraduate degrees, he has 50+ patents/copyrights, 13 authored books, 70+ research publications, and has guided 13 Ph.D. scholars. With strong international exposure through invited lectures and academic collaborations abroad, he is known for applying technology to address societal challenges. He has received 12 national and international awards for excellence in education and research.

Dr. Poornaiah Billa is a Professor in the Department of Electronics and Communication Engineering at Lakireddy Bali Reddy College of Engineering, Mylavaram, Andhra Pradesh, India. With over 22 years of teaching and research experience, he has significantly contributed to the field by publishing 10 patents, more than 30 research papers in reputed international journals, and presentations at various international conferences. His research interests include Carbon Nanotube Electronics, focusing on modeling, design, and simulation, as well as the fabrication, characterization, and reliability studies of Polymer Thick Film Resistors, Nanobiosensors, and Flexible Electronics using carbon nanotubes. Additionally, he is involved in developing innovative diagnostic techniques for healthcare systems using Image Processing, Computer Vision, Machine Learning, and Deep Learning.