Journal of Information Security and Applications 79 (2023) 103628

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression

Monu Singh [a], Naman Baranwal [b], K.N. Singh [c], A.K. Singh [a,*], Huiyu Zhou [d]

[a] Department of Computer Science and Engineering, National Institute of Technology Patna, Ashok Rajpath, Patna, 800005, Bihar, India
[b] Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, 208016, Uttar Pradesh, India
[c] Department of Computer Science and Engineering & Information Technology, Jaypee Institute of Information Technology, Noida, 201309, Uttar Pradesh, India
[d] School of Computing and Mathematical Sciences, University of Leicester, LE17RH, United Kingdom

ARTICLE INFO

Keywords:
Biometric images
Encryption
Data hiding
Feature extraction
Compression
Security
Attacks

ABSTRACT

Images are promising information carriers when compared to other media documents in the healthcare domain. However, digital data transmission over unprotected wired or wireless networks poses a threat to the security of healthcare systems. As a result, the issue of copyright violation and identity theft can occur due to the unauthorised use of these data. This paper proposes a new secure method under a framework that embeds biometric fingerprint image features in a medical image without any perceptual distortion. This paper uses ResNet152 for biometric image feature extraction in the first stage and features to generate a secret key for embedding in the second stage. The method combines encryption and compression scheme based on a generated key, novel chaotic map and Huffman coding to enhance the security of medical images while reducing the storage consumption or bandwidth requirements if images are transmitted to remote servers. Experimental results show that the proposed method presents superior security with high imperceptibility and compression performance, ensuring its effectiveness as an image protection mechanism for medical applications. Extensive experimental results show that the proposed method achieves an average peak signal-to-noise ratio (PSNR) that is above 54 dB, a structural similarity index measure (SSIM) close to 1, a bit error rate (BER) of 0 and a normalised correlation (NC) of 1. Moreover, this method compresses the images up to 70% when tested on three standard datasets.

1. Introduction

With the development of healthcare information technology, many medical images are stored and transmitted to networks daily. These images contain significant information for the accurate diagnosis, treatment planning and real-time monitoring of patients [1]. Furthermore, a significant volume of healthcare images and related records are stored and shared over hard drives or third-party clouds for various services, including tele-medicine, tele-diagnosis and tele-consultation [2]. However, protecting medical data from unauthorised access and modification for researchers and medical professionals is a significant concern. It is evident that identity theft and tempering are becoming significant problems in the healthcare domain [3–5]. It is reported that medical identity theft in 2021 affected more than 40 million people and over 550 organisations in the United States [6]. As a result, how to protect medical images from unauthorised use has become an important research topic. To meet this challenge, current research mainly focuses on the encryption [7–10] and data hiding [11,12] of medical images. Image encryption modifies an image into an output that a third-party user cannot discern [8]. However, third-party users can easily compromise and access encrypted data after decryption. Therefore, an additional technique is required to protect this sensitive data when transmitted over the public channel so it cannot be retrieved. Data hiding is an important tool in the healthcare domain, aiming to protect digital media content and prevent unauthorised access and distribution [11]. This media can then be transmitted through a public channel without drawing the attention of a malicious third party. Fig. 1 demonstrates the framework of joint data hiding and encryption in the healthcare domain. Additionally, with the popularity of images in various potential applications, many compression techniques [13–18] are proposed for stronger compression ratios and less storage consumption. Biometrics, in addition to encryption and data hiding, are widely employed in numerous fields to identify individual identification based on physiological or behavioural characteristics, due

* Corresponding author.
E-mail addresses: monus.phd20.cs@nitp.ac.in (M. Singh), namanbaranwal2002@gmail.com (N. Baranwal), knsinghait@gmail.com (K.N. Singh), amit.singh@nitp.ac.in (A.K. Singh), hz143@leicester.ac.uk (H. Zhou).

https://doi.org/10.1016/j.jisa.2023.103628

Available online 29 October 2023

to their superior security performance. The most popular biometric modalities used in government sector as well as private industries are voice, iris, face, and fingerprint [19]. Additionally, gait-based biometric recognition and palmprint recognition have attracted a lot of attention recently [20]. Furthermore, deep learning is one the promising technique for identifying people by their biometrics [21]. Due to the ability to extract features and learn from large datasets, deep learning models have grown increasingly prominent in image processing applications. Motivated by data hiding, encryption and compression, this research proposes a new secure method under a framework that embeds biometric fingerprint image features in medical images without any perceptual distortion that prevents data leakage with fewer storage consumption or bandwidth requirements in healthcare scenarios. The contributions of this paper are summarised as follows:

1. *Secure key generation for data hiding and encryption:* Initially, we use ResNet152 for biometric image feature extraction as the first stage, followed by using a novel chaotic map with extracted features to generate a secure key in the second stage. The key space in our case is$2^{2048\times32}$, which is enough to resist a brute force attack.
2. *Hiding biometric image features using a secure key:* The generated key is then used to imperceptibly hide the significant patient fingerprint image features into the cover medical media. Therefore, in the case of healthcare, the concept of data hiding provides a valuable tool for reducing the many threats to the transmission and sharing of medical images, such as piracy, theft, and tampering [3].
3. *Strong encryption scheme:* A secure key is generated from the extracted features of a doctor's biometric fingerprint image and novel chaotic map, which is used in the confusion and diffusion process for encryption. It is established that chaotic maps are very sensitive to their initial values [7]. This makes the media document more secure and enables resistance to various types of attacks.
4. *Joint encryption-compression concepts:* Joint image encryption and compression algorithms are intensively investigated due to their powerful capability of simultaneous image data compression and sensitive information protection.
5. *Experiments:* Compared to traditional methods, our method improves security while maintaining the compression ratio and data hiding performance, which proves its feasibility and effectiveness for healthcare and any other practical application.

The rest part of this work is organised as follows. Section 2 summarises the related state-of-the-art techniques; Section 3 presents proposed approach with detailed description of the feature extraction, embedding, Joint encryption-compression, and extraction procedure; Section 4 discusses the experimental outcomes. Finally, Section 5 concludes this paper.

2. Literature review

Recently, many encryptions, joint encryption-compressions and joint data hiding- and encryption-compression-based techniques have been proposed, which greatly utilise powerful tools towards securing healthcare. Specifically, a three-dimensional (3D) chaotic system-based cryptosystem for colour images has been introduced [7]. The proposed permutation approach, based on a Rubik's cube, leads to confusion in an original image. Then, iterative diffusion is employed on the confused image to obtain the cipher image. The simulation results reveal that this scheme has a low encryption cost. However, its performance against statistical attacks is inadequate. Another image encryption algorithm based on logistic-sine combinatorial modular mapping has been proposed by Chen et al. [8]. Along with the generated complex chaotic sequences, V-shaped scrambling and bidirectional dynamic diffusion methods are used to make the image entirely chaotic. This scheme is resistant to statistical, noise and brute force attacks. However, the time required to produce the cipher image is long, and it is also vulnerable to differential attacks. Alexan et al. [9] proposed a secure encryption scheme for colour images based on a sine map, a 4D hyperchaotic Chen map of fractional-order and deoxyribonucleic acid (DNA) coding. A 4D Chen map is employed to produce an S-box. The plain image is first XORed, with the secret key generated using a sine map and then scrambled using the resulting S-box. Finally, DNA coding is applied to the scrambled image to create an encrypted image. It works well in terms of security when compared to other schemes, although its time complexity can be enhanced. In [10], the authors suggested an image encryption technique based on graph theory for securing digital images. The proposed approach treats the digital image's pixels as the nodes of a graph and assigns a certain amount of actual weight to each edge connecting the nodes. Furthermore, the authors utilised a minimum spanning tree (MST) and the weighted adjacency matrix of the MST to achieve the encryption effect. The results show that the scheme has the ability to resist brute force and statistical attacks, but its performance against differential attacks needs to be investigated further. Another major drawback of this work is its high computational cost. To reduce the problem of data leaks, efficient storage and transmission, encryption then compression (ETC)-based techniques have been developed. For example, a colour image ETC system was developed in [13]. The down-sampling technique is used to compress the images after they have been encrypted using modulo addition 256. The plain image is rebuilt using decryption and customised residual dense spatial networks on the encrypted–compressed image. The findings demonstrate the efficacy of compression, although additional security evaluations are needed. Singh et al. proposed a secure and efficient ETC scheme using generative adversarial networks (GAN) for colour images [14]. A pseudo-random sequence generator is designed, first using GAN to encrypt the plain colour image. The encrypted image is then downscaled to one-quarter of its original size before being transmitted to the recipient. Finally, the image is reconstructed by employing a customised super-resolution network instead of decompressing it at the receiver side. Compared to recent schemes, its compression performance is high, and its encryption speed is good, but further security analyses must be performed in terms of noise attacks. Similarly, in [15], authors aimed to develop secure and efficient encryption before applying the compression algorithm for greyscale images. In this study, SHA-256, DNA coding and a chaotic map are utilised to encrypt the plain images. Afterwards, these encrypted images are compressed based on a zero-memory set partitioned embedded block. The suggested method performs better than existing systems in terms of encryption cost and efficiency; however, its compression performance is subpar. To lower the computational cost, compression is done before encryption. Various compression and encryption (CTE) schemes have been developed. For instance, in [16], an efficient CTE system based on block compressed sensing (BCS) and a Chen chaotic map is designed. To improve the plaintext sensitivity, the initial parameters of the Chen system are obtained from the plain image. The plain image is scrambled using a secret key after being parsed through a discrete wavelet transform (DWT). Next, the scrambled image is compressed by employing BCS and a measurement matrix (MM). Finally, a cipher image is obtained by diffusing the pixels of the compressed image. The proposed work exhibits acceptable security performance and low computational cost. However, the compression performance can be enhanced further. Another image CTE scheme for securing digital images has been proposed by Wang et al. in [17]. First, a 2D cross-coupled map lattice (2D-CCML) model is built with a large key space to enhance the security of the proposed scheme. Next, compression is achieved by combining the MM generated by the 2D-CCML and compressive sensing (CS). Confusion and diffusion are carried out using the generated secret key and SHA-512 to make an image entirely chaotic. This method can withstand noise, cropping and brute force attacks but takes more time than other recent methods. Chai et al. [18] proposed an image CTE

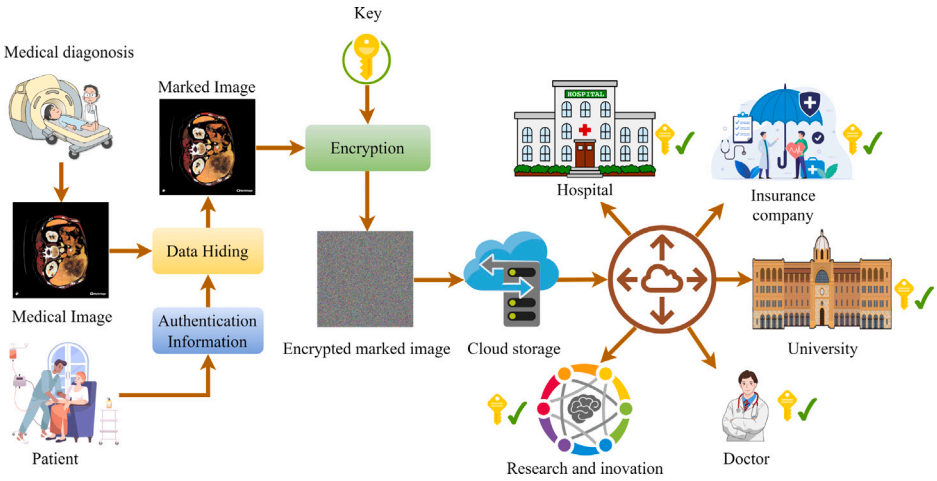

Fig. 1. A framework of joint data hiding and encryption in healthcare.

technique using a GAN, convolutional neural network (CNN), CS and chaotic map. Initially, sampling is performed to obtain the MM of the image. Then, it is scrambled using a logistic-tent chaotic map to get the compressed cipher image. The GAN is utilised to reconstruct the plain image after employing inverse scrambling operation on the cipher image. Additionally, CNN is used for de-noising to further enhance the quality of the reconstructed image. The proposed work exhibits adequate security performance at a low cost. However, the peak signal-to-noise ratio (PSNR) of the reconstructed images can be enhanced. Wang et al. [11] proposed a colour image encryption and hiding algorithm based on a chaotic map and discrete cosine transform (DCT). The authors suggested a 2D-CCCM to generate the key stream for encrypting the digital images. Confusion and diffusion were achieved using cross-plane scrambling and cyclic shift operation. Finally, an encrypted image is embedded into the carrier image using DCT. The outcomes demonstrate that the suggested technique is fast and can withstand common security attacks. However, its performance against other cryptographic attacks needs to be investigated further. In [12], Wang et al. combine a chaotic map, parallel compressive sensing and fast Fourier transform (FFT) to develop a visually secure cryptographic system. First, following a discrete DWT, Arnold scrambling is applied to two plain images. Then, a Hadamard matrix is used to compress both scrambled images. The two resulting measured secret images are then embedded into the cover image using FFT to create a final cipher image that is exactly the same size as the plain image. This approach is secure and saves a considerable amount of bandwidth but is not completely reversible, as there is an energy loss in image embedding and extraction, so the decrypted image quality will get affected. Overall, we noticed that the existing schemes struggle to strike a balance between security, compression ratio and time cost. For the encryption-then-compression technique, existing schemes have difficulty maintaining correlation in a plain image after encryption, making it hard to be compressed [22]. In contrast, for the compression-then-encryption technique, existing schemes have difficulty maintaining high security [22]. Although some methods based on encryption and compression brings a high level of security and fewer storage consumption or bandwidth requirements, there are still some difficulties in dealing with data leakage and copyright violation issues. This is especially true if you have a data leak (someone is leaking your images) and want to discover who it is. This paper proposes a new secure method under a framework that embeds fingerprint image features in medical images without any perceptual distortion. The method uses joint encryption–compression concepts, i.e. encrypts images during compression, and data hiding to address the above-discussed issues in most of the existing schemes.

3. Proposed method

The traditional encryption–compression-based methods mostly apply encryption-then-compres-sion/compression-then-encryption. In contrast, our proposed method achieves high security and compression performance by using joint encryption–compression concepts for medical images. Additionally, our method provides a solution for ownership conflicts and prevents data leakage by embedding image features through least significant bit (LSB) method in a specific location of the cover media. As illustrated in Fig. 2, our proposed method is based on a joint encryption–compression and data-hiding scheme. It can be described as follows:

3.1. Deep learning based feature extraction

We adopted deep CNN architecture, namely ResNet152, to extract the features from the fingerprint biometric images, as it has the highest accuracy among the residual network family [23]. Additionally, ResNet networks are easy to optimise because the training error does not rise significantly as the model depth increases. The ResNet152 model is pre-trained on ImageNet-1K. It utilises the concepts of residual learning and skips connections, which enables the training of the deeper model without compromising accuracy. We have extracted features of the patient's left (L) and right fingers (R) and the doctor's right fingerprint images. The doctor's fingerprint features are utilised for secure key generation, while the patient's fingerprints are hidden in the medical cover image for secure transmission and to avoid ownership conflict, if any.

3.2. Generation of secure key via biometric image features

Due to high randomness, sensitivity to the initial values and non-linear behaviour, chaotic maps have been extensively used in cryptosystems for secure key generation [7]. In our method, fingerprint biometric image features are utilised to generate the initial parameter for the proposed chaotic map. The ith parameter p_i can be obtained from doctor fingerprint image feature vector F, formulated as

$$p_i = XOR(F(8k+i) \forall k \in [0,255] \forall i \in [0,7]) \tag{1}$$

Then, initial parameters are passed to a novel proposed chaotic map, which is formulated as

$$\begin{cases} X_{n+1} = f(X_n^3 + X_n Y_n + 2ab) \\ Y_{n+1} = g(\sqrt{X_n + Y_n} + Y_n^2) \end{cases} \tag{2}$$

where $f(x) = 4x \times sin(1-x)$ and $g(x) = 4x \times cos(1-x)$, $X_{n+1} \in (0,1)$ and $Y_{n+1} \in (0,1)$ are next sequence of X_n and Y_n. a and b are the control

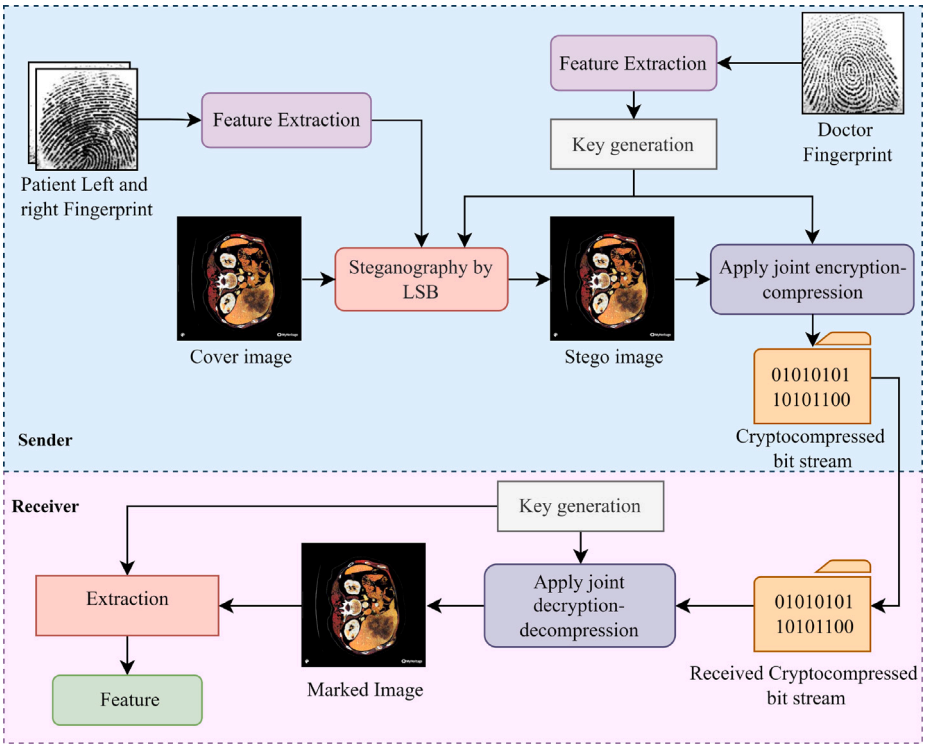

Fig. 2. Architecture of proposed scheme.

parameters. For a = 0.115 and b = 0.564 the proposed system shows the chaotic behaviour. The pseudocode for the secure key generation is shown in Algorithm 1 and the performance is discussed in experimental section.

Algorithm 1 Key Generation

Input: Doctor's Fingerprint D, Length L
Output: Key R

$F = ResNet152(D)$
$size = Length(F)$
$P = []$
for i = 0 to 8 **do**
  $T = XOR(F(i : size : 8))$
  $Push\ T\ to P$
end for
$c = 0$
for i = 0 to 16 **do**
  $P(c), P(c+1) = Map(P(c), P(c+1))$
  $c = mod(c+1, 8)$
end for
$R = []$
for i = 0 to L/2 **do**
  $P(c), P(c+1) = Map(P(c+1), P(c))$
  $Push P(c)\ and\ P(c+1)\ to\ R$
  $c = mod(c+1, 8)$
end for
Return R

3.3. Embedding process

The L and R patient features are hidden in a cover medical image. The features are first concatenated together and converted to binary. The pixels of the cover image are selected randomly by utilising the secure generated key. The position of bits is also defined by the key. In this process, each of the pixel's corresponding bits is replaced by the current feature's bits. This process is repeated until all feature bits are hidden. The process can be represented as:

$$C(R(i)) = \begin{cases} (C(R(i)) AND 254) + F(i), if\ mod(R(i), 3) = 0 \\ (C(R(i)) AND 253) + F(i), if\ mod(R(i), 3) = 1 \\ (C(R(i)) AND 251) + F(i), if\ mod(R(i), 3) = 2 \end{cases} \quad (3)$$

where F is concatenated binary features and R is key generated, C is the cover image and $i \in [0, length(F))$. Further, hiding process is depicted in Algorithm 2.

Algorithm 2 Data Hiding

Input: Features $F1$, $F2$, Cover Image C, Key$K$
Output: Stego Image S

$S = Copy(C)$
$F = Concatenate(F1, F2)$
$F = Binary(F)$
$R = Argsort(K)$
for i = 0 to length(F) **do**
  if mod(K(i), 3) = 0 **then**
    $S(R(i)) = AND(S(R(i)), 254) + F(i)$
  else if mod(K(i), 3) = 1 **then**
    $S(R(i)) = AND(S(R(i)), 253) + F(i)$
  else
    $S(R(i)) = AND(S(R(i)), 251) + F(i)$
  end if
end for
Return S

3.4. Joint encryption and compression

After the embedding process, encrypting images during compression is a key part of the proposed method. The scrambling and diffusion process is introduced in the Huffman coding scheme to achieve the joint encryption-compression scheme. As illustrated in Fig. 3, the joint encryption-compression scheme can be described as follows:

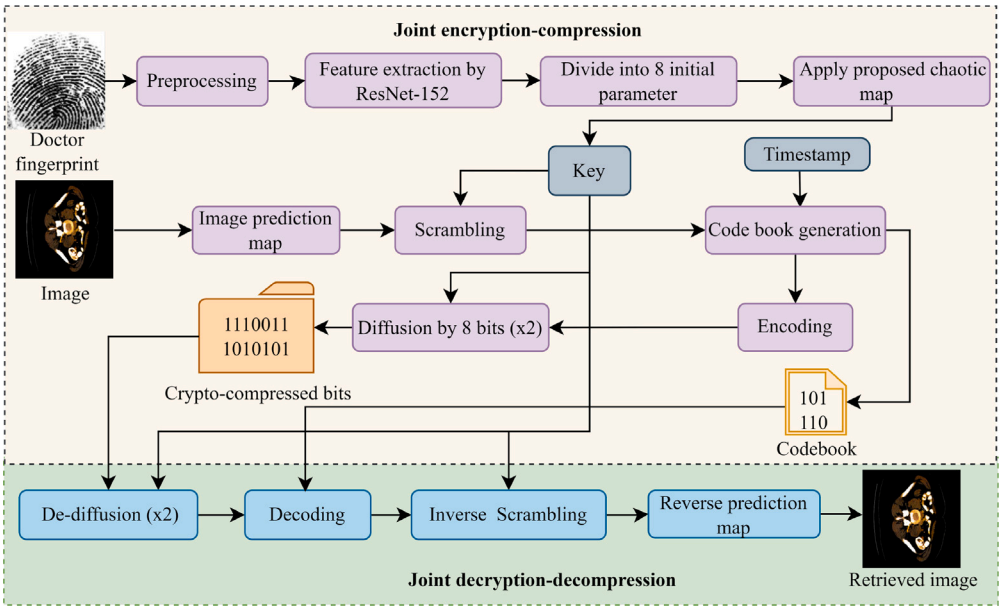

Fig. 3. Block diagram of joint encryption-compression system.

3.4.1. Prediction map creation

The stego (marked) image contains a significant amount of correlation, also known as inter-pixel redundancy. The removal of the redundancy is crucial to compress the file. The prediction map removes the correlation between adjacent pixels, thereby reducing the redundancy of the pixels of the stego image, thus, minimising the space required to store them. In this step, following [24] process is applied to the stego image to obtain prediction map which can be given as :

$$x_{i,j} = \begin{cases} x_{i,j} - x_{i,j-1}, if\ i = 0\ and\ j > 0 \\ x_{i,j} - x_{i-1,j}, if\ i > 0\ and\ j = 0 \\ x_{i,j} - \bar{x}_{i,j}, else \end{cases} \tag{4}$$

where $\bar{x}_{i,j}$ is defined as

$$\bar{x}_{i,j} = \begin{cases} min(x_{i,j-1}, x_{i-1,j}), if\ x_{i-1,j-1} \geq max(x_{i,j-1}, x_{i-1,j}) \\ max(x_{i,j-1}, x_{i-1,j}), if\ x_{i-1,j-1} \leq min(x_{i,j-1}, x_{i-1,j}) \\ x_{i,j-1} + x_{i-1,j} - x_{i-1,j-1}, else \end{cases} \tag{5}$$

Initially $\forall i$ and $j, x_{i,j} = I_{i,j}$ where $x_{i,j}$ is the pixel value of ith row and jth column of image I.

3.4.2. Scrambling of prediction map

To improve the randomness, we use scrambling of prediction map including generated key. The scrambling process is formulated as

$$X(i), X(K(i)) = X(K(i)), K(i)\ \forall i \in [0, length(X)) \tag{6}$$

where X is the prediction map calculated in previous step and K is key generated.

3.4.3. Generation of code book

Before encoding, the scrambled prediction map is utilised to create a Huffman coding tree. The Huffman tree utilises a heap structure to correspond the binary code to each symbol. It assigns the smallest binary code for the most frequent symbols. The tree contains bit sequences for all values by ranking their frequency. Once the coding tree is complete, a coding table is obtained. This coding table is divided into multiple planes that have the same length of bit sequences. These planes are shuffled, taking time to seed the value. This forms a new codebook that is used in the subsequent steps. This codebook can be represented as:

$$C = \{v_k : c_k\ where\ v_k \in X\} \tag{7}$$

where v_k is the unique value present in X which is scrambled prediction map and c_k is the respective code generated by Huffman coding tree.

3.4.4. Encoding

After the generation of codebook, every value in the scrambled prediction map X is encoded using the codebook by following process

$$E = \{C(X(i))\ \forall i \in [0, length(X))\} \tag{8}$$

where C is the codebook generated in the previous step and X is scrambled prediction map. After encoding, all values are concatenated together to form a single crypto-compressed bit sequence. This sequence is passed to the next step.

3.4.5. Diffusion

After obtained crypto-compressed bit sequences, diffusion process is applied to it. It utilises key generated by proposed chaotic map. The sequences of 8–8 bits are subjected to diffusion process. This process is given as:

$$A_i = mod((A_i + A_{i-1} + K_i), 256) \tag{9}$$

where A_i is the ith sequence of 8-bit. K_i is ith random number in key K. This process is repeated two times to ensure the maximum security. After this process, the sequence and code book is sent to receiver. The complete process of joint encryption–compression is presented in Algorithm 3.

Algorithm 3 Joint Encryption and Compression

Input: Stego Image S, Key K, Timestamp T
Output: Crypto-compressed bits E, Codebook C_s

$X = PredictionMap(S)$
$X_s = Scramble(X, K)$
$C = GenerateCodebook(X)$
$C_s = PlaneScramble(C, T)$
$X_f = Flatten(X_s)$
$E = Encode(X_f, C_s)$
for i = 0 to 2 **do**
  $E = Diffuse(E, K)$
end for
Return E, C_s

3.5. Joint decryption–decompression

Under this process, we decrypt and decompressed the crypto-compressed bit sequence back to their original form utilising the

codebook received. This process is just reverse of the joint-encryption process. It consists of first de-diffusion of bit sequence utilising the key generated. Then, the sequence is decoded using the received codebook. The obtained prediction map is descrambled. Lastly, the descrambled prediction map is subjected to inverse of prediction map using Eq. (4). The entire process is represented in Algorithm 4.

Algorithm 4 Joint Decryption and Decompression

Input: Crypto-compressed bits E, Codebook C_s, Key K, Timestamp T
Output: Stego Image S

for i = 0 to 2 **do**
  $E = DeDiffuse(E, K)$
end for
$X = Decode(E, C)$
$X_s = Reshape(X)$
$X_d = Descramble(X_s, K)$
$S = InversePredictionMap(X_d)$
Return S

3.6. Extraction process

Finally, the features from the stego image are extracted. The extraction process involves selecting the pixels where data was hidden using the key generated, realising the bit position where data was stored and extracting that bit from that pixel. The process of extraction is given in Algorithm 5.

Algorithm 5 Data Extraction

Input: Stego Image S, Key K
Output: Features $F1$, $F2$

$R = Argsort(K)$
$D = [\,]$
for i = 0 to length(F) **do**
  if mod(K(i), 3) = 0 **then**
    $V = AND(S(R(i)), 1)$
  else if mod(K(i), 3) = 1 **then**
    $V = AND(S(R(i)), 2)$
  else
    $V = AND(S(R(i)), 4)$
  end if
  Push V to D
end for
$D = Decimal(D)$
$F1, F2 = Deconcatenate(D)$
Return $F1$, $F2$

4. Experiments

This section will analyse the performance of our suggested work in terms of the randomness performance of the proposed map, security, compression ratio, data hiding, and time complexity. The fingerprint images are taken from the Sokoto Coventry Fingerprint Dataset [25]. Extensive experiments are performed on the spleen and colon datasets from the Medical Segmentation Decathlon (image size 512 × 512 × 3) [26], The Liver Tumour Segmentation Benchmark (LiTS) dataset (image size 256 × 256 × 3) [27] and Sea-animal (variable image size) [28] dataset to validate the work. The tests were performed using Python 3.10 on a PC configured with an Intel(R) Core(TM) i5-9400F CPU, operating at 4.1 GHz, 16 GB of RAM and Windows 11.

4.1. Randomness performance

Any map used in encryption should have highly chaotic behaviour. The randomness of the proposed map is assessed by the NIST test, Lyapunov exponent analysis, and bifurcation diagrams.

4.1.1. NIST test

SP800-22 Test Suite [29] is a collection of 15 standard statistical tests to measure the randomness in the sequences. For each standard test a P-value is calculated. The sequence is considered random if the p-value is greater than 0.01. The test is repeated ten times, each time a p-value higher than 0.1 is achieved for all standard statistical tests. The NIST test analysis is presented in Fig. 4. This analysis indicates that the proposed chaotic map generates highly random sequences.

4.1.2. Lyapunov exponent(LE)

LE are used to verify the chaotic behaviour of chaotic systems. A chaotic system should have at least one positive LE [30]. LE is defined as

$$LE = \lim_{n\to\infty} \frac{1}{m} \sum_{k=1}^{m-1} \ln |f'(P_k)| \tag{10}$$

where f' is the differential of chaotic map. For n dimensional chaotic map n positive LE are exist. Since our map is two dimensional hence we achieve two positive LE. The maximum LE values are achieved as $LE1 = 20.82$, $LE2 = 20.82$, Minimum LE value are $LE1 = 20.27$ and $LE2 = 20.43$, whereas average LE values are $LE1 = 20.68$ and $LE2 = 20.67$. The graphical representation of LE are shown in Fig. 5. This analysis indicates that we achieved two large LE values, therefore, the proposed map is highly chaotic in nature as well as suitable for encryption purpose.

4.1.3. Bifurcation diagram

A bifurcation diagram is a technique for examining the behaviour of a chaotic system. Bifurcation is plotted against variables vs. parameters. Bifurcation diagram shows how a variable changes when the value of parameter changes. In order to prove chaotic properties of our proposed map we have plotted bifurcation diagram of X, Y vs. A, B. Fig. 6 indicates the bifurcation diagram of our proposed chaotic map. The Figure consists of only dense areas. There is no presence of shallow areas hence it proves the chaotic behaviour of our proposed map.

4.2. Security results

The effectiveness of our work against different security assaults is measured using the following specific metrics: statistical and differential attack analysis, key space and entropy analysis.

4.2.1. Key analysis

The key space should be $> 2^{100}$ to stave off brute force attack [31]. The chaotic map suggested above is used to produce the secret key. The initial values of proposed map is generated by feature vector which has 2048 features in it and each feature is represented in 32 bit. Hence the key space of proposed scheme is $2^{2048\times32}$. The key space is large enough to resist the brute force attack.

4.2.2. Statistical analysis

(i) Histogram analysis. The histogram analysis has been used to evaluate the performance of our scheme against statistical attacks. Histogram displays the distribution of pixels in an image [31]. The histogram of the encrypted image should be uniform and differ significantly from the plain image histogram. Fig. 7 displays the histogram of plain image and the encrypted image. It is clear that the two histograms are completely distinct from one another and the histogram of the encrypted image is uniform. It implies that the information about plain image cannot be retrieved from encrypted image, and the proposed encryption scheme is immune to statistical attacks.

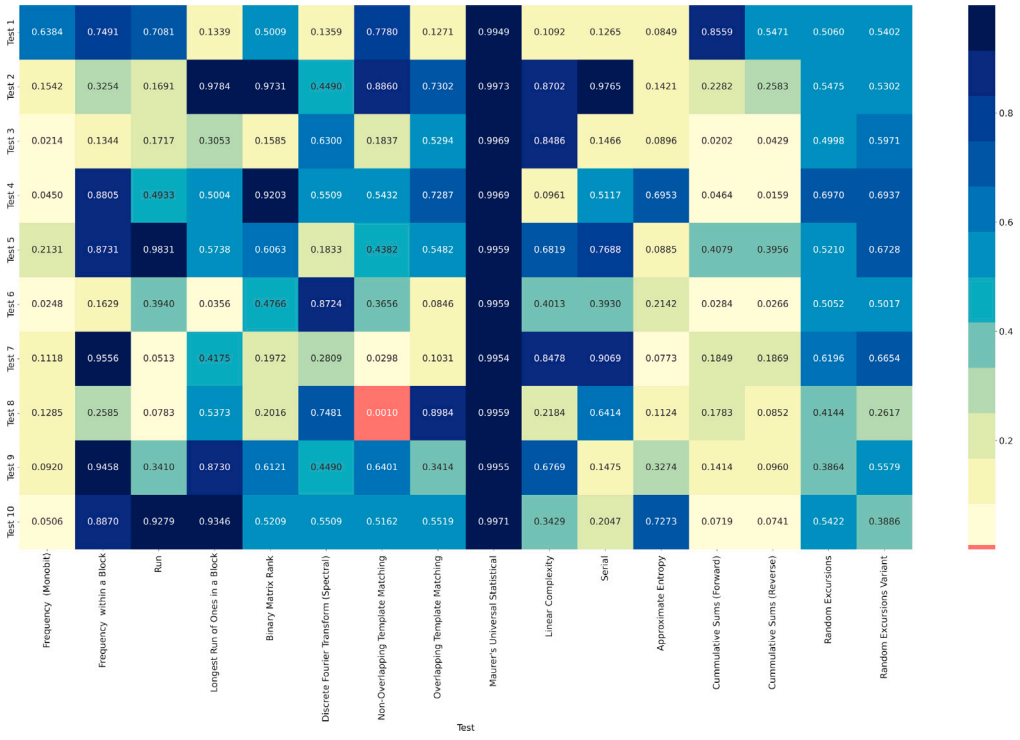

Fig. 4. Heat map of NIST test for 10 Sequences.

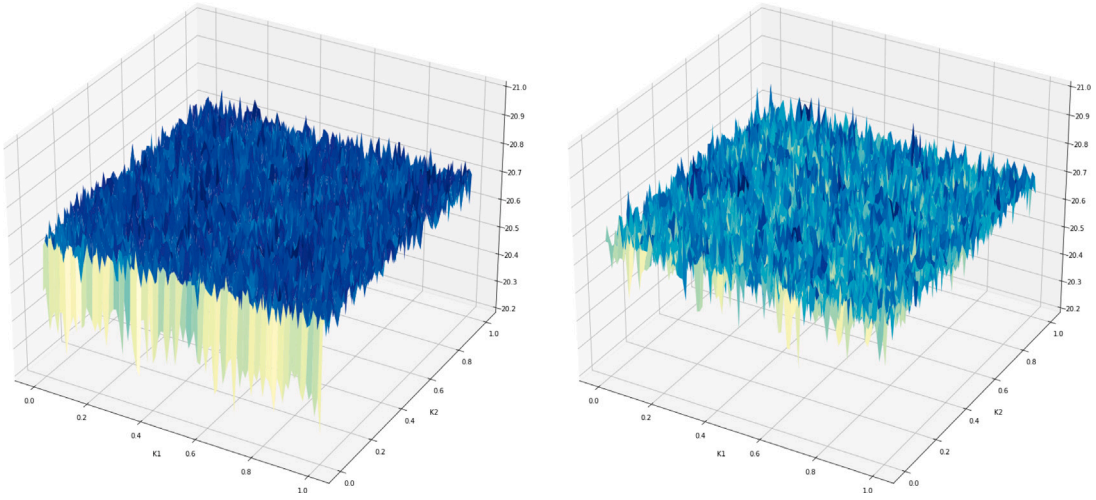

Fig. 5. LE for X, Y, and Z with respect to a and b.

(ii) Correlation analysis. It is expected that an effective encryption technique will reduce the correlation between neighbouring pixels to a negligible level [14]. The following formulas are used to define the correlation coefficients between neighbouring pixels:

$$r_{x,y} = \frac{C_{x,y}}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

$$C_{(x,y)} = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K} \tag{12}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \tag{13}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2 \tag{14}$$

where x, y = Coordinates of an image pixel; $C(x, y)$ = Covariance between samples x and y; K = number of pixel pairs (x_i, y_i); $D(X)$ and $D(Y)$ = Standard deviation of x and y, and $E(x)$ = Mean of x_i pixel values. The correlation in encrypted images should be reduced to zero. The proposed approach successfully reduces the correlation value in encrypted images near to 0 as shown in Table 1. We achieved average encrypted correlation for spleen, colon, LiTS and Sea-animal datasets are −0.00011, −0.00023, −0.00097 and −0.00021, respectively. Additionally, the correlation between plain and cipher image is shown in Fig. 8. The plain image's pixels are positioned on the coordinate axis in the diagonal position. Comparatively, the pixels of the encrypted images are dispersed over the coordinate space, which shows there is nearly no correlation. Thus, the suggested algorithm can withstand statistical attacks effectively.

Table 1
Security results analysis.

Image/Dataset	Plain image col	Enc. image col	Plain image entropy	Enc. image entropy	NPCR	UACI
1	0.97944	−0.00061	1.6091	7.9992	0.996213	0.332803
1000	0.97788	0.00179	1.8462	7.9993	0.995958	0.332900
10 094	0.97999	−0.00043	1.2972	7.9995	0.996092	0.334174
10 095	0.97881	0.00108	1.2860	7.9995	0.996195	0.333749
volume-0_slice_35	0.61719	0.00150	5.1465	7.9981	0.996193	0.335201
volume-0_slice_48	0.69012	−0.00428	5.2020	7.9983	0.996089	0.334301
10028936315_d56a1c1409_b	0.26019	0.00087	7.4729	7.9979	0.995912	0.333144
10426682916_90a97e796f_o	0.28780	−0.00468	6.2187	7.9976	0.996272	0.334023
Avg. of spleen dataset	0.97668	−0.00011	2.1324	7.9992	0.996083	0.333375
Avg. of colon dataset	0.97581	−0.00023	1.7370	7.9995	0.996090	0.334596
Avg. of LiTS dataset	0.65962	−0.00097	5.2769	7.9983	0.996106	0.334791
Avg. of Sea-Animal dataset	0.49377	−0.00021	6.8415	7.9978	0.996079	0.333301

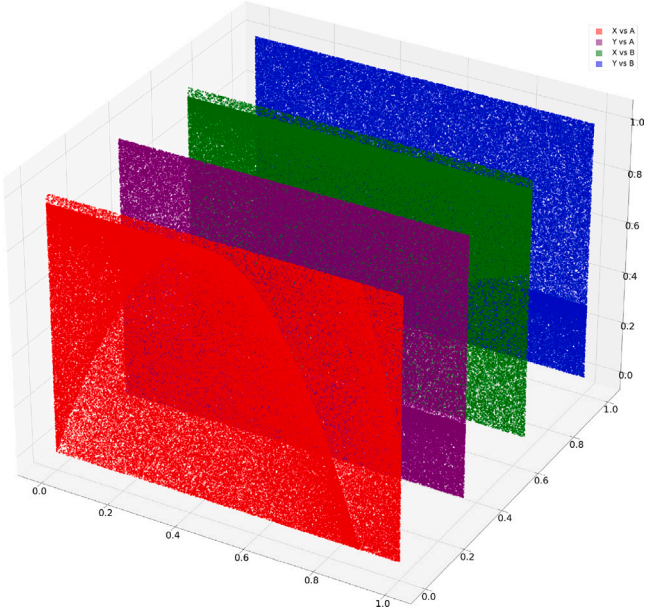

Fig. 6. Bifurcation diagram of X, Y vs. A, B.

(iii) Entropy. Entropy is an important factor to consider for evaluating the randomness of information per bit in an image [15]. We can figure it out using Eq. (15).

$$E(x) = -\sum_{i=0}^{255}(P(S_i) \times log_2 P(S_i)) \tag{15}$$

where, $H(s)$ = Entropy of message source (S) and $P(S_i)$ = Probability of occurrence of S_i. Cipher images that have entropy value near to 8 are less likely to accidentally release information. In Table 1, the entropy values of the sample images and the average entropy value across all images in the four datasets are presented. The average entropy value of the proposed scheme for encrypted spleen, colon, LiTS and Sea-animal datasets are 7.9992, 7.9995, 7.9983 and 7.9978 respectively. It can be observed that the entropy values of all encrypted images are close to the ideal score, i.e., 8. This analysis reveals that our encrypted image is highly random.

4.2.3. Differential analysis

To measure the performance of an encryption scheme against differential attacks, two metrics number of pixel change rate (NPCR) and unified average changing intensity (UACI) are often used [15]. The ideal values of NPCR and UACI for differential attack protection are 99.6094% and 33.4635% respectively. It is defined as follows:

$$NPCR = \frac{1}{W \times H}\sum_{i,j} D(i,j) \tag{16}$$

Table 2
Time cost evaluation.

Image/Dataset	Size	Encryption time (s)	Decryption time (s)
1	512 × 512 × 3	4.0090	4.0720
1000	512 × 512 × 3	4.5170	3.1640
10 094	512 × 512 × 3	4.6799	3.6253
10 095	512 × 512 × 3	4.6845	3.6309
volume-0_slice_35	256 × 256 × 3	1.4509	1.1203
volume-0_slice_48	256 × 256 × 3	1.4312	1.0952
10028936315_d56a1c1409_b	185 × 300 × 3	1.4040	0.9360
10426682916_90a97e796f_o	200 × 300 × 3	0.9390	0.6920
Avg. of spleen dataset	512 × 512 × 3	4.6890	3.4230
Avg. of colon dataset	512 × 512 × 3	4.1572	3.0842
Avg. of LiTS dataset	256 × 256 × 3	1.4925	1.1471
Avg. of Sea-Animal dataset	Variable	1.3770	1.0490

$$UACI = \frac{1}{W \times H}\sum_{i,j}\frac{|C1(i,j) - C2(i,j)|}{255} \tag{17}$$

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, otherwise \end{cases} \tag{18}$$

Here, $C1$ and $C2$ are encrypted images before and after alteration of pixel respectively. Table 1 indicates the average value of NPCR and UACI obtained with four datasets. The average NPCR value for spleen, colon, LiTS and Sea-animal datasets are obtained as 0.996083, 0.996090, 0.996106 and 0.996079 respectively, whereas the UACI values are 0.333375, 0.334596, 0.334791, 0.333301 respectively. The NPCR and UACI values of our proposed scheme are near to ideal values. Thus, the proposed scheme is immune to differential attacks.

4.2.4. Speed evaluation

The time taken by proposed approach for encryption and decryption process is shown in Table 2. We obtained encryption and decryption time for image of size 256 × 256 × 3 are 1.4312 and 1.0952 s, respectively. Whereas for image of size 512 × 512 × 3, it is 4.0090 and 4.0720 s. The average time to encrypt/decrypt spleen, colon, LiTS and Sea-animal datasets is 4.689/3.4230 s, 4.1572/3.0842 s, 1.4925/1.1471 s and 1.377/1.049 s, respectively. Time taken by the proposed method is reasonable and can be used in practical application.

4.3. Compression performance

The average values of compression ratio (CR) [12] obtained on spleen, colon, LiTS and Sea-animal datasets are 0.3047, 0.4936, 0.5460 and 0.4654 respectively. It means that the proposed method reduces the original image size up to 70%, 51%, 46% and 54% as shown in Table 3. The results of this analysis demonstrate that proposed algorithm has good compression performance. Thus, our proposed scheme is able to reduce the storage space and bandwidth requirements effectively.

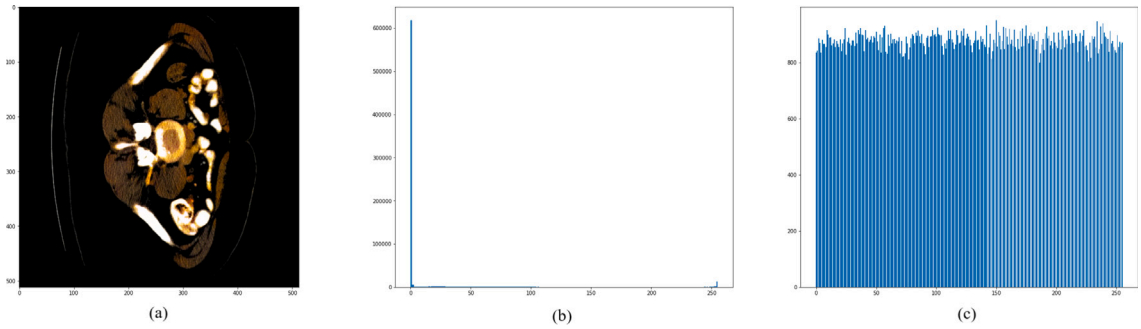

Fig. 7. (a) Plain image (b) plain image histogram (c) cipher image histogram.

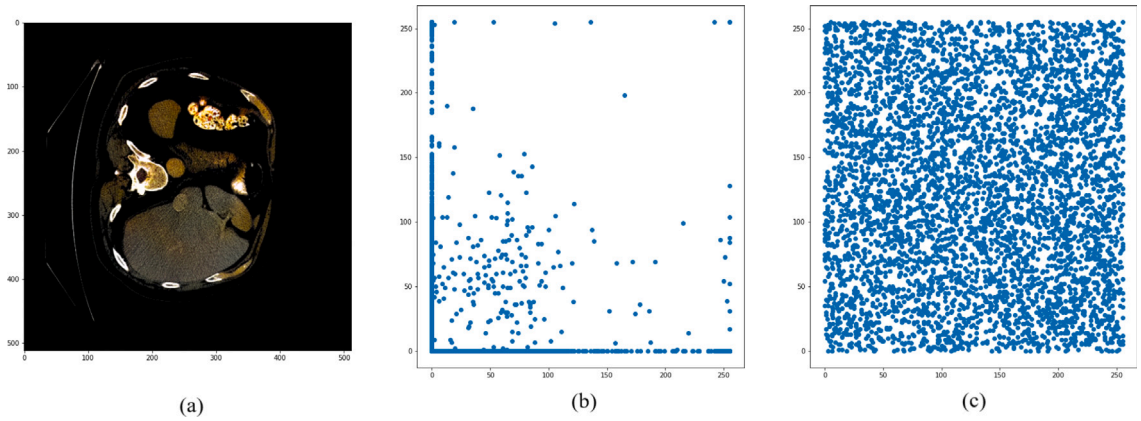

Fig. 8. (a) Original image, (b) correlation in plain image, (c) correlation in cipher image.

Table 3
Compression results.

Image/Dataset	CR	Image/Dataset	CR
1	0.2736	volume-0_slice_35	0.5437
1000	0.2752	volume-0_slice_48	0.5333
10 094	0.4660	10028936315_d56a1c1409_b	0.5319
10 095	0.4662	10426682916_90a97e796f_o	0.4322
Avg. of spleen dataset	0.3047	Avg. of LiTS dataset	0.5460
Avg. of colon dataset	0.4936	Avg. of Sea-Animal dataset	0.4654

Table 4
Data hiding results.

Cover	PSNR	SSIM	NC	BER
1	55.9508	0.99770	1	0
1000	55.8910	0.99756	1	0
10 094	42.7087	0.83475	1	0
10 095	42.7062	0.83481	1	0
volume-0_slice_35	48.6907	0.99191	1	0
volume-0_slice_48	48.6826	0.99161	1	0
10028936315_d56a1c1409_b	46.7939	0.98652	1	0
10426682916_90a97e796f_o	47.4517	0.98489	1	0
Avg. of spleen dataset	55.8327	0.99769	1	0
Avg. of colon dataset	42.7040	0.84606	1	0
Avg. of LiTS dataset	48.6726	0.99184	1	0
Avg. of Sea-Animal dataset	47.6074	0.98745	1	0

4.4. Data hiding performance

Four metrics, the PSNR, SSIM, NC [32] and BER, are utilised to assess the effectiveness of the suggested data-hiding scheme. The PSNR and SSIM are computed between the original and stego images to measure the imperceptibility of the algorithm. The BER measures the ratio between the number of wrongly extracted bits and the total number of embedded bits. In contrast, the NC demonstrates the resemblance between the embedded data (M) and the extracted data (M'). The PSNR and SSIM values for the stego image reach up to 55.8327 dB, 0.99769 for the spleen dataset, 42.7040 dB, 0.84606 for the colon dataset, 48.6726 dB, 0.99184 for the LiTS dataset and 47.6074 dB and 0.98745 for the Sea-animal dataset, respectively (see Table 4). It indicates that the stego image has a high resemblance with the carrier image and is not likely to attract the attention of hackers. Thus, we can say that the proposed algorithm is highly imperceptible. Furthermore, we achieve an NC of 1 and BER of 0 while extracting the features from the stego image. Therefore, the proposed algorithm can extract information without any loss.

4.5. Comparative analysis

To assess the performance of the proposed scheme, we compare the results with the recent state-of-the-art schemes in Table 5. We compare the average value of correlation, entropy, NPCR, UACI, key space, and encryption–decryption time (sec). From this table, it can be observed that the correlation score of our scheme is closer to zero when compared to other schemes. The entropy score of our proposed scheme is superior among all, and the NPCR and UACI scores are closer to their ideal values of 99.6094% and 33.4635%, respectively. The key space is the largest among all schemes. Furthermore, the encryption time and decryption time of our proposed scheme is also much lower. The encryption time of our scheme is about 90%, 28% and 91% faster than schemes [10,34,35], and the decryption time is 93%, 60% and 80% faster than schemes [10,33,34]. The comparative analysis demonstrates that the proposed scheme is secure and very efficient.

5. Conclusion

In this paper, we proposed an effective and new secure method that improves the security of medical images without any perceptual distortion and reduces time complexity. Specifically, the method uses

Table 5
Security comparison.

Method	Size	Correlation	Entropy	Key space	NPCR	UACI	Encryption time (s)	Decryption time (s)
[10]	256 × 256 × 3	0.022789	7.9975	$256^{16^2}-1$	–	–	15.423	–
[33]	512 × 512 × 3	0.01329	7.9993	2^{448}	0.996266	0.362376	1.493	7.807
[34]	512 × 512 × 3	−0.00092	7.997	2^{294}	0.9961	–	5.803	15.123
[35]	512 × 512 × 3	0.00110	7.9989	2^{2048}	0.997548	0.466056	47.420	–
Our	256 × 256 × 3	−0.00097	7.9983	$2^{2048\times32}$	0.996106	0.334791	1.493	1.147
	512 × 512 × 3	−0.00023	7.99953	$2^{2048\times32}$	0.996090	0.334596	4.157	3.084

biometric image features to generate a secret key for mark embedding and encryption of the carrier image before transmission over the remote server. The carrier image is marked by the biometric image features using a secret key and LSB. As a result, marked carrier images have been encrypted and compressed by a novel chaotic map and Huffman coding to contain more secure images with low storage consumption and a high compression ratio. Importantly, the fact that the biometric image feature is based on data hiding and joint encryption–compression makes it more effective in preventing data leakage with fewer storage consumption or bandwidth requirements in healthcare scenarios. To validate our proposed method's applicability in the medical field, twelve evaluation metrics are employed to evaluate the performance. Furthermore, the proposed method performs better than the most advanced schemes, effectively validating the method from illegal users. The method will further secure deep learning models along with multimedia documents while reducing the cost in future works.

CRediT authorship contribution statement

Monu Singh: Conceptualization, Investigation, Methodology, Software, Writing – original draft. **Naman Baranwal:** Methodology, Software, Validation. **K.N. Singh:** Formal analysis, Validation, Writing – review & editing. **A.K. Singh:** Supervision, Conceptualization, Validation, Investigation, Methodology, Software, Writing – review & editing. **Huiyu Zhou:** Supervision,Validation, Investigation, Editing.

Declaration of competing interest

I certify that they have NO affiliations with or involvement in any organisation or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this manuscript (Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression).

Data availability

No data was used for the research described in the article.

Acknowledgements

This work is supported by research project order no. IES212111 - International Exchanges 2021 Round 2, dt. 28 Feb 2022, under Royal Society, UK. All authors approved the version of the manuscript to be published.

References

[1] Fan C, Hu K, Yuan Y, Li Y. A data-driven analysis of global research trends in medical image: A survey. Neurocomputing 2022.
[2] Mahyudin MF, Novamizanti L, Sa'idah S. Robust watermarking using arnold and hybrid transform in medical images. In: 2021 IEEE international conference on industry 4.0, artificial intelligence, and communications technology (IAICT). IEEE; 2021, p. 180–5.
[3] Anand A, Singh AK. Watermarking techniques for medical data authentication: a survey. Multimedia Tools Appl 2021;80:30165–97.
[4] Magdy M, Hosny KM, Ghali NI, Ghoniemy S. Security of medical images for telemedicine: a systematic review. Multimedia Tools Appl 2022;81(18):25101–45.
[5] Singh AK, Anand A, Lv Z, Ko H, Mohan A. A survey on healthcare data: a security perspective. ACM Trans Multimedia Comput Commun Appl 2021;17(2s):1–26.
[6] 14 gripping medical ID theft statistics to ponder on in 2023 [Online]. https://safeatlast.co/blog/medical-id-theft-statistics/#gref.
[7] Xin J, Hu H, Zheng J. 3D variable-structure chaotic system and its application in color image encryption with new Rubik's cube-like permutation. Nonlinear Dynam 2023;1–24.
[8] Chen R, Li X, Teng L, Wang X. An image encryption algorithm based on the LSCMM chaotic map and bidirectional dynamic diffusion. Multimedia Tools Appl 2023;1–26.
[9] Alexan W, Gabr M, Mamdouh E, Elias R, Aboshousha A. Color image cryptosystem based on Sine chaotic map, 4D chen hyperchaotic map of fractional-order and hybrid DNA coding. IEEE Access 2023.
[10] Joshi AB, Kumar D, Kumar S, Singh S. A novel method of digital image encryption using graph theory. Multimedia Tools Appl 2023;1–26.
[11] Wang X, Xu X, Sun K, Jiang Z, Li M, Wen J. A color image encryption and hiding algorithm based on hyperchaotic system and discrete cosine transform. Nonlinear Dynam 2023;1–24.
[12] Wang X, Liu C, Jiang D. An efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing. Inform Sci 2022;610:300–25.
[13] Wang C, Zhang T, Chen H, Huang Q, Ni J, Zhang X. A novel encryption-then-lossy-compression scheme of color images using customized residual dense spatial network. IEEE Trans Multimed 2022.
[14] Singh M, Baranwal N, Singh KN, Singh AK. Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network. IEEE Trans Consum Electron 2023.
[15] Singh KN, Singh OP, Singh AK. Ecis: encryption prior to compression for digital image security with reduced memory. Comput Commun 2022;193:410–7.
[16] Luo Y, Liang Y, Zhang S, Liu J, Wang F. An image encryption scheme based on block compressed sensing and Chen's system. Nonlinear Dynam 2023;111(7):6791–811.
[17] Wang M, Wang X, Wang C, Xia Z, Zhou S. Novel image compression-then-encryption scheme based on 2D cross coupled map lattice and compressive sensing. Multimedia Tools Appl 2023;1–27.
[18] Chai X, Tian Y, Gan Z, Lu Y, Wu X-J, Long G. A robust compressed sensing image encryption algorithm based on GAN and CNN. J Modern Opt 2022;69(2):103–20.
[19] Rida I, Al-Maadeed N, Al-Maadeed S, Bakshi S. A comprehensive overview of feature representation for biometric recognition. Multimedia Tools Appl 2020;79:4867–90.
[20] Iqbal F, Abbasi A, Javed AR, Almadhor A, Jalil Z, Anwar S, Rida I. Data augmentation-based novel deep learning method for deepfaked images detection. ACM Trans Multimedia Comput Commun Appl 2023.
[21] Parashar A, Shekhawat RS, Ding W, Rida I. Intra-class variations with deep learning-based gait analysis: A comprehensive survey of covariates and methods. Neurocomputing 2022.
[22] Singh KN, Singh AK. Towards integrating image encryption with compression: a survey. ACM Trans Multimedia Comput Commun Appl (TOMM) 2022;18(3):1–21.
[23] He K, Zhang X, Ren S, Sun J. Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2016, p. 770–8.
[24] Yang Y, He H, Chen F, Yuan Y, Mao N. Reversible data hiding in encrypted images based on time-varying huffman coding table. IEEE Trans Multimed 2023.
[25] Shehu YI, Ruiz-Garcia A, Palade V, James A. Sokoto coventry fingerprint dataset. 2018, arXiv preprint arXiv:1807.10609.
[26] Antonelli M, Reinke A, Bakas S, Farahani K, Kopp-Schneider A, Landman BA, Litjens G, Menze B, Ronneberger O, Summers RM, et al. The medical segmentation decathlon. Nat Commun 2022;13(1):4128.
[27] LiTS dataset [online]. 2023, https://www.kaggle.com/datasets/harshwardhanbhangale/lits-dataset. Accessed: 2023-04-30.

[28] Sea-animals dataset [online]. 2023, https://www.kaggle.com/datasets/vencerlanz09/sea-animals-image-dataste. Accessed: 2023-04-30.
[29] Toughi S, Fathi MH, Sekhavat YA. An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. Signal Process 2017;141:217–27.
[30] Briggs K. An improved method for estimating liapunov exponents of chaotic time series. Phys Lett A 1990;151(1–2):27–32.
[31] Bhowmik S, Acharyya S. Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm. J Inf Secur Appl 2023;72:103391.
[32] Anushiadevi R, Amirtharajan R. Separable reversible data hiding in an encrypted image using the adjacency pixel difference histogram. J Inf Secur Appl 2023;72:103407.
[33] Ahmad I, Shin S. A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. Signal Process, Image Commun 2021;98:116418.
[34] Gan Z, Bi J, Ding W, Chai X. Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption. Neural Comput Appl 2021;33:12845–67.
[35] Setyaningsih E, Wardoyo R, Sari AK. Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. Digit Commun Netw 2020;6(4):486–503.

Monu Singh is currently pursuing her Ph.D. (Part-Time) in CSE from NIT, Patna. She has completed her M.Tech (2012) and B.Tech (2008) in CSE with first division. Her areas of interest are image processing, cryptography and deep Learning. She has published good research papers in reputed journals like Multimedia Tools and Application, IEEE Transactions on Consumer Electronics etc. in these areas. Contact her at monus.phd20.cs@nitp.ac.in.

Naman Baranwal has done his B.Tech from AKTU Lucknow and currently pursuing Ph.D. in Computer Science and Engineering from IIT Kanpur. His research interest includes Image processing and Deep learning. Contact him at namanbaranwal2002@gmail.com.

Kedar Nath Singh is currently working as Assistant Professor in the Computer Science & Engineering and Information Technology Department, JIIT, Noida. He has done his Ph.D from NIT Patna. He completed his M.Tech from AIACTR, New Delhi in 2011 and B.Tech from UPTU, Lucknow in 2008. His research interest includes Image Cryptography, Image processing and Multimedia security. Contact him at knsinghait@gmail.com.

Amit Kumar Singh is currently working as an Associate Professor in the Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India. He has authored over 200 peer-reviewed journal, conference publications, and book chapters. Dr. Singh has authored three books and edited eight books with internationally recognised publishers such Springer and Elsevier. Dr. Singh has been recognised as "WORLD RANKING OF TOP 2% SCIENTISTS" in the area of "Biomedical Research" (for Year 2020) and "Artificial Intelligence & Image Processing" (for Year 2021, 2022 and 2023), according to the survey given by Stanford University, USA. Dr Singh is currently Associate Editor of IEEE Trans. On Multimedia, ACM Trans. Multimedia Comput. Commun. Appl., IEEE Trans. Computat. Social Syst., IEEE Trans. Ind. Informat., IEEE J. Biomed. Heal. Informatics, Eng. Appl. Artif. Intell., Elsevier, IEEE Technology Policy and Ethics Newsletter etc. He is the series editor of The IET International Book Series on Multimedia Information Processing and Security. His research interests include multimedia data hiding, image processing, biometrics, & cryptography. Contact him at amit.singh@nitp.ac.in.

Huiyu Zhou is a full Professor at the School of Computing and Mathematical Sciences, University of Leicester, United Kingdoms. His research has been or is supported by UK EPSRC, MRC, EU ICT, Royal Society, Innovate UK, Leverhulme Trust, Invest NI, Puffin Trust, Alzheimer Research (UK) and the industry. He is Editor-in-Chief of Recent Advances in Electrical & Electronic Engineering, Associate Editor of IEEE Transactions on Human–Machine Systems, IEEE Journal of Biomedical and Health Informatics, Pattern Recognition, Peer Computer Science and IEEE Access, and Associate Editor of ICRA as well as Area Chair of BMVC and IJCAI. He holds a Doctor of Philosophy Degree in Computer Vision from Heriot-Watt University, Edinburgh, UK. Contact him at hz143@leicester.ac.uk.