International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18 (2026) pp. 1-16

Cerebration Science Publishing

https://doi.org/10.70917/ijcisim-2026-1959
Article

A Secure Digital Image Encryption Using Hybrid Transformation method with DNA Algorithm

Anusree L, M. Abdul Rahiman
F. A. Author is Research Scholar in APJ Abdul Kalam Technological University, Kerala 695016, Indiaand Assistant Professor in LBS College of Engineering, Kerala 671542, India
(email:anusree198@outlook.com)
S. B. Author is Research Supervisor in APJ Abdul Kalam Technological University, Kerala 695016, India andDirector, LBSCST, Kerala 695033, India

Abstract: Due to multiple assaults, securing digital images during transmission and storage is important to maintain data security. Various cryptography techniques have been employed in the past to increase the security of digital images. However, due to significant redundancy and strong correlation between neighboring pixels, conventional encryption algorithms have trouble improving the security level of images. Transform-based encryption approaches are used to secure medical images to deal with these issues. However, traditional wavelet and Fourier transform-based encryption have difficulty maintaining data after processing. The Shearlet transform Integrated Deoxyribonucleic Acid (DNA) method is proposed in this current study to protect medical images with reduced information loss. The supplied image is first transformed into a grayscale image. The input images are then decomposed into 41 sub-images using the Shearlet transform. Following that, this decomposed sub-picture is scrambled using the Generalized Arnold Transform and circularly shifted utilizing Intra-Inter bit level pixel permutation. The deconstructed sub-pictures are assembled using the vector decomposition process into a synthesized image. The final cypher image is then created using the DNA technique. The Chaos algorithm produces the key required for encryption using the DNA method. Finally, the cypher image is created by feeding the result of the DNA method through the gyrator transform. The reverse encryption method is used to recover the original image. This work achieves 0.99 correlation coefficient (CC), 56.75 Peak signal-to-noise ratio (PSNR), 0.0056 mean-square error (MSE), 0.99 Structural Similarity Index Metrics(SSIM), 0.015 Mean Absolute Error (MAE), 0.056 of Root Mean Square Error (RMSE).98.65 of the number of pixels change rate (NPCR) and 32.95 of unified average changing Intensity (UACI). According to experimental data, the algorithm has good robustness and security.

Keywords: Chaos algorithm, DNA method, Fourier Transform, Generalized Arnold Transform, Vector Decomposition, Wavelet Transform

1. Introduction

The diagnostic pictures are extensively saved and sent for various reasons, including featureselection, segmentation, image denoising, data hiding, and compression. In addition, medical photographs are often disseminated over the internet or the hospital intranet, together with a significant amount of personal information relating to patients' privacy. However, the hospital'sintranet has no substantial security measures, andthe internet has severe problems, such asunauthorised manipulation and the disclosure of privateinformation. The use of encryption on medical photographs isan efficient method for protecting these images from potential dangers [1].

As a consequence of this adaptability, weighted Fuzzy C-Means (FCM) segmentation is highly versatile and finds applications in various real-time scenarios, especially in protecting data transmitted through wireless networks. However, one drawback of selective encryption algorithms is the potential loss of data during their

application. Therefore, recent efforts have focused on developing effective transform-based encryption algorithms to minimize information loss in medical images. Various transform-based encryption algorithms, including Wavelet, Fourier, Curvelet, and Contourlet, have been devised to enhance the security of images [2]. These efforts have shifted towards the development of chaos-based symmetric cryptosystem algorithms for both general and medical image encryption.Symmetric encryption techniques involve employing chaotic models such as the Lorenz and Chen systems, the skew tent map, and the logistic map. Jovita introduced a method utilizing a cryptosystem to secure medical images.In this approach, a discrete wavelet transform is initially used to segment the medical image into different planes. These planes may utilize the same or different thresholds as those used for generating edge maps, but the resulting binary images maintain the same dimensions as the original planes. Subsequently, an XOR diffusion operation is conducted between the planes and the edge maps to complete the encryption process. Finally, the positional information of the planes obtained in the previous stage is scrambled, and the encrypted image is constructed by linking together the planes used in its construction [3].

For safeguarding medical images, a robust cryptographic method was proposed. The key generation process relied on a Pseudorandom Number Generator (PRNG) derived from a chaotic four-dimensional system. Subsequently, the initial medical image encryption employed a diffusion-confusion algorithm as its structural foundation. In this scheme, a simple replacement S-box facilitated the confusion attribute, while the diffusion property was achieved through XOR operations, wherein each pixel of the image was combined with a key stream. This encryption method was based on a straightforward chaotic system, ensuring the security of the medical data.[4].

The goal of improving the safety of medical pictures cannot be accomplished with a transform-based method alone. Researchers have recently discovered that DNA computing offers several benefits, including high storage density, low energy consumption, and wide-scale parallelism. The Shearlet transform-DNA excels in managing complex decision surfaces and handling multiple interactions between parameters. It boasts reduced processing time and offers flexibility in dealing with nonlinear shapes, addressing a wide array of challenges without the need for additional concatenation[5].

The main contributions of this work are

a) The shearlet transform can be used to extract images into the matrix.
b) Gyrator transforms and DNA algorithm combinations can be used to secure the image more.
c) The proposed method is ideal for use in sensors with little computing power since it has strong compressibility and great security while maintaining picture quality, and the encryption step uses fewer computer resources than current methods.

The remaining part of the manuscript is arranged as follows, Section 2 is based on several existing articles related to improving the security of medical images. In addition to it, the drawbacks found in the existing medical image encryption approaches are also discussed. Section 3 provides the schematic representation of the proposed architecture along with its basic concept. Following that, Section 4 illustrates the result obtained in the proposed medical image techniques. Finally, section 5 concludes the entire research work.

2. Literature Survey

Zhongyun proposed a novel encryption method for safeguarding medical images. It demonstrated resilience against impulse noise and data loss, achieved through the addition of random data to the image's surroundings followed by iterations of high-speed scrambling and pixel adaptive diffusion. While effective for various image formats, this method offers security through bitwise XOR and modulo arithmetic operations, ensuring protection against conventional encryption schemes [6]. Sha-Sha Yu et al. introduced an encryption method combining Integer Wavelet Transform (IWT) with DNA and chaos to protect digital medical photographs during transmission over public networks. Their method involved two stages: initial block shuffling followed by row and column pixel shuffling, providing reliable data protection against potential threats to electronic health records [7].

Guanghui Ren et al. proposed a method using chaotic maps on fractional Discrete Cosine Transform (FrDCT) coefficients to secure medical data, crucial amid the increasing need for high-speed networking and the exchange of medical images over public networks. Their method, utilizing FrDCT, offers flexibility in medical image encryption to prevent falsification and fraud [8]. Gaurav Verma et al. presented DICOM image encryption based on chaotic attractors and DNA sequences, using Integer Wavelet Transform (IWT) for spatial domain encryption. Their approach, leveraging chaotic three-dimensional Lorenz attractors and logistic maps, ensures data security in electronic healthcare, despite the time-consuming encryption process compared to textual data [9]. R. Kumar and C. Quan analyzed medical color image encryption employing Spiral Phase

Transform (SPT) and chaotic pixel scrambling. They modulated each color channel individually using structured phase masks and additional processing with MSPF. However, their method may be susceptible to unique iterative phase retrieval attacks, potentially compromising encrypted information [10].

The key objectives of the proposed method are given below.

a. Shearlet transform integrated DNA cryptography is proposed to increase the security of medical images.

b. Scrambling is done for each sub-image using the generalized Arnold transform and circular shifting is done using Intra-Inter bit level pixel permutation.

c. A vector decomposition method is used to connect the sub-group images into a synthesized image.

d. The result of the DNA method is then fed into the gyrator transform to produce a secure medical image.

3. Proposed Hybrid Transform With Dna Algorithm For Digital Image Encryption

The proposed method begins by converting the raw input image into a matrix format, which serves as the basis for subsequent operations. This 2D image matrix undergoes shearlet transformation, dividing it into 41 distinct sub-images. Each sub-image's pixel positions are then shuffled using a scrambling technique. After shuffling, circular shifting is applied to rearrange the pixels into rows and columns. Subsequently, a synthesis process amalgamates these shifted sub-images into a cohesive single image. In the decryption phase, novel approaches involving DNA are suggested for encoding and decoding, known as ST-DNA. Here, the reverse encryption method is employed to regenerate the original image from its encrypted form. The cypher picture resulting from the gyrator transform is converted into a synthetic image through a reversed DNA approach. Following this, the synthesized image is reverted to the original input image using the shearlet transform, effectively reversing the shifting and shuffling procedures.

A. Image Encryption Process

The raw input image has several pixels that are transformed into a matrix form at first. The 2D image matrix value is used for further processing. The matrix value is sent into the shearlet transform, which divides the matrix into 41 sub-images. Then, using a scrambling method, each sub-pixel image's position isshuffled. The shuffled result is then shifted using circular shifting to divide the pixels into rows and columns. The synthesis method is now used to connect the sub-images obtained after the circular shifting into a single image. Figure.1. shows the architecture of the encryption framework in the proposed Model.

1) Shearlet Transform

The Shearlet Transform (SHT) was devised to analyze images in a manner mirroring the human optical system, capturing all image attributes, particularly edges, faithfully. Shearlet is a multiscale extension of the classic wavelet transform that was successfully created to identify one-dimensional (1-D) and two-dimensional (2-D) directional features in pictures. Shearlet was named after the shear plane, which is a kind of shear plane. In contrast to its ancestors, such as the curvelet, which defined the direction by rotating the curve, the shearlet defines the direction by shearing the matrices that make up the shearlet. This not only makes the discrete implementation of shearlets simpler but also makes shearlets rotation-invariant [11].

The notion approximations of sparse shearlet, the shearlet analysis, parabolic scaling, and shearing have all been used to demonstrate theoretically that the qualities exist.

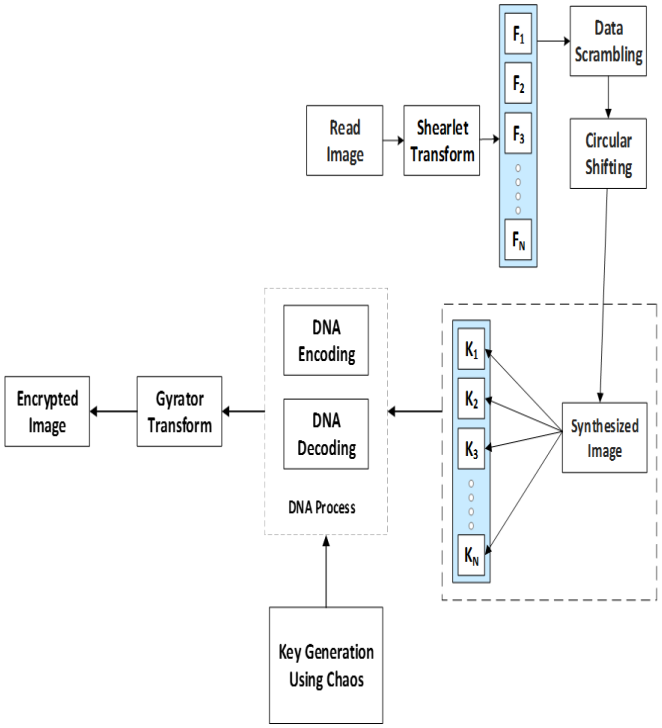


Figure 1. Architecture of the Encryption Framework in Proposed Model

The use of the parabolic scaling matrices in the creation of continuous shearlet systems has been suggested $B_b = \begin{bmatrix} b & 0 \\ 0 & \sqrt{b} \end{bmatrix}$ for b > 0. $S_S = \begin{bmatrix} 1 & S \\ 0 & 1 \end{bmatrix}$ for s ∈ ℝ. The matrices B_b and S_S represent the dilation and geometrical transforms.

Let $\psi_1 \epsilon L^2(\mathbb{R})$ be the discrete condition of the Calderon function, i.e.

$$\sum_{i\epsilon\, Z} |\hat{\psi}_1(2 - \hat{\psi}_1{}^{i}£)|^2 = 1, £ \epsilon R \quad (1)$$

Where $\hat{\psi}_1$ represented a Fourier transform of $\hat{\psi}_1$. Through $\hat{\psi}_1 \epsilon C^{\infty}(\mathbb{R})$, suppose $\hat{\psi}_1 \subseteq [-1/2, -1/16] \cup [1/16, 1/2]$. Furthermore, let $\psi_2 \epsilon L^2(\mathbb{R})$ be like $\hat{\psi}_2 \epsilon C^{\infty}(\mathbb{R})$, suppose $\hat{\psi}_2 \subseteq [-1, 1]$, then:

$$\sum_{j\epsilon\, \mathbb{Z}} |\hat{\psi}_2\,(£ + j)|^2 = 1, £ \in \mathbb{R} \quad (2)$$

Select $\hat{\psi}_2$ to be a function of smooth then

The SH (ψ) represents a classical shearlet constituted for $L^2(\mathbb{R})$ a Parseval frame that involves band-limited functions [12].

For an image $imge$, the shearlet transform is mapping by: $imge \rightarrow SH_{\psi} imge\ (scale > 0, orientation > Z, location > x)$(3)

The discrete shearlet system's associated mother function is one of its defining qualities $\psi = L\,2(\mathbb{R})$.

2) Scrambling Algorithm

Based on this generalized Arnold transform the location of the sub-image is shuffled. Along with that the position and value of the pixel in the sub image is also shuffled. Scramble the sub-images or the placements of the pixels using a randomization method. The matrix-pixel sequence is scrambled by the Arnold transform (ART) via the encoding of a single parameter. This results in a picture that resembles colour noise and decreases the key space required for storage and transmission applications [13].

The discrete shearlet system's associated mother function is one of its defining qualities in Eq (6).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1\lambda & \\ \mu 1 + & \lambda\mu \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ 1) \quad (4)$$

Where (x', y') indicates the new location after GAT has shuffled the data; the numbers that are positive $\lambda > 0, \mu > 0$; mod signifies the modulus after division. The scrambled sub-images are further sent for the circular shifting process. ART is used for the processing of two-dimensional images since it is chaotic in unit squares

and exhibits pseudo-numeration quality. The picture is scrambled by using ART for an iterative number of n, and the scrambled image may be recovered by employing inverse ART for an iterative number of m. Therefore, the iterative number in addition to the periodic scrambling transform p are both necessary to decode the original picture.

3) Circular Shifting

The process of reorganising the items in a tuple is referred to as the circular shift operation. This may be accomplished in one of two ways: either by moving the last element to the first place and shifting all of the other entries to the next position or by performing the opposite procedure. Circular shifts are a kind of cyclic permutations, which are themselves a subtype of permutations [14]. Circular shifts are also a subtype of permutations. To permute bit sequences, circular shifts are a common cryptographic operation that isutilised. Users need to perform the necessary calculations to determine the number of ones present in each row or column before completing the circular shifting procedure. The permutation is speculated to occur exclusively at the pixel level, hence referred to as intra-pixel bit-level permutation. This happens when the value of one is a multiple of 16, representing the number of bits stored within a pixel. If the value cannot be divided by 16, the permutation is carried out on a bit-by-bit basis. Inter-pixel bit-level permutation [15] involves moving bits from one pixel to the subsequent pixel to create a new image. The pixel-level permutation is performed on the image when the value is a multiple of 16. During circular shifts, also known as rotations, the shifted-out bit at one end is used to calculate the new bit value to be inserted at the other end. This process occurs at both ends of the data transfer, referencing the shifted-out bit at the other end. Circular shifts are commonly used in cryptographic applications, especially when preserving all bit values is crucial indicated in Figure. 2.

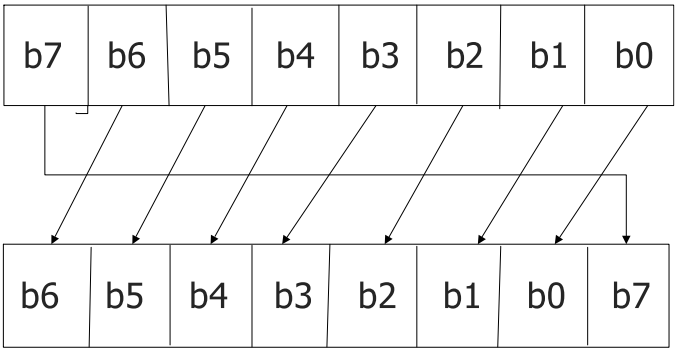


Figure 1. Circular shifting

4) Synthesized Algorithm

This synthesized algorithm combines the sub-images obtained after circular shifting into a single image [16]. The method for vector decomposition can accomplish multiple vector synthesis by only iteratively carrying out the parallelogram rule, as seen in Figure 3. It is possible to create a single vector by combining the sub-images, which may then be utilized as individual unit vectors. Create a single picture out of the individual photos that have been moved and mixed. Firstly, $f'_1(x_1, y_1)$ and $f'_2(x_1, y_1)$ are synthesized into vector $V_1(x_1, y_1)$: Synthesizedimage is calculated using Eq. (5 and 6),

$$V_1(x_1, y_1) = f'_1(x_1, y_1) + f'_2(x_1, y_1) = A_1 exp(i.\varphi_1) \quad (5)$$

Where A_1 and $\varphi_1$denote individually the amplitude and phase of the complex number$V_1(x_1, y_1)$. The phrase$\theta_1 = f_2 - \varphi_1$. Secondly, the synthesized vector$V_1(x_1, y_1)$ and $f'_3(x_1, y_1)$ are synthesised into vector$V_2(x_1, y_1)$:

$$V_2(x_1, y_1) = V_1(x_1, y_1) + f'_B(x_1, y_1) = A_2 exp \quad (6)$$

Where A_2 and $\varphi_2$denote individually the amplitude and phase of the complex number$V_2(x_1, y_1)$. The phrase$\theta_2 = f_3 - \varphi_2$. This process is repeated until all of the scrambled sub-images have been combined into a single vector$V_{n-1}(x_1, y_1)$. Take the last synthesized vector asf''.

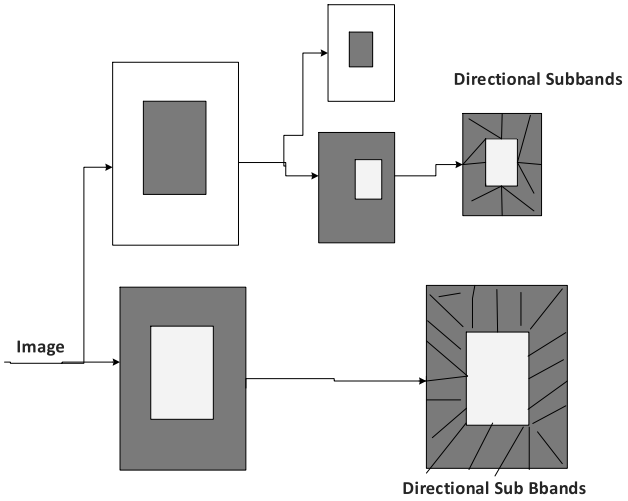


Figure 2. Gyrator transform Forward transform

5) Key Generation using Chaos Algorithm

To create the pseudorandom key sets required to activate the encryption process, 1-D logistic and sine chaotic maps are used [17].The equations for the logistic map and the sine map are included, respectively, in Eq. 7 and 8.

$$K(i+1) = \mu \times K(i) \times \big(1 - K(i)\big) \tag{7}$$

Where$\mu$the control parameter, along with its initial value ranges of

The sine map performs chaotically when the control parameter λ prevails in the range. To obtain a non-uniform chaotic sequence $K = 0.3, \lambda = 3, Y = 0.3$can be selected.

$$Y(i) = \lambda sin\big(\pi \times Y(i-1)\big) \tag{8}$$

6) DNA Cryptography

An initial test of DNA-based cryptography employed a substitution method. This method involved libraries of distinct one-time pads, each defining a specific randomly generated pair-wise mapping. Additionally, a molecular XOR scheme and indexed random key strings were utilized to encrypt a DNA sequence addition-based image encryption algorithm. These methods were used in conjunction with each other to generate a specific, randomly generated pair-wise mapping [18]. DNA-based cryptography was put to the test for the very first time. A DNA sequence matrix's production results from encoding the initial image. This matrix is then divided into several equal blocks before being combined with the assistance of two logistic maps: DNA complementarity and DNA sequence addition operation. Deciphering the DNA sequence matrix will lead to the discovery of the encrypted picture. "DNA cryptography" refers to the process of using DNA to secure information, and it is an efficient method for accomplishing this goal. The process in question can be described as follows: By utilizing an alphabet of oligonucleotide sequences, the plaintext message data is encoded in DNA strands using these methods. Message data can then be read. It is common practice to represent the sequences of oligonucleotides using the alphabet. Recoding natural DNA obtained from biological sources with nonstandard base pairings enables subsequent processing steps to be carried out. A laboratory is an ideal environment in which to carry this out. DNA chip arrays make it possible to transfer the input and output of DNA data to a conventional binary storage medium [19]. A method by which binary data can be stored in DNA strands through the utilization of an alphabet made up of brief sequences of oligonucleotides as building blocks. DNA is a part of the genetic code that is made up of two strands that form a structure known as a double helix when wound around each other. This structure is what gives DNA its double-helix shape [20]. The values 0 and 1 are reciprocal to one another in a system that employs binary digits; similarly, the values 00, 11, 01, and 10 are similar [21-22]. In a system that utilizes decimal digits, the values 0 and 1 are reciprocal.

7) Gyrator Transform

Gyrator Transform (GT) is introduced for medical processing. For a two-dimensional function(x,y), the GT can be represented as:

$$f(u,v) = G^{\alpha}[f(x,y)] = 1/|\sin\alpha| \int\int f(x,y)\, exp\big[i2\pi\big((xy+uv)cos\alpha - (xv+yu)\big)/sin\alpha\big]\, dxdy$$

(9)

where α denotes the angle of rotation of the GT. (x, y) are the input plane coordinates and (u, v) are the coordinates of the output plane. Designed for inverse GT, the rotation angle $' - \alpha'$. For α= 0, it defined the identity transform. For $\alpha = \pi/2$, it behaves like the direct Fourier Transform (FT), and $\alpha = 3\pi/2$ will give the inverse FT with the rotation of the coordinate at $\pi/2$ [23].

Encryption, space-variant filtering, and hyperbolic noise reduction are some of the applications of the GT. In addition, the GT is the same as the movement of the orbital Poincare spheres along the main meridian, which was introduced by analogy to the polarization Poincare sphere. The Hermite–Gaussian (HG) modes may be produced from the integral canonical transforms. The GT can be considered a universal mode converter because it enables the production of all fundamentally distinct structurally stable Gaussian modes. An optical setup capable of conducting this operation for various parameters to employ the GT for optical information processing [24]. Figure 4. Shows the gyrator transform.

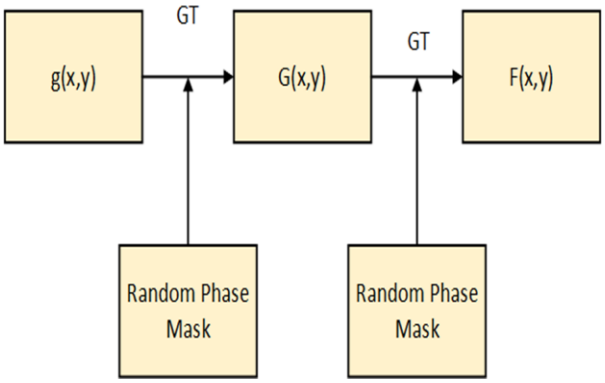


Figure 4. Gyrator transform

B. Image Decryption Process

The suggested approaches include the use of DNA in the encoding and decoding of ST-DNA. In this step of decryption, the reverse encryption method is used to GT the original picture. The stored cypher picture of the gyrator transform is then turned into a synthetic image using the reversed DNA approach. Following that, the synthesized picture is turned back

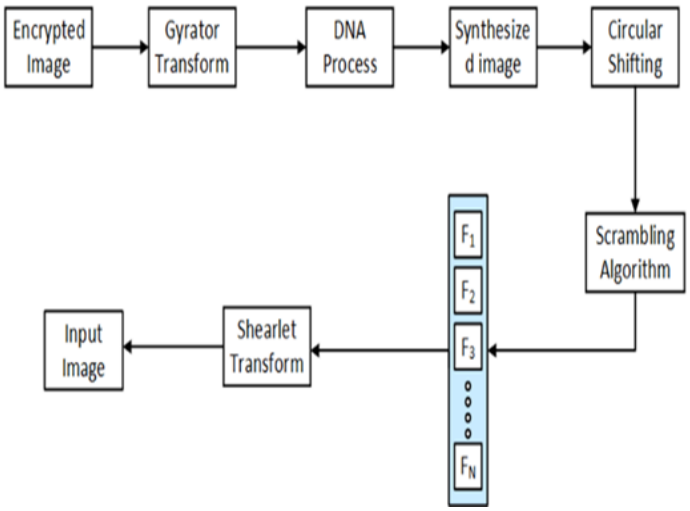


Figure 5. Block Diagram of Decryption Process

into the original input image using the shearlet transform to reverse the shifting and shuffling processes. Figure.5. shows the block diagram of the decryption process.

4. Results And Discussions

Shearlet Transform-DNA was proposed in this present researchto improve medical image security. The Shearlet Transform is applied to medical images. This involves decomposing the images into a set of shearlet coefficients, which capture various features and details in the images at different scales and orientations. The testing process likely involved taking a set of images and applying the Shearlet Transform-DNA method to them using MATLAB 2021a with CPU: Intel core i5, GPU: NVidia GeForce GTX 1650, RAM: 16GB.

A. Dataset

The pepper image was taken from [25]. It is a grey image with a size of 256x256. Thefranjipani image is grey and has been resized to 256x256.The grayscale of penguins and is sized 256x256. The grey image of the art of trees; its dimension is 536 × 371.

B. PSNR

The peak signal-to-noise ratio, or PSNR, is the ratio of the signal's greatest possible intensity to the input power when it is distorted [26]. PSNR is expressed as Eq. (10).

$$SNR = 20.\log_{10} MAX_{PY} - 10.\log_{10} MSE \tag{10}$$

Where MAX_{PY} defined an image pixel value maximum.

C. Correlation Coefficient (CC)

The correlation coefficient (CC) graphs a statistical connection between two variables [27] as seen in Eq. (11).

$$CC(K,k) = \frac{M\{[K-M(K)][k-M(k)]\}}{M\{[K-M(K)]^2\}M\{[k-M(k)]^2\}} \tag{11}$$

Here K and k represent the plain image and decrypted image.

D. SSIM

SSIM is a viewpoint paradigm that views the loss of an image as a perceived change in the structure of the picture, and it often integrates fundamental visual effects, such as the intensity of light masking and intensity masking notions shown in Eq. (12).

$$SSIM(i,j) = \frac{(2k_i k_j + r1)(2l_{xy} + r2)}{\left(k_i^2 + k_j^2 + r1\right)(l_i^2 + l_j^2 + r2)} \tag{12}$$

E. Mean Square Error (MSE)

The MSE is a measurement that determines how consistent an estimator is; it is typically positive, and numbers that are closer to zero are considered to be higher. The difference between the original and encrypted versions of the picture is reflected in the MSE, which is seen in Eq. (13).

$$MSE = \frac{1}{Px*Px}\sum_{i=1}^{Px}\sum_{j=1}^{Px} |\ \hat{I}(i,j) - I(i,j)|^2 \tag{13}$$

F. Root-Mean-Square Error (RMSE)

The standard deviation of the residuals may be computed with the help of the RMSE. The residuals are a statistic that indicates how distant the data points are from the regression line; it is denoted by Eq. (14).

$$RMSE = \sqrt{\overline{J - L}} \tag{14}$$

Where J is the expected value and L are known results

G. Mean Absolute Error (MAE)

The MAE is a statistical method for evaluating the amount of error contained in sets of data that are identically paired and reflect the same phenomena. In the equation, we see comparisons between anticipated future time against observed future time concerning the beginning time, as well as one measurement method about another.

$$MAE = \frac{\sum_{I=1}^{N} |Y_I - X_I|}{N} \tag{15}$$

H. Number of Pixels Change Rate (NPCR)

The more the NPCR approaches 100%, the more vulnerable the cryptosystem is to changes in plain image and the more effectively it can fend off attacks using plaintext.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{width \times height} \tag{16}$$

I. Unified Average Changing Intensity (UACI)

It is the degree to which the plain picture and the ciphered image differ on average. The more effectively the cryptosystem can withstand differential attack, the closer the UACI comes to 33.333...%.

$$UACI = \frac{1}{width \times height} \sum_{ij} \left[\frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \tag{17}$$

J. Standard Deviation (SD)

The standard deviation in statistics is a measure of the degree of variation or dispersion in a set of values.

$$s = \sqrt{\frac{1}{N-1} \quad \sum_{i=1}^{N} (x_i - \bar{x})^2} \tag{18}$$

K. Mean

The mean is the average of the supplied numbers and is computed by dividing the total number of numbers by the sum of the given numbers.

$$\bar{x} = \frac{1}{n} \quad \left(\sum_{i=1}^{n} x_i\right) = \frac{x_1 \quad + x_2 \quad + \cdots \quad + x_n}{n} \tag{19}$$

L. Entropy

Entropy measures the degree of uncertainty/ randomness of the message. The mathematical formula for calculating entropy is given by

$$H = -\sum_{1}^{255} P(i) \log_2 P(i)$$

P(i) represents the probability of the message occurrence. The message with higher entropy represents the higher randomness. The test image considered is 8-bit depth, so the cipher image entropy should be nearer to 8 to possess high randomness.

M. Cropping attack analysis

A cropping attack analysis is carried out to analyse the efficiency of the proposed encryption algorithm against intentional/unintentional data loss. In this analysis, the part of the cipher image is intentionally cropped, and the cropped cipher image is sent to the decryption module to retrieve the deciphered image. Cropping attack analysis is carried out for 10% (81 × 81), 30% (140 × 140), 50% (181 × 181), 64 × 64, 32 × 32 data loss as shown in Fig. 6. From Fig. 6, it can be seen that the decryption algorithm can get back the meaningful decrypted image with several data losses.

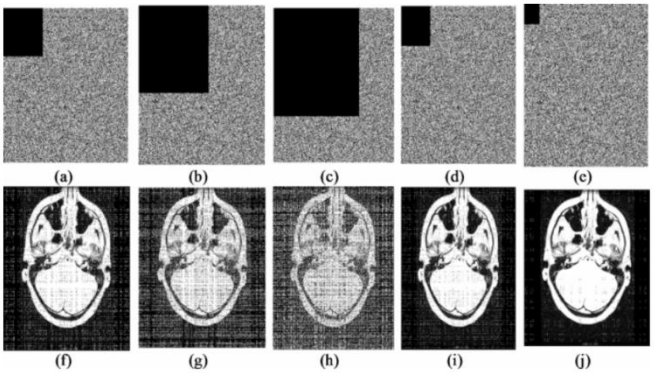


*Figure 6.Cropping attack analysis: (**a**) 10% cropped cipher image (81 × 81), (**b**) 30% cropped cipher image (140 × 140), (**c**) 50% cropped cipher image (181 × 181), (**d**) Cropped cipher image of size 64 × 64, (**e**) Cropped cipher image 32 × 32, (**f**) Deciphered image of (**a**), (**g**) Deciphered image of (**b**), (**h**) Deciphered image of (**c**), (**i**) Deciphered image of (**d**), (**j**) Deciphered image of (**e**).*

N. Noise attack analysis

To test the algorithm's efficacy against noise attacks, the cipher image is subjected to salt and pepper noise of various intensity levels. Salt and pepper noise is applied to the cipher image with varying intensity levels, such as 2%, 3%, 5%, 10% and 25%. The corresponding deciphered images are analysed, as shown in Figure 7.

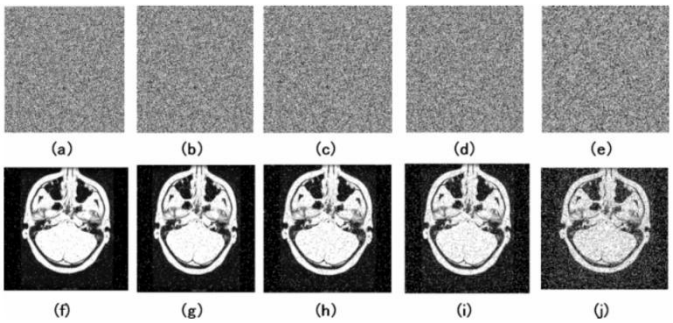


*Figure 7. Salt and pepper noise attack analysis: (**a**) Encrypted image with 2% noise, (**b**) Encrypted image with 3% noise, (**c**) Encrypted image with 5% noise, (**d**) Encrypted Image with 10% noise, (**e**) Encrypted Image with 25% noise, (**f**) Deciphered Image of (**a**), (**g**) Deciphered Image of (**b**), (**h**) Deciphered image of (**c**), (**i**) Deciphered image of (**d**), (**j**) Deciphered image of (**e**).*

Figure.8. shows the sample encrypted and decrypted images. Table 1. Demonstrates that the comparative performances of CC, PSNR, and MSE are much improved over earlier efforts. Compared to earlier techniques, this work has improved CC and PSNR while reducing MSE. Edge Map(EM) has 0.02 of CC, 46.25 of PSNR, 0.37 of MSE, 0.63 of SSIM, 0.67 of MAE, 0.076 of RMSE, Double Phase Encryption (DPE) gives 0.19 of CC, 49.29 of PSNR, 0.42 of MSE, 0.79 of SSIM, 0.49 of MAE, 0.145 of RMSE, Grayscale (GS) 0.64 of CC, 39.4 of PSNR, 0.076 of MSE, 0.83 of SSIM, 0.35 of MAE, 0.19 of RMSE, Computational Ghost Imaging (CGI), 0.46 of CC, 49.53 of PSNR, 0.035 of MSE, 0.73 of SSIM, 0.16 of MAE, 0.095 of RMSE. Finally, This work, 0.99 of CC, 56.75 of PSNR, 0.0046 of MSE, 0.98 of SSIM, 0.014 of MAE, and 0.052 of RMSE.Table 2 shows the entropy values for original and encrypted images for different images. Figure.9. shows the histogram analysis of the input plain image, encrypted image, and decrypted image.Figure.10. shows the performance of CC. Figure.11. depicts the performance of PSNR. Figure.12. shows the comparative performance of MSE, SSIM, MAE, and RMSE.Figure.13. shows the performance of PSNR based on noise attack.Table3. Shows the key sensitivity analysis.

Table-1 Comparative performances

Method	CC	PSNR	MSE	SSIM	MAE	RMSE	NPCR	UACI
EM [1]	0.0019	46.25	0.10	0.63	0.67	0.076	93.16	29.37
GI [3]	0.02	46.25	0.37	0.63	0.67	0.076	94.01	31.82
GS [11]	0.64	39.4	0.076	0.83	0.35	0.199	93.73	31.79
DPE [15]	0.19	49.29	0.42	0.79	0.49	0.145	97.94	31.05
CGI [18]	0.46	49.53	0.035	0.73	0.16	0.095	94.76	32.18
HCS[30]	0.49	48.9	0.031	0.75	0.167	0.088	95.10	33.08
Chaos[29]	0.66	49.68	0.022	0.87	0.021	0.083	96.54	33.32
This work	0.99	56.75	0.0046	0.98	0.014	0.052	98.65	33.62

Table-2 Entropy values for original and encrypted images for different images

Image	Entropy	
	Original image	Encrypted image
Lena	7.426985	7.997620
Mandrill	7.242483	7.997126
Aerial	7.313656	7.997519
Earth	7.044457	7.997273
Pepper	7.577819	7.997282

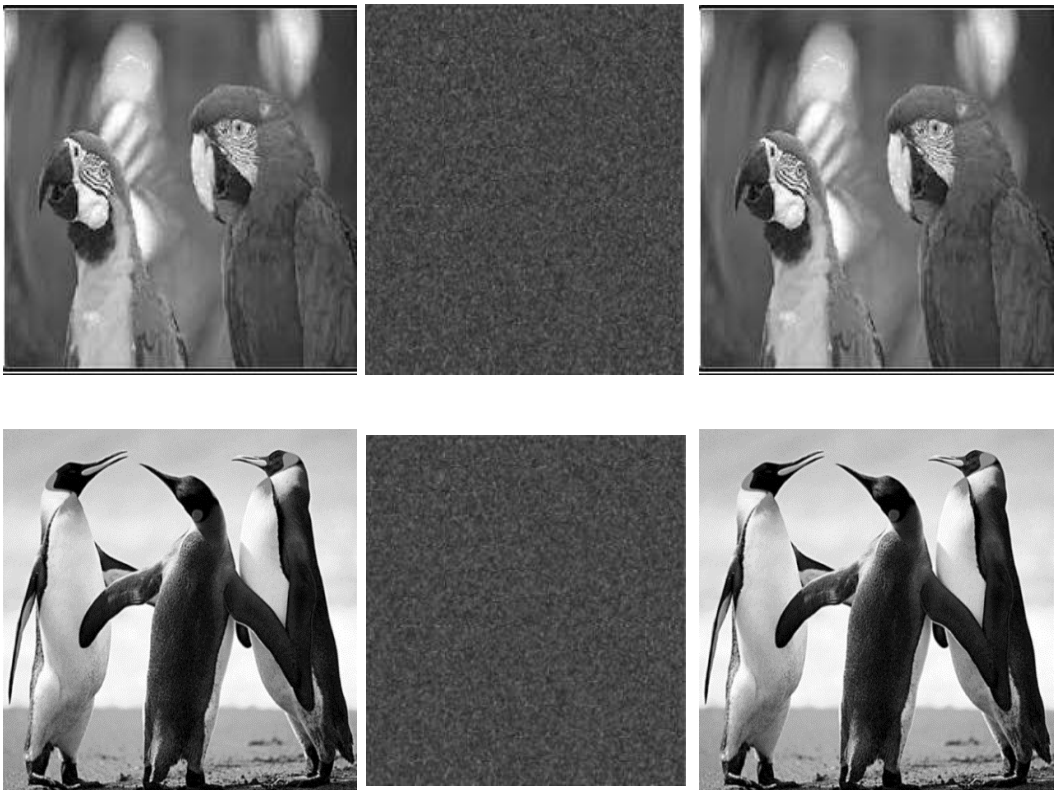
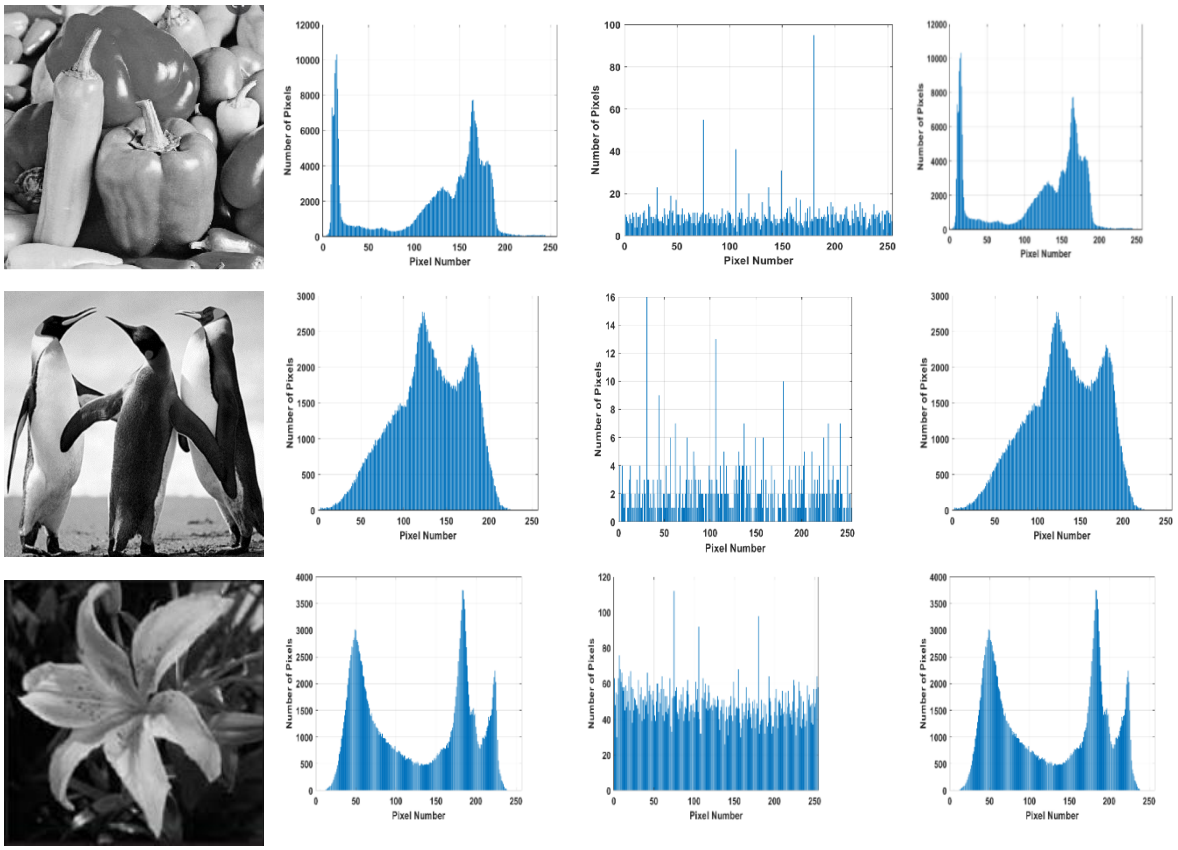


Figure 8.Sample Encrypted and Decrypted images (a) Plain image (b) Encrypted image (c) Decrypted image



(a) (b) (c) (d)

Figure 9. Histogram analysis(a) Plain image (b) Histogram of plain image (c) Histogram of Encrypted image (c) Histogram of Decrypted image

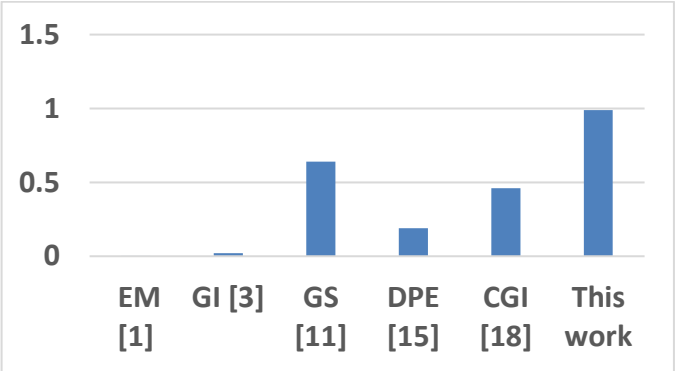


Figure 10. Performance of CC

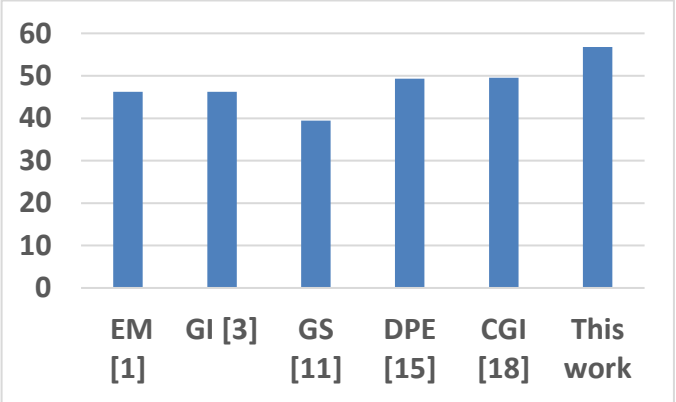


Figure 11. Performance of PSNR

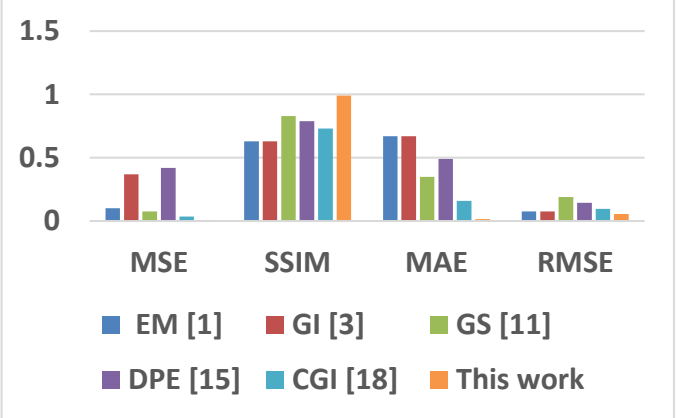


Figure 12.Comparative performance of MSE, SSIM, MAE and RMSE

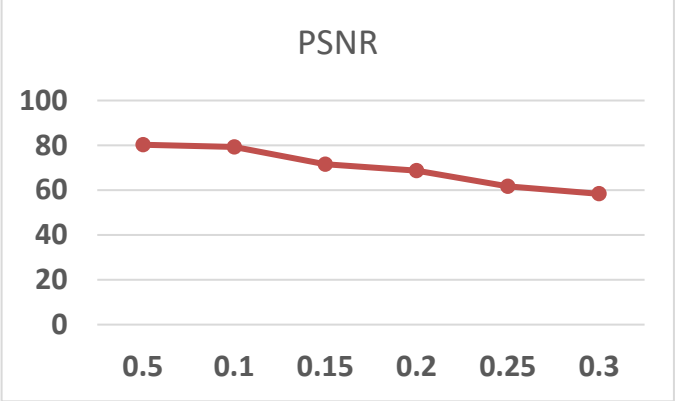


Figure 13.Performance of PSNR based on noise attack

Table 3. Key sensitivity analysis

Images	Key Sensitivity Analysis	CC	Standard deviation(SD)	Mean	MSE
	0.5	0.005	0.87	2.15	0.27
	0.9	0.010	0.79	8.21	0.55
	0.7	0.025	0.81	2.12	0.79
	0.6	0.0038	0.78	3.73	0.78

5. Conclusion

This work proposed a Shearlet transform incorporated DNA method to increase the security of images during transmission and storage. Along with strengthening security, the image's information content must be preserved after processing. First, the input medical image is transformed, and then DNA cryptography is performed to perform secure image encryption. The input image is initially broken into sub-images using the shearlet transform. After that, the shuffle and shift processes are performed using two different ways. Using the vector decomposition algorithm, the output of these processes is blended into a synthesized image. The DNA encoding and decoding process is carried out to produce the final encrypted image. Finally, the DNA process results are sent into the gyrator transform, which generates a cypher image. The proposed security model performs well in terms of the correlation coefficient, entropy, mutual information, standard deviation, and other metrics. The suggested ST DNA's performance was also validated and compared to existing approaches such as DWT, FT, FFT, FrFT, and DRPE. The proposed scheme's security may be mathematically demonstrated in the future. As a result of its high level of security, the suggested ST DNA will be widely adopted or regarded as a superior alternative to competing algorithms. This work gets 0.99 of CC, 56.75of PSNR, 0.0056 of MSE, 0.99 of SSIM, 0.015 of MAE, and 0.056 of RMSE. 98.65 of NPCR, 32.95 of UACI. This work can be enhanced for color images in the future.

6. Limitations Of Work

Despite the advancements achieved in the proposed research on optical encryption, several limitations and challenges remain that warrant further investigation. The research primarily focuses on static image encryption. The application of these models for real-time video encryption and decryption is not explored, which is crucial for dynamic and time-sensitive applications.While the techniques are robust against common attacks, the impact of environmental distortions such as compression artifacts, blurring, or noise in the communication channel is not fully explored.

References

1. Cao, Weijia, Yicong Zhou, CL Philip Chen, and Liming Xia. "Medical image encryption using edge maps." Signal Processing 132 (2017): 96-109.
2. Akkasaligar, Prema T., and Sumangala Biradar. "Selective medical image encryption using DNA cryptography." Information Security Journal: A Global Perspective 29, no. 2 (2020): 91-101.
3. Zhang, Leihong, Xiao Yuan, Kaimin Wang, and Dawei Zhang. "Multiple-image encryption mechanism based on ghost imaging and public key cryptography." IEEE Photonics Journal 11, no. 4 (2019): 1-14.
4. Chen, M., Ma, G., Tang, C., & Lei, Z. (2020). Generalized optical encryption framework based on Shearlets for medical image. Optics and Lasers in Engineering, 128, 106026.
5. Pavithran, P., Mathew, S., Namasudra, S., & Lorenz, P. (2021). A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine. Computers & Security, 104, 102160.
6. Hua, Zhongyun, Shuang Yi, and Yicong Zhou. "Medical image encryption using high-speed scrambling and pixel adaptive diffusion." Signal Processing 144 (2018): 134-144.
7. Ravichandran, D., Banu S, A., Murthy, B. K., Balasubramanian, V., Fathima, S., &Amirtharajan, R. (2021). An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. Medical & Biological Engineering & Computing, 59(3), 589-605.
8. Kumar, S., Panna, B., & Jha, R. K. (2019). Medical image encryption using fractional discrete cosine transform with chaotic function. Medical & biological engineering & computing, 57(11), 2517-2533.
9. Banu S, A., & Amirtharajan, R. (2020). A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Medical & Biological Engineering& Computing, 58(7), 1445-1458.
10. 10. Kumar, R., & Quan, C. (2019). Optical colour image encryption using spiral phase transform and chaotic pixel scrambling. Journal of modern optics, 66(7), 776-785.
11. Chuman, Tatsuya, WaritSirichotedumrong, and Hitoshi Kiya. "Encryption-then-compression systems using grayscale-based image encryption for jpeg images." IEEE Transactions on Information Forensics and security 14, no. 6 (2018): 1515-1525.
12. Jiao, Kaixin, Guodong Ye, Youxia Dong, Xiaoling Huang, and Jianqing He. "Image encryption scheme based on a generalized arnold map and rsa algorithm." Security and Communication Networks 2020 (2020).
13. Zhou, Nanrun, Yiqun Hu, Lihua Gong, and Guangyong Li. "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations." Quantum Information Processing 16, no. 6 (2017): 1-23.
14. Yao, Lili, Caojin Yuan, Junjie Qiang, Shaotong Feng, and Shouping Nie. "An asymmetric color image encryption method by using deduced gyrator transform." Optics and Lasers in Engineering 89 (2017): 72-79.
15. Zamrani, Wiam, Esmail Ahouzi, Nawfel Azami, Hassan El Ghazi, and Tayeb Sadiki. "Optical double phase encryption and spreading method applied to color image." In 2016 15th Workshop on Information Optics (WIO), pp. 1-3. IEEE, 2016.
16. Akkasaligar, Prema T., and Sumangala Biradar. "Selective medical image encryption using DNA cryptography." Information Security Journal: A Global Perspective 29, no. 2 (2020): 91-101.
17. Setyaningsih, Emy, Retantyo Wardoyo, and Anny Kartika Sari. "New Compression-Encryption Algorithm Using Chaos-Based Dynamic Session Key." International Journal on Smart Sensing & Intelligent Systems 11, no. 1 (2018).
18. Wang, Le, Shengmei Zhao, Weiwen Cheng, Longyan Gong, and Hanwu Chen. "Optical image hiding based on computational ghost imaging." Optics Communications 366 (2016): 314-320.
19. 19. Hou, Junfeng, and Guohai Situ. "Image encryption using spatial nonlinear optics." eLight 2, no. 1 (2022): 1-10.
20. 20. Chen, Linfei, Lei Chen, and Haidan Mao. "Double optical image encryption system based on near-field Fourier ptychography." Journal of Modern Optics (2022): 1-10.
21. 21. Masood, Fawad, WadiiBoulila, Jawad Ahmad, Syam Sankar, Saeed Rubaiee, and William J. Buchanan. "A novel privacy method of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos." Remote Sensing 12, no. 11 (2020): 1893.
22. Masood, Fawad, Junaid Masood, Lejun Zhang, Sajjad Shaukat Jamal, Wadii Boulila, Sadaqat Ur Rehman, Fadia Ali Khan, and Jawad Ahmad. "A new color image encryption method using DNA computing and Chaos-based substitution box." Soft Computing 26, no. 16 (2022): 7461-7477.
23. Zhang, Qinnan, and Jiaosheng Li. "Single Exposure Phase-Only Optical Image Encryption and Hiding Method via Deep Learning." IEEE Photonics Journal 14, no. 1 (2022): 1-8.

24. Yu, Xuelian, Hao Chen, Junjun Xiao, Yanqian Sun, Xiufang Li, and Kangwei Wang. "Incoherent optical image encryption based on coded aperture correlation holography." Optics Communications (2022): 127889.

25. https://www.facweb.iitkgp.ac.in/~shamik/spring2008/sca/tutorial/download/pami.uwaterloo.ca/tizhoosh/images/test12.jpg

26. Buchanan, J. G.; Sable, H. Z. In Selective Organic Transformations; Thyagarajan, B. S., Ed.; Wiley-Interscience: New York, 1972; Vol. 2, pp 1–95.

27. Inoue, Kotaro, and Myungjin Cho. "Amplitude based keyless optical encryption system using deep neural network." Journal of Visual Communication and Image Representation 79 (2021): 103251

28. Ravichandran, Dhivya, W. Sylvia Lilly Jebarani, Hemalatha Mahalingam, Padmapriya Velupillai Meikandan, Padmapriya Pravinkumar, and Rengarajan Amirtharajan. "An efficient medical data encryption scheme using selective shuffling and inter-intra pixel diffusion IoT-enabled secure E-healthcare framework." *Scientific Reports* 15, no. 1 (2025): 4143.

29. Aashiq Banu, S., L. Koteswara Rao, P. Shanmuga Priya, Thanikaiselvan, M. Hemalatha, R. Dhivya, and Amirtharajan Rengarajan. "A Review of Genome to Chaos: Exploring DNA Dynamics in Security." *Multimedia Tools and Applications* (2024): 1-28.

30. Geng, Shengtao, Jiahao Li, Xuncai Zhang, and Yanfeng Wang. "An image encryption algorithm based on improved Hilbert curve scrambling and dynamic DNA coding." *Entropy* 25, no. 8 (2023): 1178.