5
A Novel Biometric Inspired Robust Security Framework For Medical Images

In previous chapters, two perceptual hashing techniques have been presented for image authentication and identification, which is essentially required for image security. However, the privacy and confidentiality protection is another important issue which may not covered by these techniques, therefore, a novel biometric inspired technique is developed in this chapter using image encryption specially designed for medical images.

The proposed technique is based on the biometrics characteristics, parameterized all phase bi-orthogonal sine transformation, SVD and QR decomposition. The salient contribution of this approach is to introduce an efficient key management system utilizing biometrics features of the patient. Further, a new transform, namely, parameterized all phase bi-orthogonal sine transformation (PR-APBST) is proposed and used for encryption purposes. In this work, fingerprint biometric is selected to acquaint key management system as it is one of the oldest and widely practised amongst all biometrics. The common advantages of fingerprint which make it a superior biometrics among all are as follows [Choi *et al.*, 2011; Maltoni *et al.*, 2009]:

- Fingerprint has excellent statistical properties among all biometrics.
- The fingerprint essentially represents the pattern consisting of dark lines of ridges and valley along with white lines on top of the finger. Due to variation in ridges pattern, it is unique for everyone and there are no fingers having same ridge pattern in the history of fingerprinting. Even genetically identical individuals don't have the same ridge patterns nor they shared by two fingers of the same person.
- Each fingerprint can be recognized using a set of special point usually called minutiae, which essentially describes the distinctive feature in the form of location and direction.
- Fingerprints are assumed to be ageless. The ridges are created prior to birth and remain even after death, until the skin decays. The ridges patterns are robust and are not affected by diseases. Diseases may only change skin color and texture but ridges are remarkably stable and immune. The overall quality of ridges remains unchanged throughout the life makes fingerprints a noble biometric.
- The collectivity and measurability of biometric has significantly important role in several applications. The fingerprint is easily measurable biometric when compared to other biometrics and therefore is ideal for several applications.

Nevertheless, other biometrics such as palm-print, iris, face, signatures can also be used in the proposed image encryption technique. The core idea is to capture the fingerprint of the patient and use it to generate a key generation management system, which essentially provides the keys to be used. These keys are the parameter involved in PR-APBST and the initial value for the chaotic map. The biometric image is first transformed into PR-APBST coefficients followed by singular value decomposition and QR decomposition to encrypt the medical image. The simulation results

demonstrate the efficiency of proposed medical image encryption through key-space, sensitivity, statistical and perceptual security analysis using different experimental images.

5.1 PARAMETERIZED ALL PHASE BIORTHOGONAL SINE TRANSFORM

All phase biorthogonal sine transform (APBST) can be derived from the discrete sine transform by employing the sequence filtering in time domain [Zhou *et al.*, 2017] in pursuit of getting good energy concentration and high-frequency attenuation characteristics. The complete process of defining APBST initiates considering discrete sine transform matrix, which can be defined mathematically as [Saxena and Fernandes, 2013]:

$$s(i,j) = \frac{2}{\sqrt{2N+1}} \sin \frac{(2i+1)(j+1)\pi}{(2N+1)}; \;\; i,j = 1,\ldots,N-1 \tag{5.1}$$

The digital filtering can now be performed using a digital sequence. Therefore, a digital sequence $r(n)$ has been employed for the filtering, where each point of $r(n)$ correspond to n different values. The estimated mean of these values assigned as the output of all phase filtering.

$$z(n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \Big[G(i,j) r(n-i+j) \Big] \tag{5.2}$$

where

$$G(i,j) = \frac{1}{N} \sum_{i=0}^{N-1} G_N(m) s(i,m) s(j,m) \tag{5.3}$$

substituting Eqn. (5.3) in to Eqn. (5.2), we have

$$z(n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \left[\sum_{i=\tau}^{N-1} H(i,i-\tau) r(n-\tau) \right] \tag{5.4}$$

$$\Rightarrow z(n) = \sum_{\tau=-(N-1)}^{N-1} h(\tau) r(n-\tau) = h(n) * r(n) \tag{5.5}$$

where $h(\tau)$ denote the unit impulse response in the form of all phase filtering and can be expressed as:

$$h(\tau) = \begin{cases} \sum_{i=\tau}^{N-1} H(i,i-\tau); & \tau = 0,1,\ldots,N-1 \\ \sum_{i=0}^{\tau+N-1} H(i,i-\tau); & \tau = -1,-2,\ldots,-N+1 \end{cases} \tag{5.6}$$

Also, $G(i,j) = G(j,i)$, then from Eqn. (5.3) and Eqn. (5.6)

$$h(\tau) = \sum_{m=0}^{N-1} U(\tau,m) F_N(m); \;\; \tau = 0,1,\ldots,N-1 \tag{5.7}$$

This can be expressed in the form of the matrices as: $h = VF$, V denotes a transition matrix which describes the relationship between the unit pulse time response in the time domain and sequence response in an orthogonal transform domain. The matrix V is known as all phase bi-orthogonal sine matrices and computed as:

$$V(\tau,m) = \frac{1}{N} \sum_{i=\tau}^{N-1} S(m,i) S(m,i-\tau) \tag{5.8}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1-\tau} S(m,i) S(m,i+\tau) \tag{5.9}$$

substituting $i \to l$, $m \to j$, $\tau \to i$

$$V(i,j) = \frac{1}{N} \sum_{i=\tau}^{N-1} S(j,l) S(j,l+i) \tag{5.10}$$

from Eqn. (5.1) and Eqn. (5.10), all phase bi-orthogonal sin transform matrix is obtained, which is given as follows.

$$V(i,j) = \begin{cases} \frac{1}{N} & i = 0, j = 0,1,\ldots,N-1 \\ \frac{4}{N(2N+1)} * \beta & i = 1,\ldots,N-1 \\ & j = 0,1,\ldots,N-1 \end{cases} \tag{5.11}$$

where

$$\beta = \sum_{l=0}^{N-1-i} \sin \frac{(2j+1)(l+1)\pi}{(2N+1)} \sin \frac{(2j+1)(l+i+1)\pi}{(2N+1)} \tag{5.12}$$

The transform matrix V can be used for forward decomposition while its inverse (V^{-1}) can be used to reconstruct the signal. The APBT provides an elegant tool for analysing different signals [Saxena and Fernandes, 2013]. In fact, it has the capability to analyze a signal better than the most common Fourier and discrete cosine transform especially in the image coding application [Zhou *et al.*, 2017]. However, it is not appropriate for the applications involving the security aspect. The main reason is that this transform does not have any parameter involved, which can play the vital role of the key. Therefore, APBT may be capable of analyzing different kind of signals efficiently but may not be used for the security purposes. To overcome this issue, a new definition is presented based on the simple recurrences of rotation matrix. The core idea is to introduce a parameter, which will act as the key for the transform because without knowing correct value of this parameter, one cannot get the accurate transform coefficients. In order to introduce advent in the definition of APBT, rotation matrix is examined first.

In linear algebra, a rotation matrix is used to transform the set of coordinates into the orthogonal cartesian frame preserving the shape and size, i.e, the angle between a pair of vectors and vector length remains unchanged. The main property of the rotation matrix is that it is an unimodular orthogonal matrix with real entries. Generally, a 2-D rotation matrix can be described as:

$$\mathscr{R}_2 = \frac{1}{c^2+d^2} \begin{bmatrix} c^2-d^2 & 2cd \\ -2cd & c^2-d^2 \end{bmatrix} \tag{5.13}$$

where c and d are arbitrary constants. The respective degree of freedom is one and Eqn. 5.13 can be normalized by considering c and d satisfying c^2+$d^2 = 1$, then there exist a constant ψ such that $c = \cos(\psi/2)$ and $d = \sin(\psi/2)$. Owing these values of c and d the rotation matrix can be written as

$$\mathscr{R}_2^{\psi} = \mathscr{R}_2 = \begin{bmatrix} \cos(\psi/2) & \sin(\psi/2) \\ -\sin(\psi/2) & \cos(\psi/2) \end{bmatrix} \tag{5.14}$$

Here ψ describes the angle between the original coordinate and rotated coordinate axis. In other words, the elements of rotation matrix describe the projection of rotated coordinates onto the original coordinate axis. The inverse of the rotation matrix is obtained by its transpose due to reciprocal relation, i.e, $(\mathscr{R}_2^{\psi})^{-1} = (\mathscr{R}_2^{\psi})^T$. Similarly, the rotation matrix $\mathscr{R}_3$ of order three can be described as

$$\mathscr{R}_3 = \frac{1}{T} \begin{bmatrix} c^2+d^2+e^2+f^2 & -2(cf-fe) & 2(ce+df) \\ 2(cf+fe) & c^2-d^2+e^2-f^2 & -2(cd-ef) \\ -2(ce-df) & 2(cd+ef) & c^2-d^2-e^2+f^2 \end{bmatrix} \tag{5.15}$$

where $T = c^2 + d^2 + e^2 + f^2$ for some constants c, d, e and f. The degree of freedom for this matrix is three and can be normalized by the relation $c^2 + d^2 + e^2 + f^2 = 1$. The relationship among these constants are complicated and can be obtained by incorporating rotation matrix of order two. In principle, c can be assumed as $c = \cos(\theta/2)$ and other parameters can be obtained by the relation $d^2 + e^2 + f^2 = \sin(\theta/2)$. It can be observed that the set of rotation matrices are closed under multiplication and it follows that any reorientation in space can be expressed in terms of pure rotation about some fixed axis. On the other hand, if the rotation axis coincides with one of the coordinates axes, then the rotation matrix degenerates to essentially a 2-D rotation. Therefore, the parameters can have the values $e = f = 0$, $c = \cos(\theta/2)$ and $d = sin(\theta/2)$, for the rotation about x-axis. Thus, the rotation matrix of order three can be expressed as

$$\mathscr{R}_3 = \frac{1}{c^2 + d^2} \begin{bmatrix} c^2 + d^2 & 0 & 0 \\ 0 & c^2 - d^2 & -2cd \\ 0 & 2cd & c^2 - d^2 \end{bmatrix} \tag{5.16}$$

$$\Rightarrow \mathscr{R}_3^{\psi} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & \sin(\theta) \\ 0 & -\sin(\theta) & \cos(\theta) \end{bmatrix} \tag{5.17}$$

Similarly, rotation matrix about the y- and z-axis can be obtained. The above discussed matrices $\mathscr{R}_2^{\psi}$ and $\mathscr{R}_3^{\psi}$ represent the most basic rotation matrices and can be extended to obtain the higher order rotation matrix. Mathematically, the higher order rotation matrices can be formed as follows:

1. Higher even order Rotation Matrix:

$$\mathscr{R}_{2m}^{\psi} = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathscr{R}_m^{\psi} & \mathscr{R}_m^{\psi} \\ -\widetilde{\mathscr{R}}_m^{\psi} & \widetilde{\mathscr{R}}_m^{\psi} \end{bmatrix} \tag{5.18}$$

2. Higher odd order Rotation Matrix:

$$\mathscr{R}_{2m+1}^{\psi} = \frac{1}{\sqrt{2}} \begin{bmatrix} \mathscr{R}_m^{\psi} & \mathscr{R}_m^{\psi} & \mathscr{R}_0^T \\ \mathscr{R}_0^T & \mathscr{R}_0^T & 0 \\ -\widetilde{\mathscr{R}}_m^{\psi} & \widetilde{\mathscr{R}}_m^{\psi} & \mathscr{R}_0^T \end{bmatrix} \tag{5.19}$$

where $m \geq 2$, $\mathscr{R}_0$ is $1 \times m$ zero vector and the matrix $\widetilde{\mathscr{R}}_m^{\psi}$ is the flipped matrix $\mathscr{R}_m^{\psi}$ along x- and y- axis respectively. Further, it is easy to verify that these matrices are orthogonal and satisfying $\mathscr{R}_p^{\psi}(\mathscr{R}_p^{\psi})^T = 1$ for all $p \geq 2$. The higher order rotation matrices can be derived using the Eqns. (24)-(26).

A new parameterized all phase sin bi-orthogonal transform (PR-APBST) can be designed using the rotation matrix and APBST. Mathematically, the forward PR-APBST is given as:

$$X_{\psi} = PR\text{-}APBST_{\psi}(x) = \mathscr{R}_N^{\psi} E (\mathscr{R}_N^{\psi})^T x \tag{5.20}$$

the above equation suggest an unified way to reconstruct original matrix by exploiting the fact that the rotation matrices are orthogonal matrices. In other words, the inverse PR-APBST can be given by the following equation

$$x = IPR\text{-}APBST_{\psi}(X_{\psi}) = \mathscr{R}_N^{\psi} E^{-1} (\mathscr{R}_N^{\psi})^T X_{\psi} \tag{5.21}$$

Clearly from Eqns. 5.20 and 5.21, PR-APBST can be described by parameter ψ. The value of ψ can be realized as the key for the transform in the sense that without knowing the correct value of ψ, none can get the accurate transform coefficients. The following are the properties, which can be perceived from its definition.

1. *APBST Operator*: The PR-APBST of order $\psi = 0$ is the APBST operator as the rotation matrix will coincide with the identity matrix.

2. *Successive Applications of PR-APBST*: Successive applications of PR-APBST is equivalent to a single PR-APBST with order equal to the sum of the individual orders. Mathematically,

$$PR\text{-}APBST_{\psi}\big(PR\text{-}APBST_{\theta}(x)\big) = PR\text{-}APBST_{\psi+\theta}(x) \tag{5.22}$$

3. *Linearity*: PR-APBST is a linear transform. Mathematically,

$$PR\text{-}APBST_{\psi}\big(x+y\big) = PR\text{-}APBST_{\psi}(x) + PR\text{-}APBST_{\psi}(y) \tag{5.23}$$

4. *Higher Dimensional PR-APBST*: Due to the separability of the transform, the higher dimensional PR-APBST can be defined by successive implication of one dimensional PR-APBST along all the directions. For instance, two dimensional PR-APBST can be viewed as

$$PR\text{-}APBST_{\psi,\theta} = PR\text{-}APBST_{\psi}\big(PR\text{-}APBST_{\theta}\big) \tag{5.24}$$

5.2 PROPOSED BIOMETRIC INSPIRED ENCRYPTION SYSTEM

5.2.1 Key Generation Inspired by Biometrics

This section essentially introduced the key management for the proposed encryption technique. The basic idea is to capture the biometric image of the patient through a automated biometric scanner. Biometric image is then used for feature extraction and key generation process. The proposed encryption technique essentially uses two types of keys where the first one is considered as the seed value for non-linear chaotic map and the latter is the parameter associated with PR-APBST. Assuming $B = [b(i,j)|i,j \in 1,2\ldots 2^{L-1}]$ the biometrics image of size $M_1 \times N_1$, the key generation process can be summarized as follows:

1. Compute second order (ϕ_2) and third order (ϕ_3) *Hu* moments of the biometric image B.

2. Obtain the difference between ϕ_2 and ϕ_3 and calculate Z as

$$Z = |\phi_2 - \phi_3|/(2^L - 1), \qquad 0 \leq Z \leq 1 \tag{5.25}$$

3. The seed value for non-linear map is calculated as

$$K = \big(2^L * Z\big) \mod 1 \tag{5.26}$$

where the standard arithmetic modular operation ensures that $K \in [0,1]$.

4. Obtain a normalized biometric image as:

$$\widetilde{B} = \frac{B - \min(B)}{\max(B) - \min(B)} \tag{5.27}$$

5. Construct the feature matrix F_M from $\widetilde{B}$ as follows:

$$F_M(i,j) = \begin{cases} 1, & \text{if } \widetilde{B}(i,j) \geq T \\ 0, & \text{if } \widetilde{B}(i,j) < T \end{cases} \tag{5.28}$$

6. Stack the feature matrix F_M in an array to form feature vector (F_V).

7. This feature vector (F_V) is used to generate the parameter for PR-APBST. The stepwise procedure can be described as follows:

   a) Compute $l = \{r^2 : r = min(M_1, N_1)\}$ and partition final l values of F_V into two equal segments F_{V_1} and F_{V_2}, respectively.

   b) Compute the angle from both the segments as

$$\psi_1 = \left(\sum_{i=1}^{l/2} F_{V_1}(i) \right) \mod 180 \tag{5.29}$$

$$\psi_2 = \left(\sum_{i=1}^{l/2} F_{V_2}(i) \right) \mod 180 \tag{5.30}$$

   where mod represent the standard modulo operation, which is used to make sure that $\psi_i \in [0, 180]$.

   c) Compute the optimal angle as

$$\psi = \left(\psi_1 + \psi_2\right) \mod 180 \tag{5.31}$$

   This optimal angle is finally used as the parameter for the PR-APBST.

5.2.2 Proposed Encryption Technique

The primary objective of this section is to introduce the proposed encryption technique for the medical images. The medical and biometric images of the patients are the input for this section. Let they be represented respectively by I and B. The proposed encryption technique comprises of the following steps.

1. Considering the key management system (given in Section 5.2.1), obtain the key for chaotic map (K) and the order of PR-APBST (ψ).

2. Construct a sequence $\mathscr{K}$ based on nonlinear chaotic map and adopting key K such that $\mathscr{K} = \{0 < k(g) < 1 | 1 \leq g \leq L\}$, where $L = M \times N$ is the length of the chaotic sequence.

3. Stack $\mathscr{K}$ in zig-zag order to get a random matrix $\mathscr{R}_{\mathscr{K}}$.

4. Randomize original medical image (I) using random matrix $\mathscr{R}_{\mathscr{K}}$ as follows

$$R_M(i,j) = \frac{\ln \mathscr{R}_{\mathscr{K}}(i,j)}{\ln I(i,j)} \tag{5.32}$$

5. Perform (ψ)-order PR-APBST on biometric image B, denoted by $\mathscr{B}$.

6. Perform QR decomposition on transformed biometric image $\mathscr{B}$, that is

$$\mathscr{B} = \mathscr{Q}_{\mathscr{B}} \mathscr{R}_{\mathscr{B}} \tag{5.33}$$

7. Apply SVD decomposition on transformed biometric image $\mathscr{B}_{\mathscr{J}}$, that is

$$\mathscr{B} = \mathscr{U}_{\mathscr{B}} \mathscr{S}_{\mathscr{B}} \mathscr{V}_{\mathscr{B}}^{\mathscr{T}} \tag{5.34}$$

8. Adopting $\mathscr{Q}_{\mathscr{J}}^{\mathscr{B}}$ and $\mathscr{U}_{\mathscr{J}}^{\mathscr{B}}$, encrypt the randomized image R_M as follows:

$$I^E = \mathscr{Q}_{\mathscr{B}} \mathscr{U}_{\mathscr{B}} R_M \mathscr{U}_{\mathscr{B}}{}^T \mathscr{Q}_{\mathscr{B}}{}^T \tag{5.35}$$

5.2.3 Decryption Process

The main objective of this section is to reconstruct the original medical image from the encrypted image. The decrypted process can be summarized as:

1. Considering the steps 5-7 of Section 5.2.2, generate $\mathscr{Q}_{\mathscr{B}}$ and $\mathscr{U}_{\mathscr{B}}$.
2. Adopting $\mathscr{Q}_{\mathscr{B}}$ and $\mathscr{U}_{\mathscr{B}}$, construct the randomized image from I^E as

$$\mathscr{I}^D = \mathscr{U}_{\mathscr{B}}{}^T \mathscr{Q}_{\mathscr{B}}{}^T I^E \mathscr{Q}_{\mathscr{B}} \mathscr{U}_{\mathscr{B}} \tag{5.36}$$

3. Considering the steps 1-3 of Section 5.2.2, generate the random matrix $\mathscr{R}_{\mathscr{K}}$.
4. The inverse randomization process is performed to get the final decrypted image (I^D). Semantically,

$$I^D(i,j) = \exp\left(\frac{\ln \mathscr{R}_{\mathscr{K}}(i,j)}{\mathscr{I}^D(i,j)}\right) \tag{5.37}$$

5.3 EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the main security aspects are validated to show the robustness of the proposed encryption scheme. Extensive experiments are carried out using Matlab platform on different medical images including ultrasound, MRI/CT brain, Heart and X-Ray images. All of the experimental images are having the size 256×256 and are 8-bit gray-scale images. The proposed scheme utilizes two parameters, which essentially act as keys wherein the first key (K) is used as initial seed for the non-linear chaotic map while the second key (ψ) is used as the order of parameterized APBST. Both the keys are estimated from the biometrics image of the patient. Biometrics emerges as most effective and secure technique for the key generation due to its permanent and unique features. Therefore, biometric inspired key generation is deployed to provide higher and robust security to the medical images.

As Biometrics, fingerprints images, which are oldest and widely accepted biometrics for personal verification and identification, are used in all experiments. The fingerprints are believed to be unique across individuals and across fingers of the same individual. Hence, this work is concentrated to obtain keys from the fingerprints of the patients. The fingerprints are used in numerous real life applications but their performance are restricted by the quality of the captured fingerprints. In contrast, the generated keys from the fingerprint images also depend on the quality of the fingerprint images. Hence, to ensure the robust performance concerning the quality, it is essential to improve the quality of captured fingerprints for which well-known fingerprint enhancement algorithm, presented in [Hong *et al.*, 1998], is employed. The attributes of an ideal encryption technique is that it should be robust enough to secure the digital data against different kind of attacks such as brute-force and cryptanalytic attacks. Therefore, the efficiency of the proposed scheme is investigated by the evaluation of the sensitivity analysis, key-space analysis, edge distortion analysis and statistical analysis.

5.3.1 Perceptual Security Analysis

The perceptual security analysis is carried out to verify the visual performance of the proposed technique. In general, a technique is considered to be perceptually strong if the encrypted image does not reflect any information about the original image otherwise it may be possible to obtain the overview of the original image information using statistical models/properties. Therefore, visual and subjective evaluation has been carried out to measure the unintelligible nature of

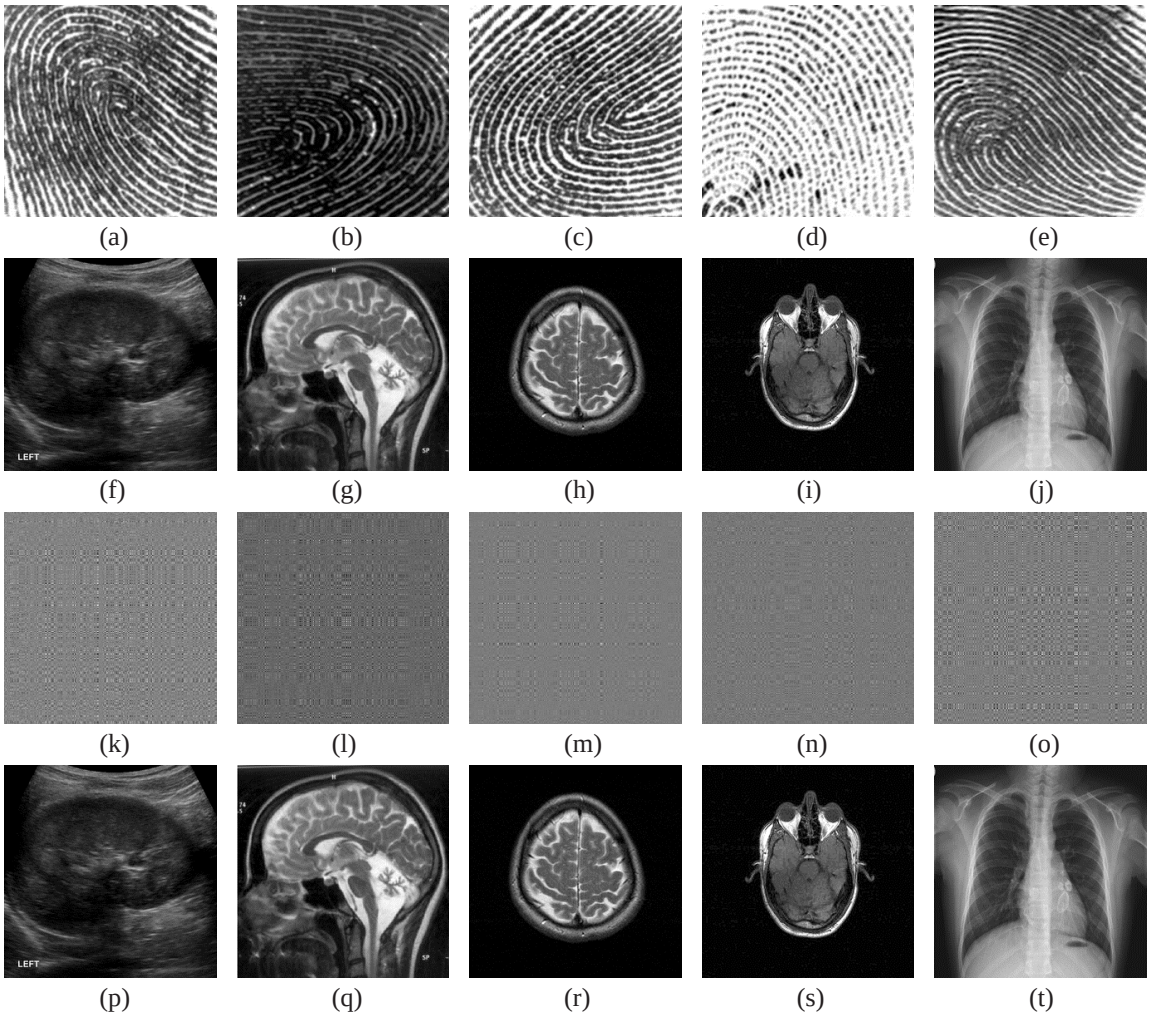


Figure 5.1 : Experimental Images:(a-e) Fingerprint images, (f-j) Original medical image, (k-o) Encrypted medical images, (p-t) Decrypted medical images.

the proposed encryption technique. The original, encrypted and decrypted images are visually depicted in Fig. 5.1 whereas subjective evaluation has been done by the standard image quality objective metrics such as peak signal to noise ratio (PSNR), universal image quality index (UQI), structural similarity index measure (SSIM) and normalized correlation coefficient (NC) respectively. The mathematical definitions of these matrices are depicted in Table 5.1. In principle, higher values of these metrics in the principal range shows higher similarity between the images [Wang and Bovik, 2006]. From Fig. 5.1, it can be observed that encrypted medical image does not exhibit any information about the original medical images. In contrast, decryption process perfectly decrypts the encrypted image and produce a high quality estimate of the original medical image according to the human visual system. A similar observation has been realized from the subjective evaluation, depicted in Table 5.2. Hence, it can be concluded that proposed technique perfectly encrypt and decrypt the medical images.

5.3.2 Key Space Analysis

Key Space size refers to the total number of different keys associated with an encryption scheme. In principle, a large key space is reasonably good enough to resist the brute-force attack. Thus, the size of key space plays a vital role in the design of an encryption technique. Two keys K

and ψ are used in the proposed technique. One of the key ψ refers to the order of PR-APBST and lie in the [0,180]. However, second key K used as the seed value for a non-linear chaotic map and contained in the interval [0,1]. The key space for the key K has been discussed as follows.

Consider two different sequences K_1 and K_2 of predefined length L with respect to seed value K and $K+d$, i.e., $K_1 = \{0 < K(g) < 1 | 1 \leq g \leq L_1\}$ and $K_2 = \{0 < K(g) < 1 | 1 \leq g \leq L_2\}$. Now, key space is estimated using mean square error of both the sequences by the following equation.

$$MAE(K_1, K_2) = \frac{1}{L} \sum_{g=1}^{L} |K_1(g) - K_2(g)| \tag{5.38}$$

The key space with respect to K is equivalent to $1/d_0$, where d_0 is the value of d for which MAE is zero. In the simulation, value of parameter d_0 is 2.361×10^{-19} for K. In a similar way, key space for other key (ψ) is calculated and is found to be 3.474×10^{-16}. The total key space for the proposed technique comes out to be 10^{35}, which indicates the the higher security of proposed encryption technique against the brute-force attack.

5.3.3 Key Sensitivity Analysis

Key sensitivity analysis determines the key variation effect in an encoding scheme. Generally, a small variation in keys of an ideal encryption should not produce the perfect decryption i.e the scheme should be sensitive to the secret keys. Therefore, the key sensitivity of the proposed technique is examined to verify the efficiency of the scheme. In the proposed scheme, keys are calculated from the fingerprint image of the main user. The sensitivity is measured by the selecting the wrong fingerprint image in the decryption process and the resultant decrypted image is compared with the original fingerprint image. Let D_C and D_W represents the decrypted medical image form correct fingerprint and wrong fingerprint images respectively. The key sensitivity factor (KS) is computed as follows:

$$KS = \frac{DSM(D_C, D_W)}{M \times N} \tag{5.39}$$

where $M \times N$ is the size of medical image. The dissimilarity factor DSM is defined as

$$DSM = \sum_{i=1}^{M} \sum_{j=1}^{N} D_C(i,j) \otimes D_W(i,j) \tag{5.40}$$

Table 5.1 : Mathematical definitions of objective metrics used in perceptual security analysis.

Objective Metric[†]	Principle Range
$PSNR(f,g) = 10\, log_{10} \frac{255^2}{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [f_{i,j} - g_{i,j}]^2}$	≥ 28
$UQI(f,g) = \frac{\sigma_{fg}}{\sigma_f\ \sigma_g} \cdot \frac{2\mu_f \mu_g}{\mu_f^2 + \mu_g^2} \cdot \frac{2\sigma_f \sigma_g}{\sigma_f^2 + \sigma_g^2}$	$[0,1]$
$SSIM(f,g) = \frac{(2\mu_f \mu_g + C_1)(2\sigma_{fg} + C_2)}{(\mu_f^2 + \mu_g^2 + C_1)(\sigma_f^2 + \sigma_g^2 + C_2)}$	$[0,1]$
$NC(f,g) = \frac{E(x - E(x))(y - E(y))}{\sqrt{E(x^2) - (E(x))^2} \sqrt{E(y^2) - (E(y))^2}}$	$[0,1]$

[†] The interpretation of the symbols used in these definitions can be seen in [Wang and Bovik, 2006].

Table 5.2 : Perceptual Security Analysis for experimental images.

Metric	Values between original and									
	Encrypted Image					Decrypted Image				
	Ultrasound	Brain-1	Brain-2	Heart	X-Ray	Ultrasound	Brain-1	Brain-2	Heart	X-Ray1
PSNR	8.5472	11.6102	8.6762	8.4126	13.0676	292.8110	296.2816	301.1565	302.404	296.2415
UQI	0.0005	0.0012	0.0023	0.0018	0.0006	0.9725	1.00	1.00	0.9756	0.9898
SSIM	0.0739	0.0970	0.0325	0.0348	0.1577	1.00	1.00	1.00	1.00	1.00
NC	0.0021	0.0051	0.0064	0.0074	0.0049	1.00	1.00	1.00	1.00	1.00

$$D_C(i,j) \otimes D_W(i,j) = \begin{cases} 1, & \text{if } D_C(i,j) \neq D_W(i,j) \\ 0, & \text{if } D_C(i,j) = D_W(i,j) \end{cases} \tag{5.41}$$

For a perfect encryption technique, the key sensitivity factor should near about 100%. Five different fingerprint images are considered for the decryption purpose of the medical image. In order to test key Sensitivity for medical images, the replacement of fingerprint has been performed from each other. For example, the decryption of images Fig. 5.1 (f) have been performed with other fingerprint image Fig. 5.1 (b-e) and similar to other images. This notifies that the decrypted image from wrong fingerprint images are visually un-recognizable and look similar to the encrypted image. This indicates that no one can obtain the original image without original biometric. Hence proposed technique is highly sensitive regarding the key variation. The key sensitivity factor for medical images are depicted in Table 5.3.

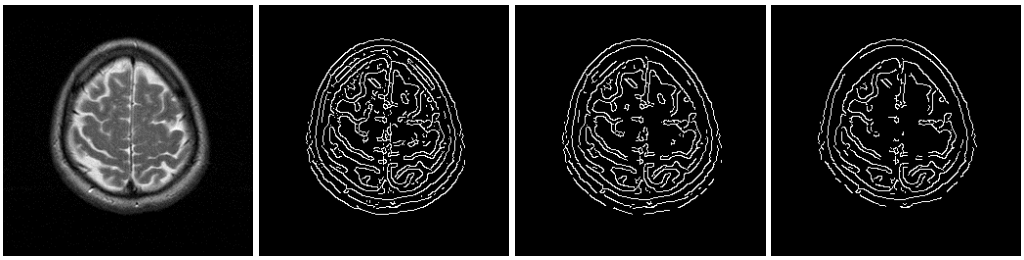
Table 5.3 : Key Sensitivity Analysis for All Medical Images.

Image	Fig. 5.1(b)	Fig. 5.1(c)	Fig. 5.1(d)	Fig. 5.1(e)	Fig. 5.1(a)
Ultrasound	100%	100%	100%	100%	100%
Brain-1	100%	100%	100%	100%	100%
Brain-2	100%	100%	100%	100%	100%
Heart	100%	100%	100%	100%	100%
X-Ray	100%	100%	100%	100%	100%

5.3.4 Edge Similarity Analysis

Edges are the most prominent and natural features within an image. They indicate the local variation in the intensity level of an image. Typically, edges describe the shape and geometry of the objects concealed in the image and can be determined using gradient information and a threshold. This information can be estimated using standard edge detection methods with single threshold. However, edges determined using higher threshold value indicate larger discontinuity whereas edges obtained at lower threshold values generally suffered from false edge information. More precisely, the edges obtained using multiple thresholds with respective suitable weights provide the better accuracy. Therefore, edge detection is applied using multiple threshold to obtain the accurate information in encrypted domain.

Let S_T be a set of threshold values considered in for edge detection algorithm $E_{Det}(I,t)$, where I is an input image and $t \in S_T$. Edges detection operation is employed on the original image I_o and its encrypted version I_e to estimate the binary edge images given by $B_o^{(t)} = E_{Det}(I_o,t)$ and $B_e^{(t)} = E_{Det}(I_e,t)$ respectively. Let $B^{(t)}$ denote the common edges present in the image for a given threshold t, then the set of edges can be obtained as follows [Xiang *et al.*, 2016]



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

Figure 5.2 : Edge images detected by the Canny edge detector with different thresholds: (a) Original image. (b) t = [0, 0.1]. (c) t = [0.1, 0.2], (d) t = [0.2, 0.3].

$$B^{(t)}(x,y)=\begin{cases}\left(1-\frac{|I_o(x,y)-I_e(x,y)|}{\ell}\right), \text{ if } B_{I_o}^{(t)}(x,y)\wedge B_{I_e}^{(t)}(x,y)=1 \\ \qquad\qquad \text{and } |I_o(x,y)-I_e(x,y)|\le \ell \\ 0, \qquad\qquad \text{otherwise}\end{cases} \tag{5.42}$$

where $\wedge$ signify the logical **AND** operation. To control the difference between $I_o(x,y)$ and $I_e(x,y)$, a threshold ℓ, $0 \le \ell \le 255$ is introduced. Both edge detection and the change in the luminance are used to obtain the more accurate results.
For a given threshold t, the edge similarity $E_S^{(t)}$ can be determined between $I_o(x,y)$ and $I_e(x,y)$ as follows [Xiang *et al.*, 2016]

$$E_S^{(t)}(I_o,I_e)=\frac{N(B^{(t)})}{N\left(B_{I_0}^{(t)}\right)} \tag{5.43}$$

where $N(\cdot)$ is the L_1 norm operation. The threshold parameter t play a decisive role in the edge detection of the image. The binary images obtained through canny edge detector for different threshold t: [0.0, 0.1], [0.1, 0.2], and [0.2, 0.3] are depicted in Fig. 5.2. It can be observed that high threshold results into fewer edges because pixel points with lower discontinuity are considered as the non-edge points in the image. In contrast, lower threshold may leads to false identification, where irrelevant information such as noise may be considered as the edges in the results because the algorithm is highly sensitive to the magnitude of the gradient. It may be noted that all the points, regardless of noise, with maximum discontinuity are always retained. As a result, points with maximum discontinuity will contribute strongly to edge similarity measure. Edge similarity for for different threshold is depicted in Table 5.4.

Table 5.4 : Edges similarity between the original and encrypted image for different threshold value.

Image	t=[0,0.1]	t=[0.1,0.2]	t=[0.2,0.3]	t=[0.3,0.4]
Ultrasound	0.5357	0.4375	0.4000	0.2500
Brain-1	0.1362	0.1875	0.0845	0.1429
Brain-2	0.3443	0.2105	0.2712	0.1600
Heart	0.5714	0.3143	0.2059	0.1290
X-Ray	0.3333	0.2615	0.1569	0.1154

5.3.5 Edge Distortion Analysis

Edges are the most prominent and natural features within an image. They indicate the local variation in the intensity level of an image. Typically, edges describe the shape and geometry of the objects in the scene. In an encryption scheme, the encryption should be done in a way such that

the encrypted image must not revile any information about the edges. Let g and h are the original and encrypted image with associated edge binary matrix B_g and B_h. Then, edge distortion ratio (EDR) can be determined as follows:

$$EDR = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|B_g(i,j) - B_h(i,j)|}{(B_g(i,j) + B_h(i,j))} \times 100\% \tag{5.44}$$

For edge binary matrix, the edge detection operation can be performed using Canny edge detector, Prewitt or Sobel operator. Here, Prewitt operator is selected for edge detection due to its better performance. Practically, a perfect encryption technique should reflect the higher EDR value. The EDR of encrypted medical image Ultrasound, Brain-1, Brain-2, Heart and X-ray are 97.56, 95.63, 98.99, 96.00 and 97.03 respectively. These values essentially imply that most of the edges are displaced in the encrypted counterpart of the considered medical images.

5.3.6 Statistical Analysis

A robust encryption technique can ensure the security by preventing the information leakage to the attacker. For this purpose, spectrum and correlation analysis have been discussed to measure the statistical robustness of the proposed technique. These analysis can be described as follows.

Spectrum Analysis

Spectrum analysis provides the basic structure of spectrum that characterize the frequency content of a digital signal. It is primarily used to measure the strength of the different frequency component. Therefore, the spectrum of original and encrypted medical images have been estimated to compare the respective amplitude spectra. If the amplitude spectra of the encrypted image are almost uniformly distributed and structurally dissimilar from the amplitude spectra of original image then it represents the perfect encryption. However, the amplitude spectra of the original and decrypted image should be similar to make the decryption process perfect. The amplitude spectra corresponding to original, encrypted and decrypted images have been shown in Fig. 5.3. It can be observed from Fig. 5.3(a) that there exist a peak in the middle which corresponds to highest narrow spectrum. Also, it notifies the pattern of information distribution and energy concentration of medical images. This pattern increases the risk of information leakage during the transmission. Hence, if the information is equally concentrated all over the region of an image then risk of information leakage will be minimal. This can be observed in listed Fig. 5.3(b). In contrast, the identical amplitude spectra of original and decrypted images (depicted in Fig. 5.3(a) and Fig. 5.3(c) respectively) verified the efficiency and completeness of the decryption process.

Correlation Analysis

Correlation is an important tool to express the relationship between the neighbouring pixels of an image and determines the randomness in an image. For a secure image encryption, the encrypted image should have a weak correlation among the adjacent pixels. For this purpose, P different pairs of adjacent pixels are randomly selected in any direction (either horizontally or vertically or diagonally) and calculate the correlation coefficient using the definition listed in Table 5.1. Figure 5.4 shows the distribution of correlation coefficients among the horizontal adjacent pixels in original, encrypted and decrypted medical images. In contrast, the correlation coefficients of all experimental images in horizontal and vertical directions are shown in Table 5.5.

5.4 EFFICIENCY OF DECRYPTION PROCESS

In this section, the efficiency of decryption process has been measured using sensitivity of the fingerprint images. In other words, the authentic person must only be able to decrypt the

medical image with fingerprint images. For sensitivity analysis, the fingerprint images have been interchanged in the decryption process. The fingerprint image used in the encryption of a medical image is used in the decryption of other medical images and vice versa. The obtained results for the same are depicted in Fig. 5.5. From the figure, it can be seen that ultrasound, MRI/CT brain, Heart

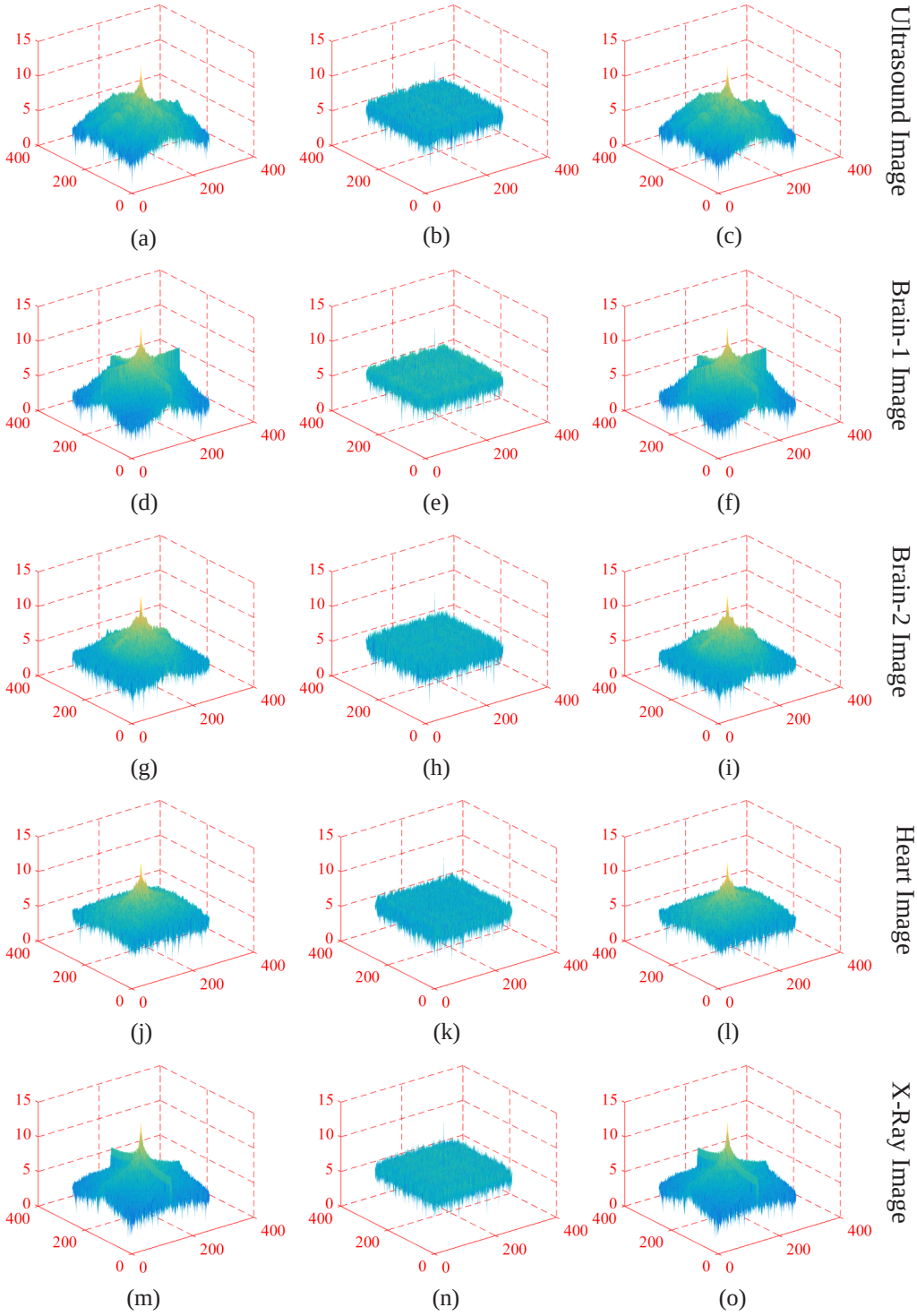


Figure 5.3 : Amplitude spectra of Original Images (left column), Encrypted Images (middle column), Decrypted Images (right column).

and X-Ray images are perfectly decrypt with true fingerprint images only. In contrast, the wrong fingerprint images are not able to perfectly decrypt the medical image, further obtained images do not reveal any information of the original medical images. This experiment is further extended by

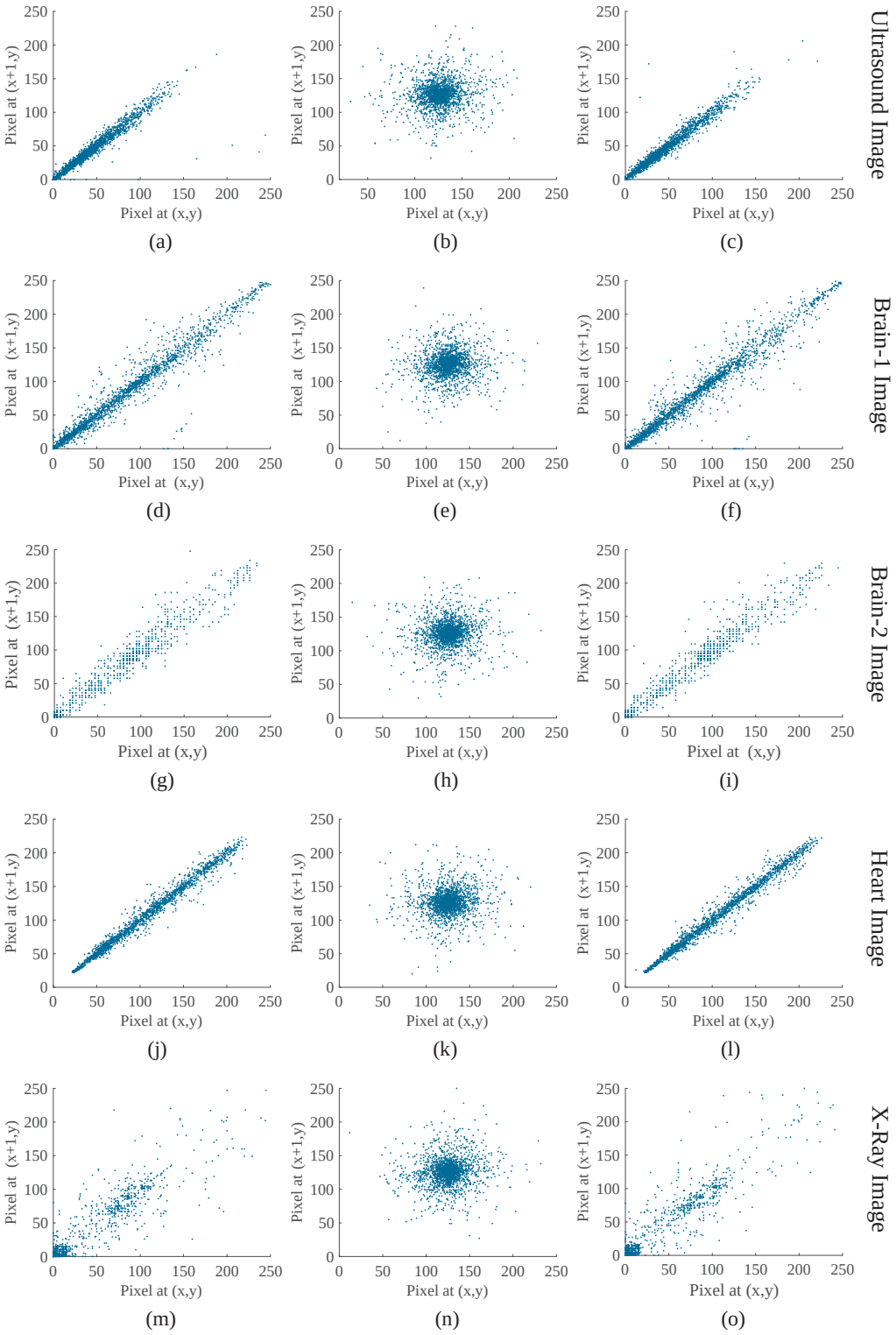


Figure 5.4 : Correlation distribution of horizontal pixels in: Original Images (left column), Encrypted Images (middle column), Decrypted Images (right column).

Table 5.5 : Correlation Coefficients of Two Adjacent Pixels for All Medical Images.

Images	Direction	Original	Encrypted	Decrypted
Ultrasound	Horizontal	0.9741	0.1610	0.9715
	Vertical	0.9412	0.1150	0.9210
Brain-1	Horizontal	0.9675	0.0458	0.9667
	Vertical	0.9767	0.0336	0.9618
Brain-2	Horizontal	0.9832	0.0710	0.9825
	Vertical	0.9844	0.0287	0.9828
Heart	Horizontal	0.9409	0.0475	0.9401
	Vertical	0.9673	0.0678	0.9572
X-Ray	Horizontal	0.9899	0.9908	0.9892
	Vertical	0.9951	0.9949	0.9914

considering 1000 random fingerprint images. These images are taken from the FVC2000, FVC2002 and FVC2006 fingerprint dataset. These fingerprint images are employed in the decryption process and obtained an estimate of medical image, which is then compared with the original medical image. The comparison is done in terms of NC, PSNR, SSIM and UIQI.

The estimated results are shown in Fig. 5.6. From the figure, it can be observed that the estimated NC lie between 0 and 0.03 with average correlation value 0.0012, 0.0036, 0.0031, 0.0036 and 0.0032 corresponding to Ultrasound, Brain-1, Brain-2, Heart and X-Ray images. The red line in the graph shows the average correlation with different fingerprint images. Similarly, the objective metric PSNR, SSIM and UIQI is also analyzed for medical images. The results indicate there is no similarity between decrypted image with true and wrong fingerprint images, i.e, no one can decrypt the medical image other than the authentic person. Hence, proposed technique is highly efficient and secure. The medical images are encrypted with fingerprint images other than these images. The fingerprint images form the dataset that are employed in the decryption process one by one and the decrypted images are compared with the decrypted medical image with true fingerprint image in the terms of the ESA, NC, PSNR, SSIM and UIQI.

5.5 COMPARATIVE ANALYSIS

Another approach to assess the performance, of proposed technique is the comparison with some of the related state-of-the-art techniques. In this section, three techniques presented by [Cao *et al.*, 2017], [Zhou *et al.*, 2014] and [Liu *et al.*, 2018a]. The performance is evaluated considering the ESA, EDR, NC, UIQI, PSNR and SSIM. Edge similarity is estimated between the plaintext and ciphertext images for a weighted threshold t, parameter ℓ and the obtained results are shown in Table 5.6. In the experiment, the empirical value of parameter $\ell = 10$ and weight threshold is 0.15 over the set of considering threshold $t = \{0, 0.1, 0.2, 0.3\}$. It can be observed that proposed algorithm holds lower edge similarity among the existing algorithms for all the experimental images. On the other hand, EDR is also compared to analyze the capability of the proposed scheme. The performance of our scheme is equivalent to the performance of [Cao *et al.*, 2017] and better than all other existing techniques.

More comparative experiments are conducted to show the perceptual security considering similarity metric NC and UIQI. The obtained results are shown in Table 5.7. In the both the cases, the proposed scheme works well when compared to other existing schemes. Similarly, SSIM and PSNR are also used for comparative study using the considering schemes and obtained results are

Table 5.6 : Edge based comparison of proposed scheme with existing schemes.

	ESA				EDR			
	Cao Method	Zhou Method	Liu Method	Proposed Method	Cao Method	Zhou Method	Liu Method	Proposed Method
Ultrasound	0.2214	0.3333	0.3279	0.2881	97.29%	96.12 %	96.27 %	97.56%
Brain-1	0.1695	0.4667	0.3390	0.1038	96.01%	94.41 %	96.52 %	95.63 %
Brain-2	0.2571	0.3390	0.3226	0.2321	97.76%	96.87 %	97.33 %	98.99%
Heart	0.2857	0.4280	0.3652	0.2686	96.13%	94.36 %	96.10 %	96.00 %
X-Ray	0.1462	0.4713	0.2857	0.0981	96.45%	95.62 %	96.42 %	97.03 %

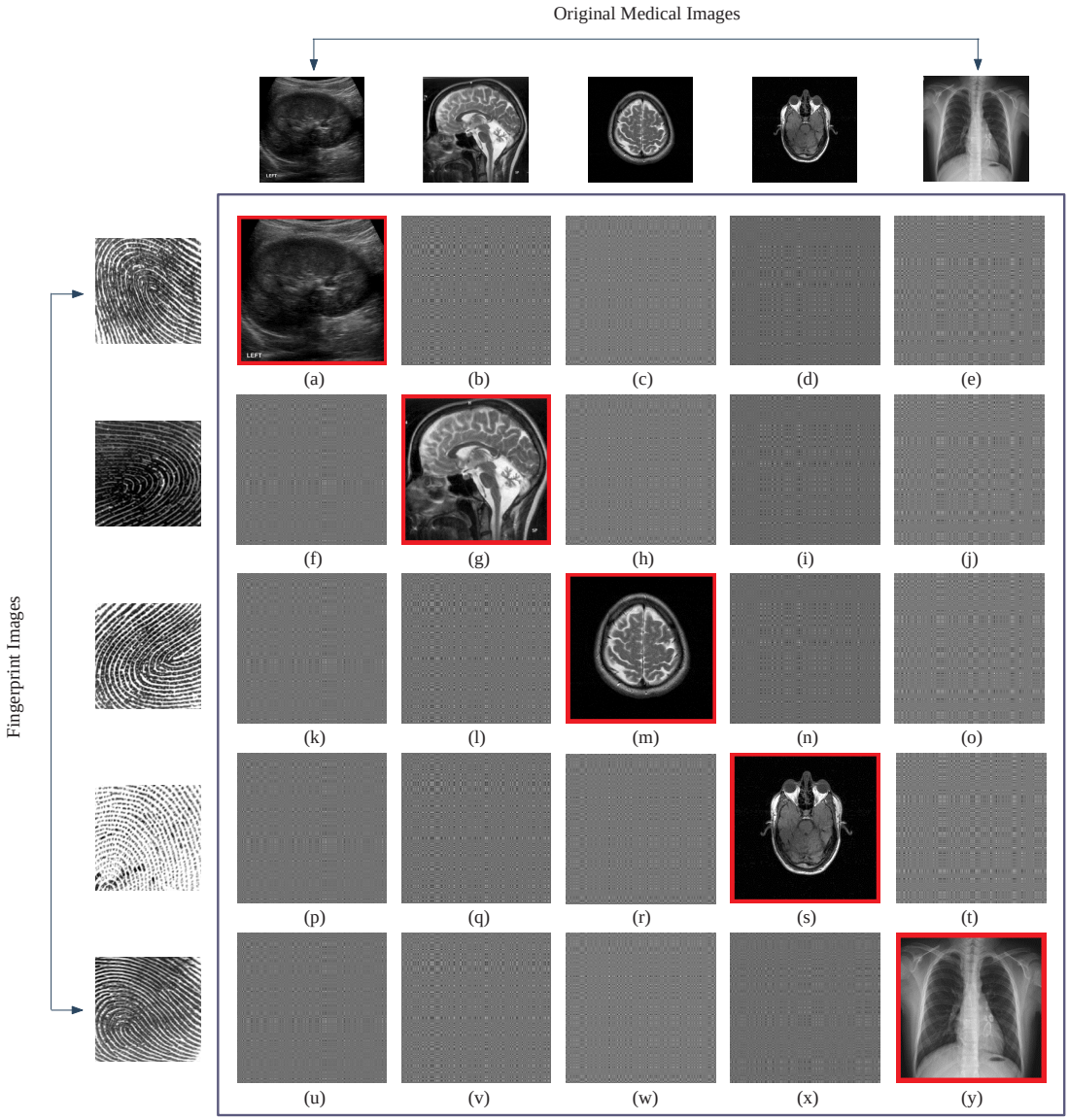


Figure 5.5 : Experimental Images: (a-y) Decrypted medical images; (a,g,m,s,y) Decrypted images with true fingerprint images.

listed in Table 5.8. From table, it is clear that the scheme shows lower structural similarity and peak signal to noise ratio between the original and cipher images, which is another sign of an efficient encryption scheme.

Table 5.7 : Comparison of proposed scheme with existing scheme in terms of NC and UIQI.

	NC				UIQI			
	Cao Method	Zhou Method	Liu Method	Proposed Method	Cao Method	Zhou Method	Liu Method	Proposed Method
Ultrasound	0.0032	0.0046	0.0037	0.0021	0.0010	0.0020	0.0012	0.0005
Brain-1	0.0058	0.0087	0.0068	0.0051	0.0021	0.0061	0.0031	0.0012
Brain-2	0.0064	0.0091	0.0071	0.0064	0.0025	0.0056	0.0053	0.0023
Heart	0.0069	0.0080	0.0056	0.0074	0.0023	0.0051	0.0043	0.0018
X-Ray	0.0061	0.0051	0.0054	0.0049	0.0008	0.0031	0.0018	0.0006

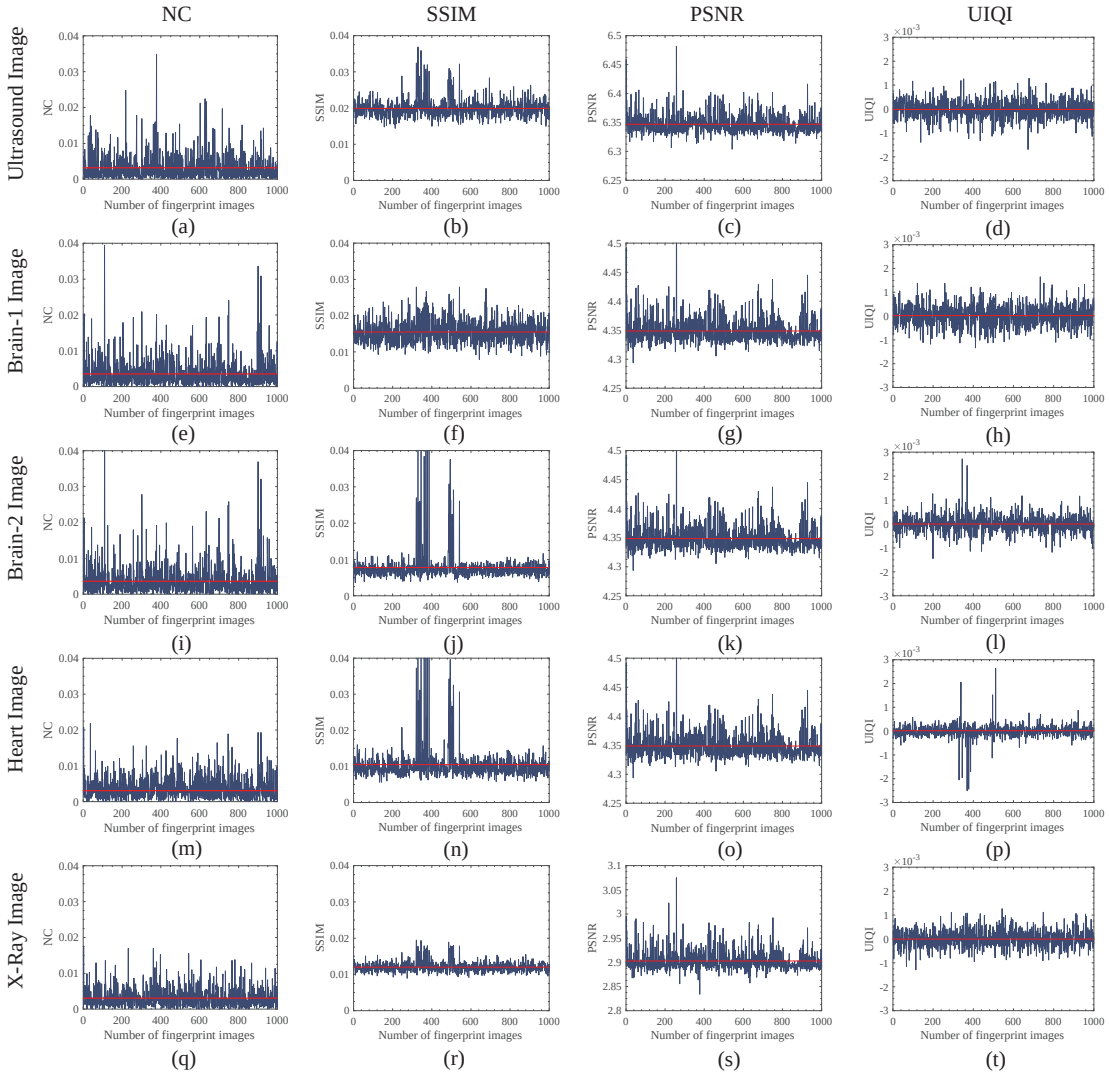


Figure 5.6 : Objective metric with different fingerprint images and decrypted medical images- First column: Normalization coefficients; Second column: structural similarity; Third column: Peak signal to noise ratio; Fourth column: Universal image quality index.

Table 5.8 : Comparison of proposed scheme with existing scheme in terms of SSIM and PSNR.

	SSIM				PSNR			
	Cao Method	Zhou Method	Liu Method	Proposed Method	Cao Method	Zhou Method	Liu Method	Proposed Method
Ultrasound	0.0790	0.1058	0.1420	0.0739	8.6140	9.5272	10.3642	8.5472
Brain-1	0.0836	0.1171	0.1931	0.0970	7.7913	9.6131	8.9317	11.6102
Brain-2	0.0470	0.0725	0.1331	0.0325	8.9150	10.0087	9.2606	8.6762
Heart	0.0540	0.1030	0.0854	0.0348	8.9321	8.8448	9.2457	8.4126
X-Ray	0.1061	0.1117	0.1523	0.1577	8.7682	9.7802	9.9466	13.0676

5.6 SUMMARY

In this work, an efficient and robust encryption technique to protect medical images is proposed. It is equipped with an efficient key management system incorporating the biometrics of the patient. The biometrics enhance the security of medical data due to its unique and natural features. It essentially provides a new mechanism of entering the secret key in the system. A new finding in the definition of all phase orthogonal transformation (APBST) namely parameterized all phase orthogonal transformation (PR-APBST) has been made where the transform is parameterized using higher order rotation matrix. PR-APBST is then coupled with QR and singular value decomposition to proposed an elegant encryption technique. For the validation of proposed technique, a detailed experimental analysis has been conducted through perceptual security, key-space analysis, key sensitivity, edge distortion and statistical analysis which demonstrate high robustness and security of medical image data.