International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 5, September-October 2019, pp. 81-94, Article ID: IJARET_10_05_009
Available online at http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=5
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

A DISTINCTIVE AFO ALGORITHM FOR SECURED MEDICAL IMAGE TRANSMISSION USING CHAOTIC CRYPTO TECHNIQUE

K.S. Tamilkodi*
Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India
Associate Professor in Computer Science, Presidency College, Chennai, Tamil Nadu, India

Dr. N. Rama
Principal, Dr. M.G.R. Government Arts and Science College for Women, Villupuram, Tamil Nadu, India
*Corresponding Author Email: tamil_vizhi@hotmail.com

ABSTRACT

The proposed system aims to develop a secure medical image encryption algorithm by combining chaotic map and cryptographic technique. In this paper, an innovative AFO (Arnold Cat Map, Fibonacci sequence and One Time Pad) algorithm for medical image encryption has been proposed. This AFO algorithm consists of four phases, in which diffusion, and confusion takes place two times. The pixels of the original (OI) and the key (KI) image are diffused by Arnold Cat Map first. Then the pixels of diffused images are confused with the help of Fibonacci sequence. Next, N unique random numbers are generated. Using these random numbers, the confused OI and KI image pixels are again permuted. The values of the resultant OI and KI pixels are pooled by utilizing the Vernam Cipher (also known as One Time Pad) in the final confusion phase. The quality of the reconstructed and an encrypted images are evaluated by some of the most widely used objective measures like MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), AD (Average Difference), MD (Maximum Difference), MAE (Mean Absolute Error), (CC) Correlation Coefficient, IF (Image Fidelity), SSIM (Structural Similarity Index Metrics). Results of these measures commends that the proposed AFO encryption algorithm is suitable for secure medical image transmission.

Keywords: Cryptography, image scrambling, confusion, diffusion, ACM, Fibonacci sequence, OTP, objective measures, AFO.

Cite this Article: K.S. Tamilkodi and Dr. N. Rama, A Distinctive AFO Algorithm for Secured Medical Image Transmission Using Chaotic Crypto Technique, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 10 (5), 2019, pp 81-94.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=5

1. INTRODUCTION

A secured data transmission was not the great requirement, when the idea of computer network was introduced. With the current technical and scientific advancements in digital transmission and imaging technology, people around the globe is interconnected by interchanging multimedia data (text / image / audio / video). With the ability of an imaging and communicating devices, every single moment of an individual can be documented and transmitted. The transmitted multimedia data can be used in the region of military, medical, educational, entertainment, industrial or social media.

Telemedicine or E-health services has taken center stage, in order to nullify the doctors - patient's physical distance, reduce the travelling time and medical expenses [1]. Also, it is used for administrative, clinical, research, remote educational and consultation purpose. Consequently, the paper based medical record are replaced by an Electronic Medical Records (EMR) which contains sensitive information about a patient's medical histories, medical images, financial and demographic details. The success of E-health services rely on medical images which plays an important role in earlier and effective diagnosis. Innovations in medical imaging techniques supported the doctors to view the internal organs of the patient throughout surgical procedure for effortless diagnosis of the diseases. Medical images which contain patient's health information need to be transferred from one place to another using unsecured high speed network. Thus, the progress in technology end up in privacy, confidentiality, integrity, availability and high level security threats for transmitted and stored data. If the sensitive health information is accessed by a hacker, there is a chance of using it either for selling those details to an advertising agency or for an individual usage leading to misdiagnosis [17]. A common preventive and defensive technique against this cyber criminals would be an encryption. Encryption converts the plain image into cipher image by using secret key. The core idea of cryptography is that, only the intended recipient should get intelligible image and it should be unintelligible for all others. Only by using the same secret key, the encrypted image can be decrypted to get back the original image in the case of private key cryptography. Conventional encryption algorithms which can provide high security for the text like Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), and RC4 are not suitable for image encryption in real time, because images have inbuilt qualities like bulk in size, high pixel redundancy and correlation among its adjacent pixels.

Considering these distinctive features of image, many image encryption algorithms have been proposed. Among them, chaotic image encryption technique become more popular because it has cryptographic confusion and diffusion properties. Pseudorandom sequences can be generated by chaotic maps, since it possess the features like nonlinearity, deterministic, ergodicity, mixing, unpredictability, control parameters and the sensitivity to initial conditions[15]. These driving factors influenced the researchers around the world to develop many chaotic image encryption algorithms.

In some applications, chaotic crypto techniques have almost overtaken cryptographic algorithms. The proposed AFO encryption scheme comprises two confusion and diffusion phases with biometric key image, since A. N. Pisarchik and M. Zanin [4] stated that pseudo-random numbers generated by only one chaotic system is not secure enough to withstand powerful cryptographic attacks. Arnold Cat Map and Unique random numbers are used for diffusing [31] the image pixels. For image pixel confusion, Fibonacci series and One Time Pad (OTP) operations are employed. The height and width of the key image is same as that of the original image. As required by the OTP, the key image is large enough to encrypt the original image.

Chaotic maps are simple unstable dynamical systems with high sensitivity to initial conditions [Devaney 1992] [11]. Arnold Cat Map (ACM) was proposed by Russian mathematician Vladimir Arnold in 1968 and it is based on a matrix with 1 as its determinant. ACM is reversible because of this determinant value [2]. To test his chaotic equation, he used a cat image. Hence, it is called as Arnold Cat Map. The use of ACM in an image encryption changes the position of the pixels and it does not alter the value of the pixels. After N iterations, the image pixel positions are fully transformed and the original image appears intelligible [20]. But, if iterated adequate number of times [6], the original image reappears. Arnold Cat Map is a periodic [23] and an invertible chaotic map defined as:

$$\begin{bmatrix} X_n' \\ Y_n' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} * \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \bmod N \quad (1)$$

Where

p and q are control parameters.

X_n and Y_n are actual pixel locations

X_n' and Y_n' are new pixel locations

Image scrambling is mainly used to preserve the confidentiality in image transmission. Fibonacci sequence generating technique is used to make visually distorted OI and KI. Fibonacci number F_n is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \quad (2)$$

With seed values of $F_0 = 0$ and $F_1 = 1$.

There is no degradation in the decrypted image using Fibonacci sequence.

The Vernam cipher is the simplest cryptosystem also called as one-time pad cipher. Vernam cipher is a special case of substitution cipher implemented by bitwise XOR operation and it is widely used in the design of modern encryption algorithms like DES and AES [27]. One-Time Pad (OTP) cipher is an encryption technique that cannot be cracked if used correctly. It was invented by Gilbert Vernam and Joseph Mauborgne in near the end of WWI. Claude Shannon proved mathematically that one-time pad was unbreakable in his work published in the late 1940s.

Following an introductory section, section 1 which provides relevant background information about the proposed scheme. This paper is organized into five sections. Section 2 examines about an existing image encryption algorithms based on chaotic maps and one time pad. Section 3 deals with an architecture of the proposed scheme. The experimental results and performance analysis of the proposed algorithms are demonstrated in Section 4. A conclusion of this paper is given in Section 5.

2. LITERATURE REVIEW

The importance of medical image security is widely acknowledged by the researchers, only a few ensure a proper level of confidentiality, integrity and availability before using the open network for transmission. Due to the rise of the communication network and imaging technologies, full-fledged security of the sensitive images transmitted over the insecure network is very difficult to achieve. Recently much attention has been devoted to the security of medical image transmission. As a result, number of chaos based cryptographic encryption algorithms have been developed by researchers.

In the year 2011, a chaos-based image encryption scheme with a novel permutation process has been proposed by Xin Ma, Chong Fu, Wei-min Lei, Shuo Li [29]. The diffusion performance is enhanced by applying Chebyshev map after a lightweight bit- level permutation algorithm, as a result the overall security is also enhanced. The authors concluded that the proposed image encryption technique is perfectly suitable for the real time secure image transmission over public networks.

In the year 2013, an efficient image encryption scheme based on multiple generalized Bernoulli shift maps and Arnold maps is proposed by Ruisong Ye and Yuanlin Ma [25]. Six generalized Bernoulli shift maps and one six-dimensional Arnold map are utilized to distort the pixel positions in the permutation process. Four generalized Bernoulli shift maps and one Arnold map are employed to change the gray values by a two-way diffusion process. The authors claimed that the proposed scheme can be a potential candidate for multimedia encryption.

In 2014, Asia Mahdi Naser Alzubaidi [6] suggested a novel and efficient color image encryption and decryption schemes by iteratively dividing image pixels into sixty four blocks and rotate each in 90 degree clockwise direction. Then 2D Arnold cat map is used to make more distortion in order to hide the statistical structure of original image pixels. 2D Henon map is used for diffusion. To encrypt the image, XOR operation is applied. Author resolved that more flexible, reliable, and higher encryption quality can be achieved by the proposed work.

In September 2014, Junqin Zhao, Weichuang Guo, Ruisong Ye [14] proposed a row-by-row / column-by-column one round permutation - substitution image encryption scheme based on generalized Arnold map to increase the speed of encryption. They recommended that the proposed image encryption scheme is robust and secure and can be used for secure image and video communication applications.

In September 2015, Anand Joshi, Maneesha Kumari [5] proposed a new approach for colour image encryption and decryption using involuntary matrix with Arnold transformation. They have compared the proposed method with some other existing methods and shown that the proposed method is better than those methods. The authors concluded that the proposed method can be used in digital RGB image processing to secure image data.

In the year 2018, Ranvir Singh Bhogal, Baihua Li, Alastair Gale and Yan Chen [22] developed an algorithm using a cat map combined with AES and tested it against AES in its standard form. The authors concluded that an encryption quality can be improved by applying a chaotic map to change the initial state of an image.

Though various research articles were perused, the proposed AFO algorithm a unique combination of Arnold Cat Map, Fibonacci sequence and One Time Pad were not encountered. Hence, this AFO algorithm is developed in order to avoid the limitation in the existing algorithms.

3. PROPOSED CHAOTIC CRYPTO MEDICAL IMAGE ENCRYPTION SCHEME

The main objective of this AFO algorithm is to increase the confidentiality and integrity of the transmitted image. The proposed encryption scheme comprises of following steps in order to secure the medical image transmission over the unsecure internet. This chaotic cryptosystem is the combination of image confusion and diffusion phases. Medical image as an original image and biometric image (fingerprint) as the key image are the inputs for this encryption algorithm.

3.1. Encryption Algorithm

The steps for the encryption process are as follows:

Step 1: Load the original image **OI** and key image **KI** of size N×N pixels.

Step 2: Convert **OI** and **KI** into N x N matrix.

Step 3: Set the control parameters **P** and **Q** of Arnold transform.

Step 4: Shuffle the OI and KI using 2D Arnold transform with parameters P and Q.

$$X_n' = X_n + PY_n$$
$$Y_n' = QX_n + (PQ + 1)Y_n$$

Step 5: Let the confused image obtained after 2D Arnold transform as **ATOI** and **ATKI**.

Step 6: Diffuse the pixel values of **ATOI** and **ATKI** by the Fibonacci sequence and let it be **FTOI** and **FTKI**.

$$FTOI_n = ATOI_{n-1} + ATOI_{n-2}$$
$$FTKI_n = ATKI_{n-1} + ATKI_{n-2}$$

Step 7: FTOI and **FTKI** is confused again by the unique random numbers (27, 73, 51, 76, 78, 100, 85, 86, 74, 1, 25, 30, 5……..) generated after giving the **seed** value and it is named as **RTOI** and **RTKI**.

Step 8: Finally **RTOI** and **RTKI** are given as input to One Time Pad encryption algorithm, which in turn will give the final encrypted image **EI** on the sender side.

$$\mathbf{EI(i) = RTOI\ (i)\ RTOK(i)}$$

The complete working flow for the encryption process of the proposed chaotic cryptosystem is portrayed in Figure 1. Original and Key images are provided as an input along with the control parameters p, q to the ACM. ACM equation (1) generates new x, y coordinates x', y' for shuffling the pixels of OI and KI. ATOI and ATKI are the two new images generated by ACM. After ACM, only the pixel positions are changed. The pixel values remain unaffected. In order to alter the pixel values Fibonacci sequence is used. Hence, ATOI and ATKI are set as an input to the Fibonacci sequence. It produces FTOI and FTKI after making changes in the pixel values. Using N unique random numbers, the pixel locations of FTOI and FTKI are changed again to produce an output as RTOI and RTKI. Cipher image gets generated after providing RTOI and RTKI as an input to the OTP. This cipher image is sent to the receiver and it gets revoked by using the decryption algorithm.

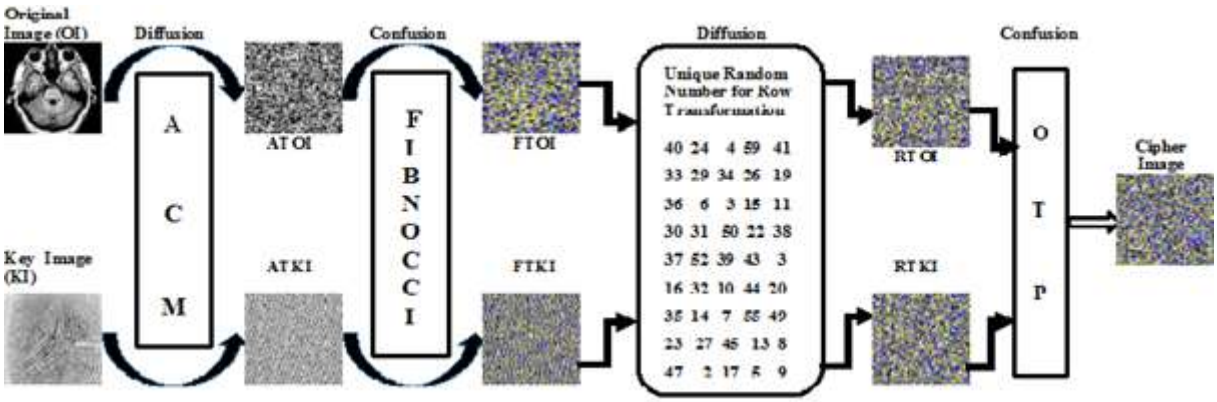

Figure 1. Encryption Process of the proposed system

3.2. Decryption Algorithm

The inverse order of the above encryption steps are followed in the decryption process of the proposed work to get back the original image OI on the receiver side. The decryption process steps are depicted in Figure 2. KI is not directly given as an input to the inverse OTP equation. Before providing KI as an input, it has to be encoded as RTKI by applying the equations of ACM (1), Fibonacci (2) and finally unique random numbers for row transposition. Now RTKI is given as an input to inverse OTP, it generates RTOI as its output. FTOI is formed by row transposition of RTOI. FTOI is set as an input to inverse Fibonacci and ATOI is formed as its output. An original image gets decrypted after passing ATOI as an input to inverse ACM. The receiver is able get back the original image without any distortion finally and it is evident from the Figure 3.

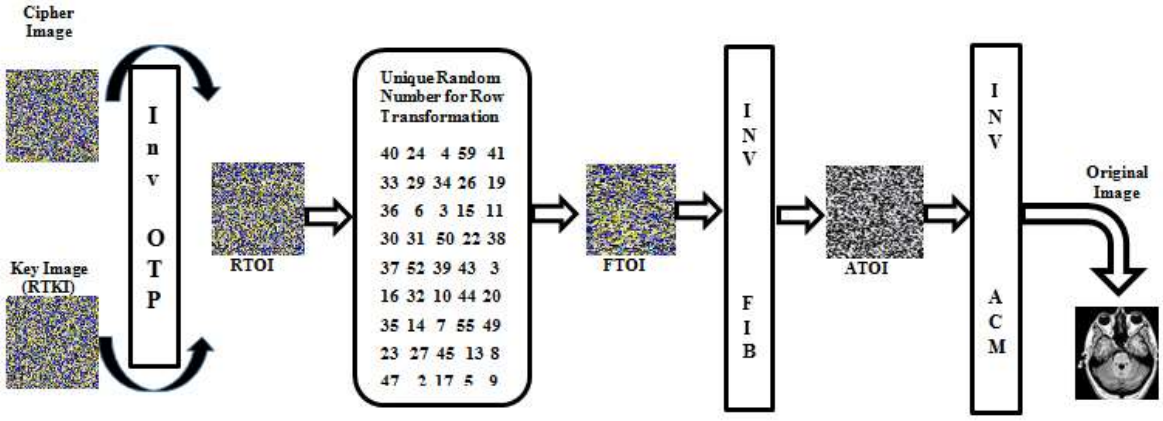

Figure 2: Decryption Process of the proposed system

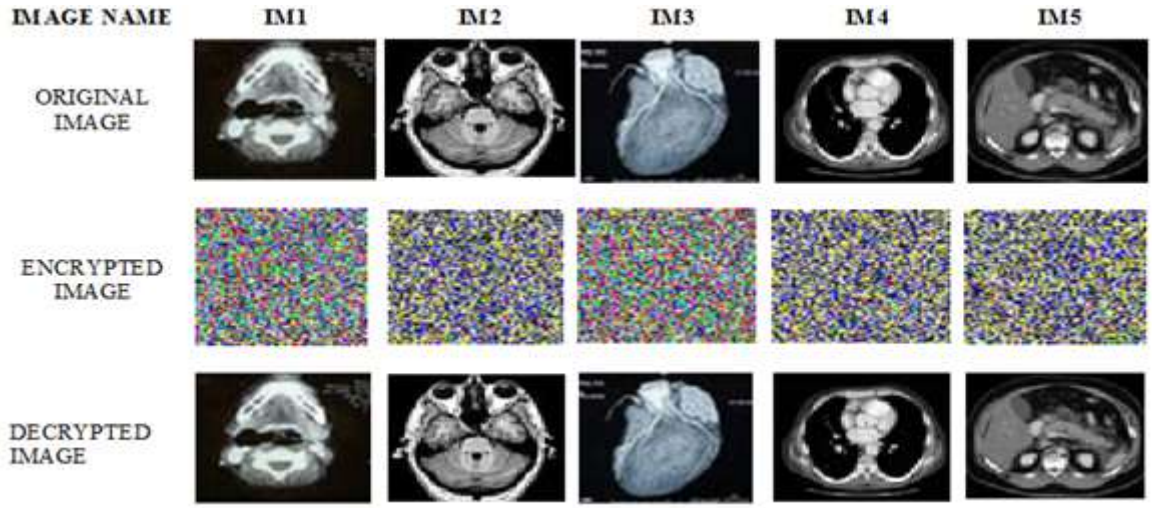

Figure 3. Original, Encryption and Decrypted Images

Using the numbers generated by the Arnold Cat Map, the position of the pixel values are changed in confusion phase [7]. The pixels are confused by Pseudo Random Numbers yet again. While in diffusion phase each and every pixel of the scrambled image is converted into new value first by using Fibonacci sequence and then by OTP. After encryption, the cipher image can be transmitted through the internet. The original image along with encrypted and decrypted images are shown in the Figure 3. From the visual inspection, the original and an encrypted images are looking absolutely dissimilar. Whereas the original and the decrypted images are looking completely similar.

4. RESULTS AND DISCUSSIONS

The proposed encryption algorithm is implemented using Java (Eclipse - Photon), on a Windows 8.1 machine (Intel i5-4210U CPU @ 1.70GHz). Mug shot data set was created by downloading few medical and fingerprint images from the internet. From the above data set, images of size (60 × 60, 100 × 100, 256 × 256, and 512 × 512) and types like JPEG, PNG and BMP were tried in this proposed algorithm. Here the results were given only for PNG typef of 60X60 image size. The following steps were carried out for pre-processing of these images.

- Images are resized to 60 x 60 pixels.
- Converting the above from RGB to Gray Scale.
- Changing values from Double precision to an Integer.

Transmission of medical images experience distortion triggering image quality degradation. Before using medical images for treatment, assessing the quality of a transmitted image plays vital role in image encryption in order to find the similarities between an original, encrypted and decrypted images. Hence, image quality metrics has become very popular and new metrics are continuously being proposed. Image quality metrics can be classified as Subjective and Objective approach [12]. In subjective approach, the quality of an image can be evaluated by human experts through visual comparison between an original, encrypted and decrypted images. Whereas in an objective method, it is measured by mathematical algorithms. Since subjective evaluation is time-consuming, expensive, and resource intensive, objective methods of evaluation is used. The efficiency of an image encryption and decryption quality of this method is determined by some of the most widely used objective measures which are discussed under two sets. First set is the Statistical test which includes Correlation test, Histogram analysis, Image Entropy, MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), MD (Maximum Difference), MAE (Mean Absolute Error), IF (Image Fidelity), SSIM (Structural Similarity Index Metrics). Differential attacks like NPCR (Net Pixels Change Rate), UACI (unified average change intensity) and Sensitivity analysis is the second set. The results of the AFO algorithm is not compared with earlier results, due to the inadequacy of similar chaotic- crypto algorithms.

4.1. Statistical Analysis

An ideal cryptosystem supposed to be strong against any statistical attacks, pointed out by Shannon. The following tests are conducted to verify the strength and stability of the proposed chaotic crypto system to withstand against statistical and differential attacks, along with the key sensitivity analysis.

4.1.1. Pixels Correlation Analysis

The correlation between an original and an encrypted images are analyzed in the horizontal and diagonal directions in this paper. The results of the correlation coefficients between an original and an encrypted images using the formula in (3) are listed in Table 1. If $r_{xy} = 1$, then, it implies that the pixel values of an original image are not changed after encryption. If $r_{xy} = 0$, then, it implies that the pixel values of an original image are completely changed after encryption [13]. The value of r_{xy} can be from -1 to +1. If $r_{xy} = -1$, then, it implies that the pixel values of an original image are inversely dependent with the pixel values of an encrypted image. Observing the r_{xy} values (approximately equal to 0) from the Table 1, it reveals that there is no or least correlation between the original and encrypted images using the proposed algorithm and it can withstand against correlation based attacks.

$$r_{xy} = \frac{\mathbf{Cov}(\mathbf{x},\mathbf{y})}{\sqrt{\mathbf{D}(\mathbf{x})}\sqrt{\mathbf{D}(\mathbf{y})}} \quad (3)$$

Where

$\mathbf{Cov}(\mathbf{x},\mathbf{y}) = \frac{1}{\mathbf{N}}\sum_{i=1}^{N}(X_i - \mathrm{E}(X_i))\,(Y_i - \mathrm{E}(Y_i))$

$\mathbf{D}(\mathbf{X}) = \frac{1}{\mathbf{N}}\sum_{i=1}^{N}(X_i - E(X_i))^2$ & $\mathbf{D}(\mathbf{Y}) = \frac{1}{\mathbf{N}}\sum_{i=1}^{N}(Y_i - E(Y_i))^2$

$\mathbf{E}(\mathbf{X}) = \frac{1}{\mathbf{N}}\sum_{i=1}^{N}(X_i)$, N is the total number of pixels in an image

X_i and Y_i are the pixel values of an original and an encrypted images.

4.1.2. Histogram Analysis

The histogram of an image is primarily used to visually compare the original and cipher image. In image histograms, pixel or intensity values are shown on the X-axis and number of pixels at each intensity values are shown on the Y-axis. A bar on the histogram represents one pixel level.

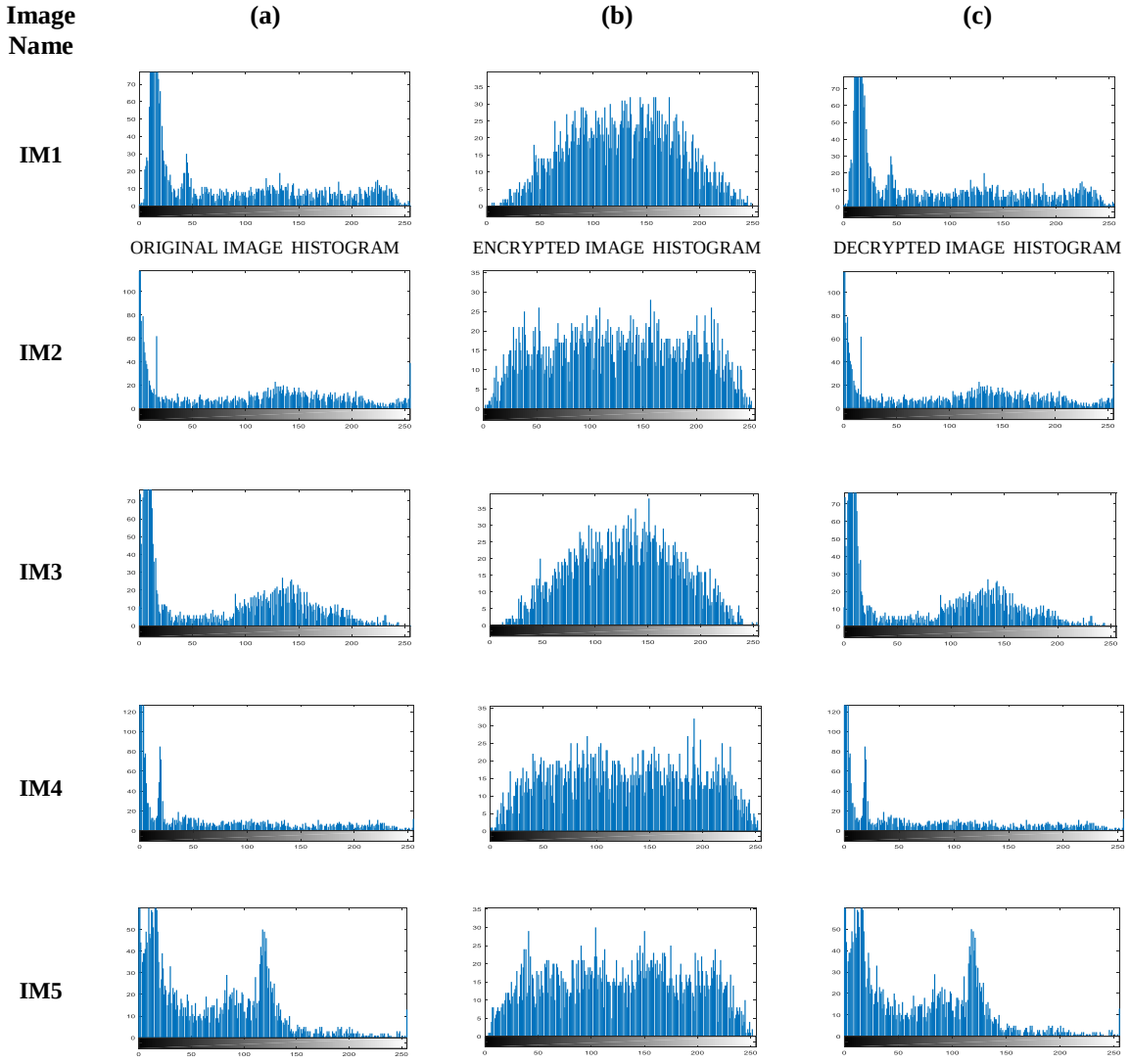

Figure 4: Histogram of the (a) Original Image (b) Encrypted Image (c) Decrypted Image

The histogram of an encrypted image should be completely different from that of the plain image. The histograms of the original, encrypted and decrypted images are presented in the Figure 4. The histograms of the encrypted image are fairly uniform and significantly different

from the plain image. The histograms of the original and decrypted images are looking identical.

4.1.3. Image Entropy Analysis

Shannon's entropy is used to find the randomness and unpredictability of an original image structure. Ideal value for an image entropy is 8 [30], since the gray image can have utmost 256 gray levels. Medical images of size 60 × 60 pixels are encrypted and the information entropy is calculated for OI, CI and DI. Entropy results are listed in Table 1. It is noticeable that the entropy of the encrypted images are very close to the ideal value of 8 and hence the proposed algorithm is secure against entropy analysis.

4.1.4. Mean Square Error (MSE)

MSE is the cumulative squared difference between the original and encrypted images [16] can be used to check the avalanche effect. MSE is a pixel difference based metric. Let X(i, j) and Y(i, j) are the pixel values of an original image and an encrypted image respectively, then MSE is calculated by using (4). The outcome of MSE are listed in Table 1.

$$\mathbf{MSE} = \frac{1}{\mathbf{MN}} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{i,j} - E(Y_{i,j}))^2 \quad (4)$$

Where M and N are number of pixels in OI and CI.

MSE = 0, if pixel values of the original and encrypted images are same. MSE will be maximum, if pixel values of the original and encrypted images are different. MSE can give 0 to any maximum value depending upon the pixel values of two images. MSE values in the Table 1 demonstrated that proposed encryption algorithm is secure and efficient.

4.1.5. Peak Signal to Noise Ratio (NPCR)

The PSNR is an image quality metric to measure the pixel value difference between the original and the encrypted image. PSNR is used to find the quality of an encrypted image by verifying the abnormalities in its pixel values. It is calculated in decibels by using (5) and inversely proportional to MSE. If an encrypted image is noisier, then the value of PSNR will be less [34]. The expected value of PSNR for an encrypted image should be smaller. From the Table 1, PSNR value for all the images are less than 10dB. Hence without knowing the secret key it is impossible to deduce the original image from an encrypted one.

$$\mathbf{PSNR} = \mathbf{10} \log_{\mathbf{10}} \mathbf{Max\ I^2} / \mathbf{MSE} \quad (5)$$

Where I = 255 for an 8 bit gray image.

4.1.6. Mean Absolute Error (MAE)

Mean Absolute Error (MAE) is an average of absolute difference between the original and encrypted images. It is calculated by using the equation (6). If the result of MAE is high, then the quality of the images (OI and EI) are worse in general. The MAE results of the proposed Chaotic Crypto medical image encryption algorithm is shown in the Table 1. For all the five medical images, the MAE values in Table 1 are high. Hence, using the proposed chaotic crypto algorithm, the encrypted image, which is completely different from original image.

$$\mathbf{MAE} = \frac{1}{\mathbf{MN}} \sum_{i=1}^{M} \sum_{j=1}^{N} |X_{i,j} - Y_{i,j}| \quad (6)$$

Where $X_{i,j}$an original image and $Y_{i,j}$ is an encrypted image at i and j co-ordinates.

4.1.7. Maximum Difference (MD)

MD is the maximum pixel difference between the original image and its corresponding encrypted image. It is calculated using the formula in (7) and its simulation results for entropy

analysis are shown in the Table 1. If the result of MD is high, then the encrypted image quality will be low or the OI and EI are entirely different.

$$\mathbf{MD = MAX}|X_{i,j} - Y_{i,j}| \quad (7)$$

Where $X_{i,j}$an original image and $Y_{i,j}$ is an encrypted image at i and j co-ordinates.

4.1.8. Image Fidelity (IF)

Image fidelity is used to find the accuracy of the decryption algorithm to pull back the original image from an encrypted image without any distortion or information loss. The results of image fidelity are listed in the Table 1.

4.1.9. Structural Similarity Index Metric (SSIM)

SSIM is calculated by using the equation (8) and its result for the proposed scheme is shown in the Table 1 SSIM is used to measure the similarity between the two images. In this paper, SSIM is used to measure the similarity between the original image and an encrypted image. SSIM can have its value from 0 to 1. If SSIM = 0, then both the images are dissimilar. If SSIM = 1, then the two images are same [34]. From Table 1, it is observed that all the values for SSIM are almost equal to 0, which means that both the original and an encrypted images are completely different.

$$\text{SSIM}= \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(x^2+\sigma_y^2+c2)} \quad (8)$$

Where

$$\mu_x = \frac{1}{\mathbf{MN}}\sum_{i=1}^{MN} X_i \,,\ \mu_y = \frac{1}{\mathbf{MN}}\sum_{i=1}^{MN} Y_i \,,$$
$$\sigma_x^2 = \frac{1}{\mathbf{MN}}\sum_{i=1}^{MN}(X_i-\mu_x)^2 \,,\ \sigma_y^2 = \frac{1}{\mathbf{MN}}\sum_{i=1}^{MN}(Y_i-\mu_y)^2,$$
$$\sigma_{xy} = \frac{1}{\mathbf{MN}}\sum_{i=1}^{MN}(X_i-\mu_x)(Y_i-\mu_y)$$

4.2. Differential Analysis

A small change in an original image should cause a substantial change in an encrypted image is a desirable property for any efficient encryption algorithm. Differential analysis is used to test the amount of change in an encrypted image with respect to a small change in its original image. Number of Pixel Change Rate (NPCR) and Unified Average Changed Intensity (UACI) are the two image quality metrics used widely to measure the strength of an encryption algorithm against the differential attack. The value of these metrics will be zero, if both the original and an encrypted image are same [3, 18, 24].

4.2.1. Number of Pixel Change Rate (NPCR)

$$\text{NPCR}= \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} D_{i,j}}{\mathrm{N}*\mathrm{N}} \times 100\% \quad (9)$$

Where

$$\mathrm{D}_{i,j} = \begin{cases} 0, & \text{if } \mathbf{C1}\,(\mathbf{i},\mathbf{j}) = \mathbf{C2}\,(\mathbf{i},\mathbf{j}) \\ 1, & \text{if } \mathbf{C1}\,(\mathbf{i},\mathbf{j}) \neq \mathbf{C2}\,(\mathbf{i},\mathbf{j}) \end{cases}$$

$C1_{i,j}$ and $C2_{i,j}$ are an original image and its encrypted image of size N×N.

NPCR measures the number of pixels which has changed its value in the encrypted image, when one pixel value is altered in its respective original image. NPCR is calculated using (9). If the percentage of NPCR is high, then the encryption algorithm is robust against differential attack. The NPCR results of the proposed algorithm is shown in the Table 1. For all the five medical images, the NPCR value is 100% and it is concluded that a trivial change in original image will results in an entirely different encrypted image.

4.2.2. Unified Average Changed Intensity (UACI)

UACI is computed using equation (10) to determine the average intensity difference between the two images (OI and EI) [3, 18, 24]. UACI results are shown in Table 1 and it demonstrates that the proposed algorithm yields acceptable values.

$$UACI = \frac{1}{MN}\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}|C1_{i,j} - C2_{i,j}|}{255} \times 100\% \quad (10)$$

Where
$C1_{i,j}$ and $C2_{i,j}$ - original image and its encrypted image of size N×N.
255 denotes the largest pixel value.

From Table 1, the values of NPCR and UACI demonstrates that this algorithm has strong resistance against differential attacks.

4.3. Sensitivity Analysis

4.3.1. Key space Analysis

The proposed algorithm make use of large key size which is same as that of its original image. The ACM parameters P, Q, number of iterations and the seed value for generating the random numbers are all sufficiently large to make the brute force attack infeasible.

4.3.2. Key Sensitivity

The key sensitivity property of the proposed chaotic crypto encryption system is tested by changing the key used for encryption is shown in Figure 5(a), the same key is used in decryption with a small change in the value of P is shown in the Figure 5(b), Q in Figure 5(c), seed value for generating the random numbers in Figure 5(d), and changing one pixel value in original image in Figure 5(e). Images in the Figure 5 reveals the sensitivity of the proposed chaotic crypto encryption scheme, which is not able to decrypt the original image. Only with the actual key and its parameters, original image can be decrypted by the receiver.

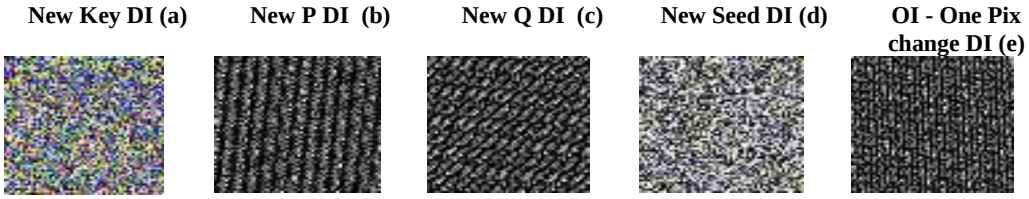

Figure 5: Decrypted Images after changing the key, P, Q, Seed and One pixel in OI

Table 1 Results attained by the proposed Chaotic Crypto medical image encryption algorithm

IM No.	MSE	PSNR	NPCR%	UACI	CORRELATION FOR OI & EI (r_{xy})		ENTROPY FOR OI, CI and DI			SSIM	MAE	MD	IMAGE FIDELITY
					HORI	DIAG	OI	CI	DI				
1	11408.85	7.5584	100.00	48.8089	-0.0282	-0.0415	6.8017	7.5839	6.8013	0.0065	58.2339	253.0	-83.7218
2	12999.96	6.9914	100.00	50.8031	-0.0323	-0.1838	6.6326	7.8259	6.6334	0.0030	-5.8472	255.0	-118.0554
3	10633.23	7.8642	100.00	50.8534	0.0115	0.2324	6.6786	7.5801	6.6791	0.0100	49.5711	251.0	-73.8188
4	14969.99	6.3786	100.00	49.2822	-0.0081	-0.1767	6.0443	7.8357	6.0444	0.0121	28.0064	255.0	-105.4678
5	11220.89	7.6305	100.00	49.8846	-0.0055	0.1463	7.0319	7.8337	7.0329	0.0168	43.8781	254.0	-71.1404

5. CONCLUSIONS

A distinctive chaotic crypto technique for medical image encryption using a unique combination of Arnold Cat Map, Fibonacci sequence and One Time Pad (AFO algorithm) is proposed in this paper. Transmitted medical image is encrypted with the use of same size biometric key image. The pixels of an original and the key images are efficiently confused and diffused. The result of various image quality metrics like correlation, entropy, MSE, PSNR, NPCR, UACI, SSIM, MAE, IF are exhibited in the Table 1, which demonstrates the competence of the AFO algorithm. By observing the Figure 5, the resultant decrypted images after changing the key, P, Q, Seed and One pixel in OI indicates that the proposed algorithm is having high sensitivity towards a small change either in secret keys or in an original image.

Hence, this proposed algorithm is highly secured, robust and appropriate for real time medical image transmission.

REFERENCES

[1] Ahmed Mahmood, Charlie Obimbo, Tarfa Hamed, Robert Dony, "Improving the Security of the Medical Images", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 9, 2013

[2] Ali Soleymani, Md Jan Nordin, and Elankovan Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", The Scientific World Journal, Volume 2014, Article ID 536930, 21 pages

[3] Alireza Jolfaei, Abdol Rasoul Mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, 2010. (NPCR & UACI)

[4] A. N. Pisarchik, M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps", Physics D 237 (20) (2008) 2638_2648.

[5] Anand Joshi, Maneesha Kumari, "Encryption of RGB Image using Arnold Transform and Involutory Matrices", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 9, September 2015

[6] Asia Mahdi Naser Alzubaidi, "Color Image Encryption and Decryption Using Pixel Shuffling with Henon Chaotic System", International Journal of Engineering Research & Technology (IJERT), Issn: 2278-0181 Vol. 3 Issue 3, March - 2014

[7] Asia Mahdi Naser Alzubaidi, "Selective Image Encryption With 3d Chaotic Map", European Academic Research ,Vol. Ii, Issue 4/ July 2014

[8] B. Schneier, "Applied Cryptography Protocols, Algorithms, and Source Code", Second Ed., C. John Wiley & Sons, Inc., New York, 1996.

[9] C. Sasi Varnan, A. Jagan, Jaspreet Kaur, Divya Jyoti, Dr. D.S. Rao, "Image Quality Assessment Techniques Pn Spatial Domain", IJCST Vol. 2, Issue 3, September 2011

[10] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton, Fl, 1995.

[11] George Makris , Ioannis Antoniou, "Cryptography with Chaos", Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece

[12] Hantao Liu, Zhou Wang, "Perceptual Quality Assessment of Medical Images", Chapter in *Encyclopedia of Biomedical Engineering*, Elsevier, 2018

[13] Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04

[14] Junqin Zhao, Weichuang Guo, Ruisong Ye , "A Chaos-based Image Encryption Scheme Using Permutation-substitution Architecture", International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 4 – Sep 2014

[15] Ljupco Kocarev, Shiguo Lian, "Chaos – Based Cryptography Theory, Algorithms and Applications", Springer-Verlag Heidelberg, 2011.

[16] Khalid Hamdnaalla, Abubaker Wahaballa, Osman Wahballa, "Digital Image Confidentiality Depends Upon Arnold Transformation And Rc4 Algorithms", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:13 No:04

[17] Kirti V.Thakur, Omkar H.Damodare and Ashok M.Sapkal, "Identification Of Suited Quality Metrics For Natural And Medical Images", Signal & Image Processing : An International Journal (SIPIJ) Vol.7, No.3, June 2016

[18] M. Manju, P. Abarna, U. Akila, S. Yamini, "Peak Signal to Noise Ratio & Mean Square Error Calculation for Various Images using the Lossless Image Compression in CCSDS Algorithm", International Journal of Pure and Applied Mathematics, Volume 119 No. 12 2018, 14471-14477

[19] *Musheer Ahmad and Tanvir Ahmad, "*A Framework to Protect Patient Digital Medical Imagery for Secure Telediagnosis*", Elsevier, Procedia Engineering 38 (2012) 1055 – 1066*

[20] Narges Mehran, Mohammad Reza Khayyambashi, "Performance Evaluation of Authentication-Encryption and Confidentiality Block Cipher Modes of Operation on Digital Image", *I. J. Computer Network and Information Security,* 2017, 9, 30-37

[21] Osama M. Abu Zaid , Nawal A. El-Fishawy, E. M. Nigm , Osama S. Faragallah, "A Proposed Encryption Scheme Based On Henon Chaotic System (PESH) For Image Security", *International Journal Of Computer Applications (0975 – 8887) Volume 61– No.5, January 2013* 29

[22] Ranvir Singh Bhogal, Baihua Li , Alastair Gale and Yan Chen, "Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard", *I.J. Information Technology and Computer Science,* 2018, 8, 1-10

[23] Ravi Kumar, Munish Rattan, "Analysis of Various Quality Metrics for Medical Image Processing", *International Journal Of Advanced Research In Computer Science And Software Engineering 2 (11), November- 2012, Pp. 137-144*

[24] S. Rajkumar And G. Malathi, "A Comparative Analysis on Image Quality Assessment for Real Time Satellite Images", Indian Journal Of Science And Technology, *Vol 9(34), Doi: 10.17485/Ijst/2016/V9i34/96766, September 2016*

[25] Ruisong Ye, Yuanlin Ma, "A Secure and Robust Image Encryption Scheme Based on Mixture of Multiple Generalized Bernoulli Shift Maps and Arnold Maps", I. J. Computer Network and Information Security, 2013, 7, 21-33

[26] Sachin Kumar, Rajendra K. Sharma, "Securing Color Images Using Two-Square Cipher Associated with Arnold Map", Multimedia Tools Appl , 29 March 2016, © Springer Science+Business Media New York 2016

[27] Shrija Somaraj and Mohammed Ali Hussain, "Performance and Security Analysis for Image Encryption using Key Image", Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/73141, December 2015*

[28] T. Venkat Narayana Rao, A. Govardhan, "Assessment of Diverse Quality Metrics for Medical Images Including Mammography", *International Journal Of Computer Applications (0975 – 8887) Volume 83 – No4, December 2013*

[29] Waleed Khalid Abduljabbar, Syariza Abdul-Rahman, Razamin Ramli, "A New Processing of Chaos-Based Fast Image Encryption Algorithms", Journal of Theoretical and Applied Information Technology 15th June 2017. Vol.95. No 11

[30] Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson, Fifth Impression, 2012

[31] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice-Hall of India, Fourth Edition, 2007.

[32] Xin Ma, Chong Fu, Wei-min Lei, Shuo Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process", International Journal of Advancements in Computing Technology Volume 3, Number 5, June 2011

[33] Xingyuan Wanga, Siwei Wanga, Yingqian Zhangb, And Kang Guoa, "A Novel Image Encryption Algorithm Based On Chaotic Shuffling Method", Information Security Journal: A Global Perspective 2017, Vol. 26, No. 1, 7–16

[34] Yusra A. Y. Al-Najjar, Dr. Der Chen Soong, "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI", International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012 ISSN 2229-5518

[35] V. Praneeth Kumar Reddy and Annis Fathima A, Stegano-Cryptography for Secured Transmission of Medical X-ray Images using Chaotic Maps., *International Journal of Mechanical Engineering and Technology*, 9(10), 2018, pp. 784–798

[36] Bhagya Maybel J and A. Umamakeswari, Hardware Implementation of Secure Image Transmission in Raspberry PI, *International Journal of Mechanical Engineering and Technology*, 9(2), 2018, pp. 670–678

[37] K. Muralibabu, Dr. K. Ramanaidu, Dr. S. Padmanabh an and Dr. T.K. Shanthi, "Novel PAPR Reduction Scheme using Discrete Cosine Transform Based on Subcarrier Grouping in OFDM System", *International Journal of Electronics and Communication Engineering & Technology (IJECET)*, Volume 3, Issue 3, 2012, pp. 251 -257

[38] N. Hanuman Reddy, M. Vinay Kumar Reddy, K. L. Raghavender Reddy and S. Sai Satyanarayana Reddy, A Novel Approach to Medical Image Processing Quality Enabled Image Smoothing, Mixed Noise Reduction and Enhancement, *International Journal of Mechanical Engineering and Technology*, 8(12), 2017, pp. 441–446