IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Chaos Based Secure Medical Image Transmission Model for IoT-Powered Healthcare Systems

To cite this article: Sujarani Rajendran and Manivannan Doraipandian 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1022** 012106

Chaos Based Secure Medical Image Transmission Model for IoT- Powered Healthcare Systems

Sujarani Rajendran[1], **Manivannan Doraipandian**[2]
[1]Department of Computer science, SASTRA Deemed University, Kumbakonam 612001, India
[2]School Of Computing, SASTRA Deemed University, Thanjavur613401 , India
Email- rsujarani@src.sastra.edu, dmv@cse.sastra.edu

Abstract. Due to the extensive development of Internet of Things (IoT) in e-healthcare environment, security and integrity of the medical data especially medical images became a big issue. This paper proposes a chaotic security architecture for ensuring the security of the medical images during transmission and storage. The proposed model is built by comprising of three main stages. At first, message digest 5 algorithm is applied to the plain image for generating the seed key of Lorenz chaotic map. Subsequently Lorenz map is iterated to generate the chaotic key series utilized for further process. In second stage, dual confusion such as row-by-row and column-by-column confusion is executed on the plain image. At last, dual diffusion process is performed by applying binary reverse and compliment operation, in addition to that XOR operation is executed between diffused image and Lorenz chaotic key image. Simulation results and analysis of security level by applying different attacks indicates that the developed cryptosystem has the potential of satisfying the security requirements of IoT healthcare applications.

Keywords: Health care system, IOT application, medical image, diagnosis, e-healthcare.

1. Introduction

Internet of Things (IoT) leads the next generation of digital communication revolution. IoT applications are expanding at a rapid rate in almost all key sectors like military, government, education, security, surveillance, banking system and healthcare[1]. Medical images plays a vital role for diagnosing the disease in IoT base e-healthcare application, so transmission of medical images over network and storage in cloud based services becomes crucial. Therefore, it is essential to build up an effective model to ensure the confidentiality and integrity of patient's medical images which are transmitted and stored in IoT environment[2]. Security architecture of medical image are expected to accomplish strong degree of resistance to withstand against different attacks, at the same time quality of the medical image should not be comprised, because a small changes in medical images might result in irrevocable wrong diagnosing. Traditional encryption systems like MD5, RC5, DES and AES has been used for protecting medical image, however these cryptosystems are proved as inefficient for protecting images due to huge pixel capacity and high correlation among pixels[3]. Consequently, chaotic map based cryptosystem has been proved as a desirable one for protecting images. Numerous researchers identified that the chaotic cryptography is one of the recent technology which is completely opt for image cryptosystem. Different directions and techniques of chaos based image cryptosystem is discussed in the state of the arts [4–6]. Some of the chaos based medical image cryptosystem is briefly given below.

Dagadu et.al [7] proposed an efficient medical image cryptosystem by utilizing Bernoulli shift map for pixel permutation and the chaotic series used for select the rule for DNA code to execute substitution process . Ravichandranet. al [8] developed a new two fusional 1D chaotic maps for extensively confuse the pixels and XOR operation is utilized for diffusing the image. Different attack analysis visualized the efficiency and security of the cryptosystem. Sathishkumar et.al [9] utilized 1D Bernoulli map and logistic map for seed key generation and to generate chaotic series for executing diffusion operation, in this cryptosystem images are read in the form of zigzag order and divided into 8 x 8 blocks and then confusion and diffusion is applied on each blocks for encrypting the medical image. Shahzadi et al.[10]presented a secure medical image protocol by combining RC5 and 2D chaotic map. Chaotic series generated by 2D chaotic map is utilized as round keys in RC5 algorithm. Experiments and analysis results of that cryptosystem demonstrated the strength of that algorithm.

Most of the medical image cryptosystem discussed above are utilized 1D map for generating the chaotic sequence applied for confusion and diffusion stage. Eventhough 1D map has its own merits due to its lower key size and limited life of randomness, it may cause threats to the security of the images [3]. As a consequence, higher dimensional map became popular among researchers and different cryptosystem has been developed using multi-dimensional map. Chen et.al [11]developed a medical image cryptosystem by employing four dimensional (4D) Lorenz chaotic map and also they proposed the new hierarchical diffusion to increase the security level. Three and four dimensional chaotic maps are found to possess good chaotic properties with larger key space. Chai et.al[12] proposed a novel 4D memristive chaotic map and they designed a new Latin square based confusion and bi-directional diffusion process for implementing in medical image cryptosystem. Based on this motivation of using higher dimensional map for developing medical image cryptosystem. We have developed a new chaos based medical crypto model by utilizing three dimensional (3D) Lorenz chaotic map which have sufficient key space and longer chaotic behaviour which will enhance the security of the image, a dual confusion and diffusion process of the proposed model greatly decrease the correlation among pixels of the medical image. Security analyses has been executed by employing different attacks and the results indicates the efficiency and security of the developed cryptosystem.

The paper framed as follows. Section 2 described the basics of the developed cryptosystem. Detailed description of the proposed design is given in section 3. Simulation results are shown in section 4. Different security analysis and comparison are evaluated in section 5. Section 6 concluded the proposed work.

2. Preliminary Concept

2.1 *3D Lorenz chaotic map*

One of the three coupled dynamic equations which having good chaotic behaviour is 3D Lorenz map [13]. This map is highly sensitivity to initial conditions and the constant value of system parameters. The mathematical form of the Lorenz map is defined in equation (1).

$$\begin{matrix} du = \alpha(v-u) \\ dv = u(\beta - w) \ - v \\ dw = (uv - \gamma w) \end{matrix} \begin{cases} 0 < u, v, w < 1 \\ \alpha = 10 \\ \beta = 28 \\ \gamma = 8/3 \end{cases} \qquad (1)$$

The Lorenz map consist of six seed keys, three initial conditions (u_0, v_0, w_0) and three control parameters (α, β, γ). Lorenz map generate the chaotic sequence is in the pure chaotic state only when these six seed values should be in the specified range. The chaotic attractors of each combination of xyz plane is shown in figure.1 which demonstrates the chaotic behaviour of the Lorenz map.

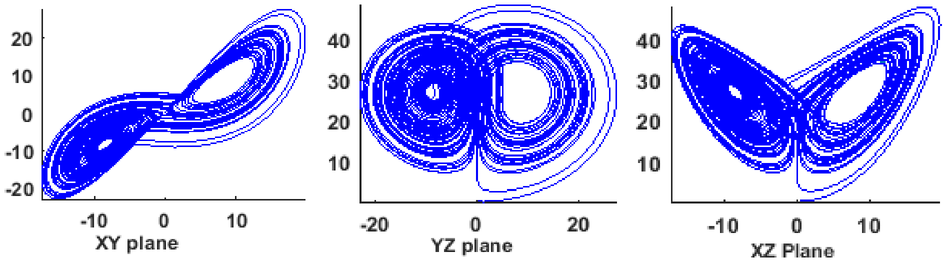

Figure1. Chaotic attractors of each plane of 3D Lorenz chaotic map.

3. Proposed Cryptosystem

The proposed model is the combination of three phases: seed key generation using MD5, dual confusion and diffusion process. The architecture of the proposed model can be visualized in figure.2. At first, Seed keys of Lorenz map is created by using the plain image, 128-bit has key and external key values. Subsequently these seed keys are taken as initial values for the Lorenz map and chaotic series are generated which are utilized for further process. The step by step structure of seed key generation, confusion and diffusion process is given as follows.

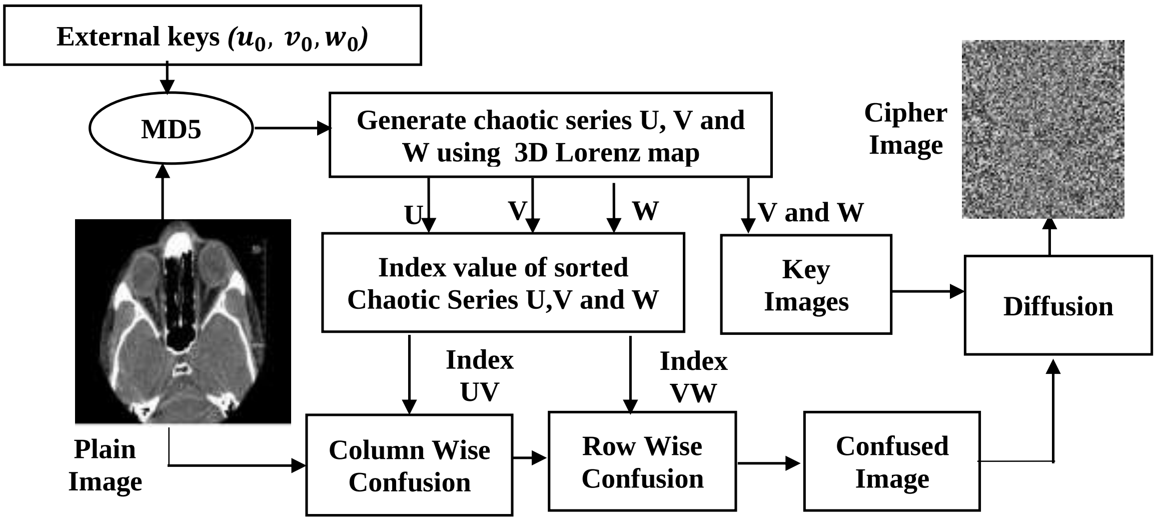
External keys (u_0, v_0, w_0)
MD5
Generate chaotic series U, V and W using 3D Lorenz map
U
V
W
V and W
Cipher Image
Index value of sorted Chaotic Series U,V and W
Key Images
Diffusion
Index UV
Index VW
Plain Image
Column Wise Confusion
Row Wise Confusion
Confused Image

Figure 2. Block diagram of the proposed medical image security architecture.

3.1 Seed key generation

Step 1 : Get the Plain Image PI with size L and B which represents length and breadth of the image.

Step 2 : Execute MD5 algorithm on PI to attain a 128 bit hash key, The obtained hash value by applying MD5 to figure 4(a) is given below.

Hash Value = ae32dfb845509201a2052bbe8a520e34

Step 3 : Split the has value into four blocks and execute XOR operation between each block to obtain three blocks of hex values, then convert the obtained hex values into integer form. Finally the integers are converted into decimal form for executing XOR operation with external seed keys. The following figure 3 demonstrate the conversion of has value to integer form.

Step 4: Convert integer form of hash values to decimal form by taking the maximum precision of 10^{-14} as given in equation (2).

$$key_1 = k1 \times 10^{-14} \quad key_2 = k2 \times 10^{-14}$$
$$key_3 = k3 \times 10^{-14}$$
(2)

Step 5:$\{u_0, v_0, w_0\}$ are considered as external seed keys of Lorenz map to generate chaotic series, then for each specific medical image, the new seed keys $\{u_0', v_0', w_0'\}$ are generated using equation (3).

$$u_0' = (u_0 + key_1) mod\,1 \quad v_0' = (v_0 + key_2)\, mod\,1$$
$$w_0' = (w_0 + key_2)\, mod\,1 \qquad (3)$$

From equation (2 and 3) it can be found that the seed keys $\{u_0', v_0', w_0'\}$ depends on the plain image. If there is a difference in just one bit of the plain image, then MD5 produces an entirely different hash value. Hence, our proposed cryptosystem is highly sensitive to the original image, it can withstand differential attack.

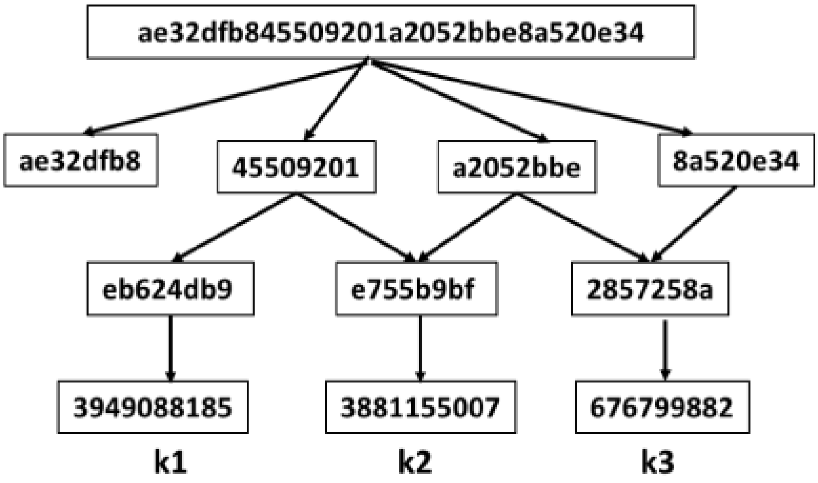

Figure3. Conversion of hex-hash value to integer form.

3.2 Confusion phase

Step 1 :Input Image (PM) and three key series $U=\{u_1,u_2,u_3,\dots\dots\ u_{size}\}V=\{v_1,v_2,v_3,\dots\dots\ v_{size}\}$ and $W=\{w_1,w_2,w_3,\dots\dots\ w_{size}\}$ are originated from Lorenz map depends on the seed keys $\{u_0',v_0',w_0'\}$. Where $size=(L\ \times B)/2$.

Step 2 : In ascending order chaotic series are sorted and store the new index value as given in equation (4).

$$[sortu1, indexu]=sort(U)$$

$$[sortv1, indexv]=sort(V)$$

$$[sortw1, indexw]=sort(W)(4)$$

Step 3 : At first, Shuffle the pixels column wise using U, V chaotic series, and again the resultant image is shuffled based on row wise using V and W chaotic series. The pseudocode for the confusion process given in table 1.

Table 1. Confusion procedure

Column wise confusion	Row wise confusion
For i = 1: L	*For i = 1: L*
For j = 1: B	*For j = 1: B*
Temp = PI(i, j)	*Temp = CPI(j, i)*
PI(i, j) = PI(indexu(i), indexv(j))	*CPI(j, i) = CPI(indexv(j), indexw(i))*
PI(indexu1(i), indexv1(i)) = Temp	*CPI(indexv(j), indexw(i)) = Temp*
End	*End*
End	*End*
CPI = PI	*CIM= CPI*
	(CIM = Confused Image)

3.3 Diffusion Process

Input: Confused image CIM, Key streams V and W.

Output: Final encrypted image EIM.

Step1: Transform the decimal form chaotic series into integer form and store it as a two-dimension array that is taken as key image with the size equal to the image. The creation of key1 is depicted in equation (5).

$$
\begin{aligned}
Key1_{i,j} &= ((V \times 10^{14}) mod\ 256\ \ if((j\ mod\ 2) == 0) \\
Key1_{i,j} &= ((W \times 10^{14}) mod\ 256\ \ if\big((j\ mod\ 2)\ ! = 0\big)
\end{aligned}
\qquad (5)
$$

Step 2: Execute bitwise reverse and compliment of each pixel of CIM, further the XOR operation is executed between the resultant image and key image as depicted in equation (6).

$$
\begin{gathered}
DIM = bitwise_{reverse_{compliment}}(CIM) \\
EIM = DIM \oplus CIM
\end{gathered}
\qquad (6)
$$

Here, DIM specified Diffused image and EIM specified Final Encrypted image. Assumed that the external keys hash values are shared between sender and receiver in secured manner. In receiver side, the decryption process is executed as the entire reverse process of the encryption algorithm, seed key generation is common in both process.

4. Experimental result

The developed cryptosystem is executed in the platform of Matlab 2016a. Samplesare shown in figure.4 with size 256 x 256. For considering the time efficiency and compatibility we have used .jpg format images instead of DICOM. The chosen key for the experimental purpose is $u_0 = 0.54678543467876$, $v_0 = 0.23456592028475$, $w_0 = 0.32456543428475$. We have taken the same constant value for α, β andγ. First the chaotic series are generated and after the confusion process is executed to get the confused image and finally the diffusion process is executed to obtain the final encrypted image. The result of the developed cryptosystem is illustrated in figure 4.

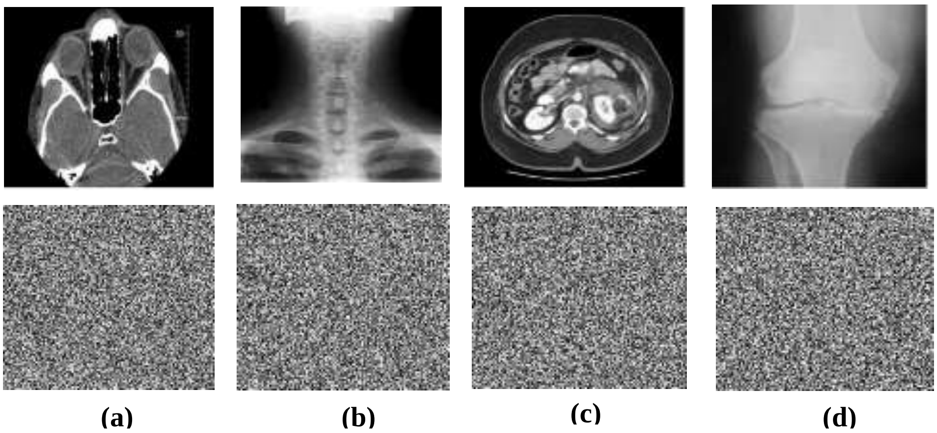

Figure 4. Experimental results First row shows the original image and second row shows its corresponding cipher image

5. Performance and Security Analysis

A good cryptosystem must be able to withstand against different attacks. Security level of the cryptosystem can be identified by different attack analyses like correlation coefficient, histogram and entropy analysis[14]. These analyses are used to identify the randomness of the encrypted image achieved by the developed cryptosystem. Robustness level can be identified by applying cipher attack analyses. These analyses are executed and the results are discussed in the following subsections.

5.1 Histogram analysis

One of the best way to evaluate the uniform distribution of encrypted image is histogram analysis [15]. figure.5 illustrate the pixel distribution of original and encrypted image in graphical form for figure.

4(a). On observing the diagram, it can be clearly recognized that the pixelsuniformly distributed in cipher image, so the proposed architecture strongly resists the statistical attacks.

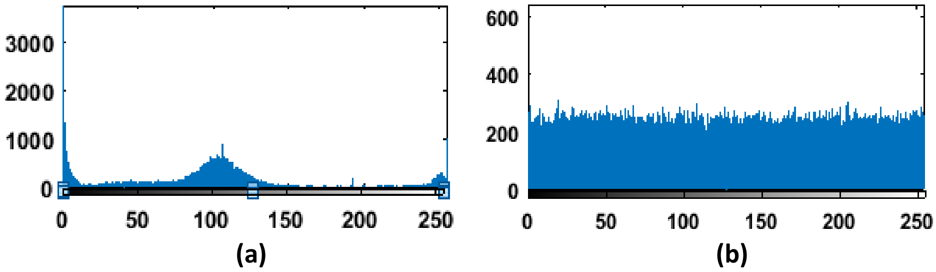

Figure 5. Histogram analysis. Histogram of (a) Original image (b) Cipher

5.2 Correlation Coefficient Analysis

Correlation among pixels in medical image is always high[16]. A good cryptosystem should greatly decrease such correlation among the pixels. The effective method to identify the level of correlation is to execute the correlation coefficient analysis between all direction of the encrypted image. Equation (7).represents the computation and figure.6 shows the distribution of pixels in all direction of the cipher image. From figure.6 it can be recognized that the proposed scheme efficiently reduced the correlation among pixels, so it can withstand statistical attack.

$$cr_{p,q} = \frac{N.cov(p,q)}{\sqrt{\sum_{i=1}^{N}(p_i - E_p)^2 . \sum_{i=1}^{N}(q_i - E_q)^2}} \quad \text{Where} \begin{cases} E_x = \frac{1}{N}\sum_{i=1}^{N} p_i \\ cov(p,q) = E\big((p - E_p)(q - E_q)\big) \end{cases} \qquad (7)$$

Here p and q denotes the value of each pixels. Table 2 represents the Correlation results of cipher image. It can be realised that all the results are closest to 0 so the developed crypto model can withstand statistical attacks. Pictorial representation of correlation in all direction of the enciphered image is shown in figure 6, which indicatesthat the proposed modelgreatly decreased the correlation. In table 2 HC, VC and DC represents Horizontal, Vertical and Diagonal Correlation. From the comparison it can be identified that the proposed system highly reduced the correlation among pixels than the state of the art.

Table 2. Correlation coefficient and Entropy results and comparison.

Test	Proposed Scheme				Enayatifar et.al [17]			
Images	HC	VC	DC	Ent	HC	VC	DC	Ent
4(a)	0.0015	-0.0013	-0.0017	7.9971	0.0032	0.0223	0.0029	7.9975
4(b)	-0.0024	-6.18e-^{04}	0.0036	7.9972	-0.0019	0.0132	-0.0042	7.9973
4(c)	0.0020	0.0049	0.0015	7.9969	-0.0002	0.0176	-0.0071	7.9970
4(d)	-0.0076	0.0049	-0.0034	7.9971	-0.0016	0.0239	0.0002	7.9969

5.3 Information Entropy

Uncertainties is an essential features of randomness and it can be identified by entropy analysis [18].The common entropy value for the random image is accurately 8. So, if any cryptosystem achieved the result of entropy as nearest to 8 then it can withstand against linear attacks. Entropy of the encrypted image is computed by employing the equation. (8).

$$ENT(I) = \sum_{k=0}^{L} P(PI_k) log_2 \frac{1}{P(PI_k)} \qquad (8)$$

PI_krepresents the k^th pixel value of L size medical image. $P(PI_k)$means the probability of (PI_k). The entropy value of encrypted medical image and it's comparison is shown in table 2. From the result it can be realized that all the entropy result is nearest to 8, hence the proposed cryptosystem can fight against linear attacks.

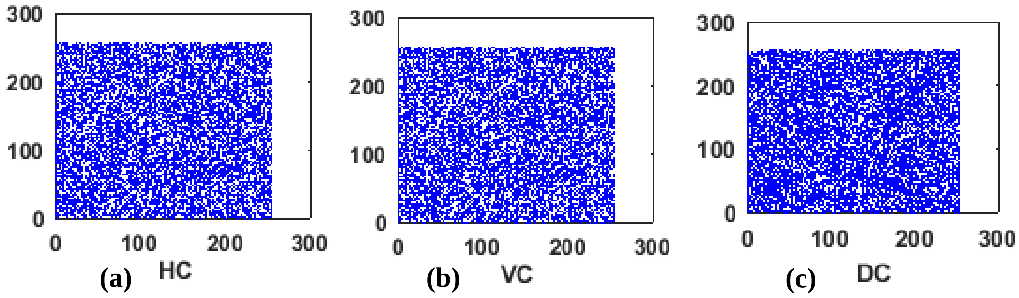

Fig. 6 Correlation Coefficient Analysis in all the three directions

5.4 Key Space and Key Sensitivity Analysis

The proposed model is developed with the intent of overcoming the drawback of lesser key space in chaotic based cryptosystem, so that we have utilized 3D Lorenz chaotic map which have three seed keys and three system parameters. If the size of each key set to its maximum range with the precision of value of 10^{-14}, then we get 10^{-42} seed key size and MD 5 128 bit key is also taken as secret key. Thus, the key size is sufficient to withstand brute force attack. Apart from the key size, key sensitivity is an essential element for building a cryptosystem. A robust image cipher should be more sensitive to the keys [19,20]. A small change in key set produces an entirely different cipher image. To illustrate key sensitivity, test image figure 4(a) is encrypted with two-keys having minor differences. The decryption result of the two cipher images are shown in figure 7. Hence, on analysing the figure 7 it can be concluded that the developed cryptosystem has high sensitivity to tiny changes in keys.

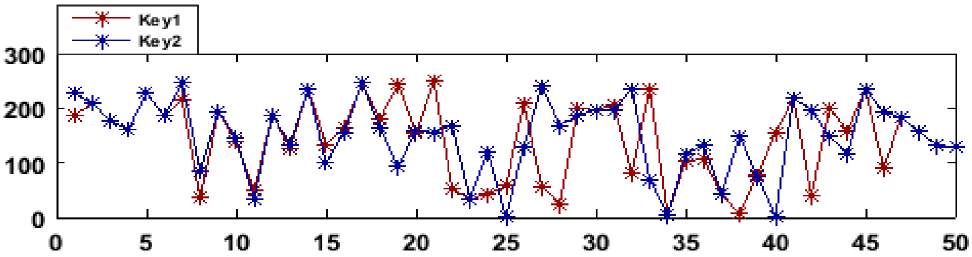

Figure7. Visualization of key sensitivity analysis.

5.5. Robustness analysis

*5.5.1 Cropped Attack Analysis***.** Robustness of the cryptosystem can be identified by analysing the result of crop attack [21]. The familiar logic for applying crop attack is to crop the encrypted image intentionally by different size. Thus the encrypted image is cropped and the resultant decrypted image is shown in figure.8. Table 3 shows the quality of decrypted image by calculating the quality metrics MSE, PSNR and Correlation between original and decrypted image. The mathematical function used to calculate the MSE and PSNR are described in equations (9 and 10). This results illustrates that our cryptosystem can withstand cipher image attack.

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j) - D/E(i,j))^2 \tag{9}$$

$$PSNR = 20\log_{10}\frac{I_{max}}{\sqrt{MSE}} \tag{10}$$

O and D indicate the Original and Decrypted image. M and N represents the image size.

*5.5.2 Noise attack analysis.*Sometimes, during transmission noises are added to the images, salt and pepper is one of the popular noise embed with the encrypted image by nature[22]. In order to prove the robustness, noise is intentionally added to the encrypted image with different densities and their corresponding decrypted image is given in figure 8 and the quality metrics values of decrypted image is given in table 3. On seeing figure 8 and table 3, it can be accepted that the developed cryptosystem withstand up to 0.01 amount of salt and pepper noise attacks.

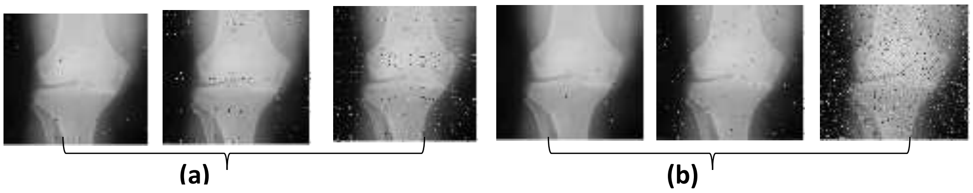

Figure 8. Robustness analysis: Decryption result of (a) cropped cipher with 0.5%, 1% and 2% (b) cipher image with noise of 0.001, 0.01,0.1.

Table 3. Quality of decrypted image against crop and noise attack analysis

Cipher Image of figure 4(d)	AFFECTED RATIO	MSE	PSNR	CORRELATION
Crop attack:	0.5%	39.51	32.16	0.9962
	1.0%	104.96	27.92	0.9900
	2%	357	22.60	0.9661
Salt & pepper noise	0.001	6.40	40.06	0.9994
	0.01	112.54	27.61	0.9893
	0.1	1.07e^{03}	17.83	0.8989

6. Conclusion

A new chaotic map based medical image cryptosystem has been developed in this paper by utilizing 3D Lorenz map. Seed key values are generated by using MD5, so the proposed model has high degree of integrity. Dual confusion and diffusion process increased the degree of security and confidentiality of the medical images which is transmitted over network on IoT healthcare environment. So in IoT powered Telemedicine patient's medical images are securely communicated between Doctors and patients by calculating the encryption keys using their authentication attributes. So there is no need for sharing the external key separately. We executed statistical, key size, cipher image attack analyses to illustrate the level of security of the proposed cryptosystem. The results conclude that the proposed one satisfied the expected level of security for secure transmission and storage of medical images in real time online medical application.

References

[1] Wazid M, Das A K, Hussain R, Succi G and Rodrigues J J P C 2019 Authentication in cloud-driven IoT-based big data environment: Survey and outlook *J. Syst. Archit.***97** 185–96

[2] Fu C, Meng W hong, Zhan Y feng, Zhu Z liang, Lau F C M, Tse C K and Ma H feng 2013 An efficient and secure medical image protection scheme based on chaotic maps *Comput. Biol. Med.***43** 1000–10

[3] Rajendran S, Krithivasan K and Doraipandian M 2020 Fast pre-processing hex Chaos triggered color image cryptosystem *Multimed. Tools Appl.* 12447–69

[4] Mollaeefar M, Sharif A and Nazari M 2017 A novel encryption scheme for colored image based on high level chaotic maps *Multimed. Tools Appl.***76** 607–29

[5] Hu T, Liu Y and Ouyang C 2017 An image encryption scheme combining chaos with cycle operation for DNA sequences *Nonlinear Dyn.***87** 51–66

[6] Rajendran S and Doraipandian M 2018 Biometric template security triggered by two dimensional logistic sine map *Procedia Comput. Sci.***143** 794–803

[7] Fu C, Meng W hong, Zhan Y feng, Zhu Z liang, Lau F C M, Tse C K and Ma H feng 2013 An efficient and secure medical image protection scheme based on chaotic maps *Comput. Biol. Med.***43** 1000–10

[8] Ravichandran D, Praveenkumar P, Balaguru Rayappan J B and Amirtharajan R 2016 Chaos based crossover and mutation for securing DICOM image *Comput. Biol. Med.***72** 170–84

[9] Sathishkumar G A, Bhoopathybagan K, Sriraam N, Venkatachalam S P and Vignesh R 2011 A novel image encryption algorithm using two chaotic maps for medical application *Commun. Comput. Inf. Sci.***133 CCIS** 290–9

[10] Shahzadi R, Anwar S M, Qamar F, Ali M and Rodrigues J J P C 2019 Chaos based enhanced rc5 algorithm for security and integrity of clinical images in remote health monitoring *IEEE Access***7** 52858–70

[11] Chen J, Chen L, Zhang L Y and Zhu Z liang 2019 Medical image cipher using hierarchical diffusion and non-sequential encryption *Nonlinear Dyn.***96** 301–22

[12] Chai X, Zhang J, Gan Z and Zhang Y 2019 Medical image encryption algorithm based on Latin square and memristive chaotic system *Multimed. Tools Appl.***78** 35419–53

[13] Kumari K A, Akshaya B, Umamaheswari B, Thenmozhi K, Amirtharajan R and Praveenkumar P 2018 3D lorenz map governs DNA rule in encrypting DICOM images *Biomed. Pharmacol. J.***11** 897–906

[14] Rajendran S, Abilashaa S and Doraipandian M 2019 Elliptic curve blended cross chaos based secure image communication *Int. J. Recent Technol. Eng.***8** 4481–4

[15] Chai X, Fu X, Gan Z, Lu Y and Chen Y 2019 A color image cryptosystem based on dynamic DNA encryption and chaos *Signal Processing***155** 44–62

[16] Stalin S, Maheshwary P, Shukla P K, Maheshwari M, Gour B and Khare A 2019 Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences (NL4DLM_DNA) *J. Med. Syst.***43**

[17] Nematzadeh H, Enayatifar R, Motameni H, Guimarães F G and Coelho V N 2018 Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices *Opt. Lasers Eng.***110** 24–32

[18] Chai X, Zheng X, Gan Z and Chen Y 2020 Exploiting plaintext-related mechanism for secure color image encryption *Neural Comput. Appl.***32** 8065–88

[19] Gong L, Qiu K, Deng C and Zhou N 2019 An image compression and encryption algorithm based on chaotic system and compressive sensing *Opt. Laser Technol.***115** 257–67

[20] Ali T S and Ali R 2020 A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map *IEEE Access***8** 71974–92

[21] Chai X, Fu X, Gan Z, Lu Y and Chen Y 2019 A color image cryptosystem based on dynamic DNA encryption and chaos **155** 44–62

[22] Babaei A, Motameni H and Enayatifar R 2020 A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence *Optik (Stuttg).***203**