Medical Image Encryption Into Smart Healthcare IOT System

Conference Paper · December 2019

DOI: 10.1109/ICCWAMTIP47768.2019.9067592

CITATIONS
16

READS
301

9 authors, including:

Jalaluddin Khan
Koneru Lakshmaiah Education Foundation
51 PUBLICATIONS **1,495** CITATIONS
SEE PROFILE

Ghufran Ahmad Khan
Southwest Jiaotong University
37 PUBLICATIONS **695** CITATIONS
SEE PROFILE

Mohammad Shahid
National Taiwan University of Science and Technology
18 PUBLICATIONS **420** CITATIONS
SEE PROFILE

Happy Nkanta Monday
Oxford Brookes College of Chengdu University of Technology
50 PUBLICATIONS **574** CITATIONS
SEE PROFILE

MEDICAL IMAGE ENCRYPTION INTO SMART HEALTHCARE IOT SYSTEM

JALALUDDIN KHAN[1], JIANPING LI[1], AMIN UL HAQ[1], SHADMA PARVEEN[2], GHUFRAN AHMAD KHAN[3], MOHAMMAD SHAHID[1], HAPPY N. MONDAY[1], SANA ULLAH[4], SUN RUINAN[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054，China

[2]School of Management and Economics, University of Electronic Science and Technology of China, Chengdu 610054，China

[3]School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China

[4]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu

E-MAIL: jalal4amu@yahoo.com*, jpli2222@uestc.edu.cn, khan.amin50@yahoo.com, yourshadma@yahoo.com, ghufraan.alig@gmail.com, shahidinsy@yahoo.com, mh.nkanta@gmail.com, sanaullah.cs@fuuast.edu.pk, rui-nan@outlook.com

Abstract:

The security and privacy of medical data are highly required when it involved in connecting with smart and intelligent sensor devices in the hospital ecosystem. The Internet of things is mutually integrated with healthcare to produce effective and smart working system but it still needs better security mechanism which can protect patient's privacy. This paper is focusing to protect medical data by using image encryption techniques. In which we are applying three rounds of high-speed scrambling as well as pixel adaptive diffusion concept for shuffling random neighboring pixels. In addition, implementing pixel adaptive diffusion our mechanism is used modulo arithmetic operation. Simulations and experiments demonstrate that the encryption mechanism employing modulo arithmetic operation have comparatively higher levels of security. It can adapt better than several traditional as well as state-of - the-art image encryption.

Keywords:

Medical data; Information security; Privacy; Encryption

1. Introduction

Digital medical images play an increasingly important role in the diagnosis and treatment of diseases in modern hospitals which is operated mutually with internet of things ecosystem and therefore attract increasing attention [1-3]. These medical images can generally contain a lot of patients privacy and some of them are very sensitive as well as confidential. Disastrous accidents can occur when unauthorized accesses rob, view or use these private images. A malicious database administrator or hacker, for example, may utilize unauthorized medical images for their personal paybacks, for instance fraudulent claims for insurance and medical marketing, which may highly threatening risk of life. It is therefore very important to protect medical images[4].

In order to secure each types of images, for example medical images, many technologies have been developed so far. Encryption is among these technologies the most spontaneous and efficient means of transforming images into unrecognized patterns [5-9]. Only with the enforcing right (secret) key, can the original image be recovered efficiently [10]. Several image encryptions schemes have recently been proposed which can be used to protect high-security medical images [11].

Farah et al. [6] proposed encryption mechanism by implementing fractional Fourier transform. His algorithm is focused on Shannon's state of diffusion and confusion. The cycle of confusion is focused on DNA sequencing and the use of DNA XOR to confuse the object pixel values. Wang et al. [7] reported scheme together with the DNA encoding rules chaotic selection process, hamming length, cyclic shift, addition of DNA, subtraction of DNA, operation of DNA XOR and other operations. The cyclic shift operation and Hamming distance are mutually combined to properly diffused images into the DNA level. Wang et al. [12] reported in his article for medical image solution in terms of acquisition and transmission. He addressed that original medical image reduced to 20% and attained well confidentiality by using homomorphic aggregation.

Ghoneim et al. [13] proposed new healthcare framework medical image forgery detection scheme to verify that medical images are not altered or changed. The scheme works on an image's noise map, relates a multi-resolution

regression detector to the noise map, and continues to feed throughput to classifiers based on support-vector-machine (SVM) as well as extreme-learning. The noise map is generated in an edge computation system, while a core cloud computing resource is used for filtering as well as classification. Dzwonkowski et al. [14] is addressed Quaternion-based Digital Image and Medicine Communication (DICOM) lossless encryption methodology. In which author crumbles a DICOM image in multiple 8-bit gray scale in order to achieve encryption.

This paper is contributed to address privacy and security issues in the smart healthcare system. We applied encryption method to secure medical image data. Attaining encrypted image, proposed method combined two process one is high speed scrambling and second one is adaptive pixel diffusion. It Implemented three round of these process and used arithmetic modulo operation to shuffle neighboring pixels. The proposed method showed robust and high level of security to protect medical image data.

The remaining architecture of this paper as follows: efficient proposed work discussion in the section 2. Produced result and discussion in the section 3. Brief discussion of security analysis with various parameter in the section 4 and at last conclusion with future work in the section 5.

2. Medical image encryption

The proposed medical image encryption mechanism is showing in Fig. 1, in which a plain medical image processed with effective way by using a methodology to obtain accurate cipher image in the smart healthcare IoT system. The methodology consists of key which is 256-bit long and used entire process to obtain desired results. The high-speed scrambling and diffusion operation performed three rounds simultaneously to obtain random shuffle pixel places and alteration in the pixel values as well. Performing three rounds in our proposed mechanism benefited to reach high level of security in terms of encrypted cipher medical image.

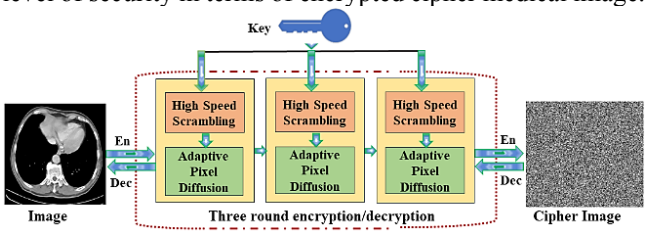

Fig.1 Medical image encryption mechanism

Functionally the encryption operation is performed like Eq(1):

$$Cipher = \text{Encryption}\left(\text{Plain Image, Key}\right) \quad (1)$$

and decryption operation can be performed like Eq (2):

$$Plain\ \text{Im}age = Decryption\left(Cipher, Key\right) \quad (2)$$

2.1. Key structure

For proposed mechanism, the stable key K is utilized to produce pseudo-random numbers. Key K is generated by using Logistic Sine System and denoted pseudo-random numbers as LSS-PRNG which is can defined by Eq (3)-

$$X_{n+1} = \left(rX_n\left(1-X_n\right)+\left(4-r\right)Sin\left(\left(\pi X_n\right)/4\right)\right) \bmod 1 \quad (3)$$

Where r is a control parameter $r \in [0,4]$ and iterative variable is X_n, $X_n \in (0,1)$. Initial state (X_0, r) and $\{X_i \mid i = 1,2,3.....\}$ is the determinates pseudo-random sequence generation. The three round generation key K consists of variables (X_0, r), U_1 and U_2 are the float in nature which will convert 52-bit stream.

$$\text{FN} = \sum_{i=1}^{52} Bin_i \times 2^{-i}$$

S_1 and S_2 two integer can be obtain as a 24-bit stream.

$$\text{IN} = \sum_{i=1}^{24} Bin_i \times 2^{i-1}$$

Three round initial state can be generated by following Eq (4):

$$\begin{cases} X_0^{\,i} = S_i \times \left(X_0 + U_i\right) \bmod 1 \\ r^i = S_i \times \left(r + U_i\right) \bmod 4 \end{cases} \quad (4)$$

Where ($i = 1,2,3.....$).

2.2. High-Speed Scrambling

High-speed scrambling method is to quickly scramble each pixel positions among the medical images. This simultaneously shifts pixel row as well as column places and can thus effectively diminish the high correlation among adjacent pixels. Initially a matrix D is created by the help of LSS-PRNG through initial state $\left(X_0^{\,i}, r^i\right)$ where i=1,2,3 for three round operation. The pixels can then be fairly uniform with D.

2.2.1. Creation of Scramble Matrix D

Suppose plain medical image has size MxN. Step 1: We need firstly two G and H vector for each M and N, implementing LSS-PRNG through initial state $\left(X_0^{\,i}, r^i\right)$.

Step 2: sorting G and H, maintaining two index vector J and I. Step 3: initiate with initial sate using size MxN, assigning individually row of matrix D as H, at last replace each row as G to obtain matrix D. Table 1 is briefly explaining high speed scrambling algorithm.

Table 1 algorithm 1 high- speed scrambling

Input	Medical image (V) Size MxN, initial state $\left(X_0^{\,i}, r^i\right)$
Output	Scramble image (Z)
	U= LSS-PRNG $\left(X_0^{\,i}, r^i\right)$
	$G=U_{1:M}$, $H=U_{(M+1):(N+1)}$
	Sort G as 'G, 'G=G_I Sort H as 'H, 'H=H_J
	Set $D \in N^{M\times N}, Z \in N^{M\times N}$
	for i=1 to M
	for j=1 to N
	$m=\left(\left(j-H\left(i\right)-1\right)\bmod N\right)+1$
	$D_{i,m}=G_j$
	end for
	end for
	for j=1 to N
	for i=1 to M
	$r=i, c=D_{i,j}$
	$m=\left(\left(r-D_{1,j}-1\right)\bmod M\right)+1, n=D_{m,j}$
	$Z_{m,n}=V_{r,c}$
	end for
	end for

2.3. Pixel adaptive diffusion

This operation is just to disperse minimal plain-image change over these cipher-image pixels. To change the overall pixel, it is executed using the former pixel and the randomized value. Arithmetic modulo operation is used as an adaptation of software environment to perform pixel adaptation diffusion process into the entire plain medical images. The proposed approach of using arithmetic modulo can be expressed by Eq (5):

$$Z_{i,j}=\begin{cases}\left(V_{i,j}+V_{M,N}+H_{i,j}\right)\bmod E & \text{case 1: if i=1,j=1,}\\ \left(V_{i,j}+Z_{M,j-1}+H_{i,j}\right)\bmod E & \text{case 2: if i=1,j}\neq 1,\\ \left(V_{i,j}+Z_{i-1,j}+H_{i,j}\right)\bmod E & \text{case 3: if i}\neq 1,\end{cases} \quad (5)$$

Where E is intensity number which is 256 if 8-bit pixel representation.

3. Result and discussion

The simmulation results of proposed mechanism using airtmetic modulo operation is performed in the MATLAB 2018a environment. Achieving the expermental work, we utilize two different medical image dataset. One is SPIE-AAPM Lung CT Challenge dataset [15] and second one is MedPix® [16]. The results are showed in the Fig 2. As the result demonstrated that the proposed approch is provided uniform pattern of the cipher image which indicated that this approach is quite acceptable to perform encryption for securing smart healthcare system.

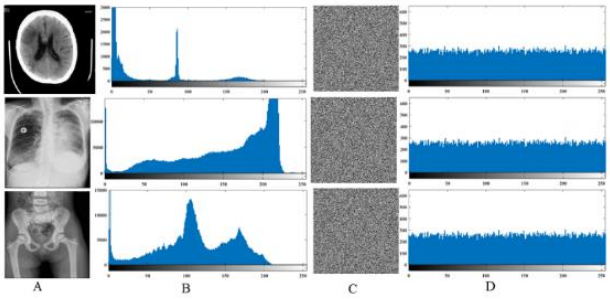

Fig.2 Simulation results of different image A) plain image, B) Histogram of Pain Image, C) Cipher image, D) Histogram of cipher image

4. Security analysis

In order to validate security aspect of the proposed mechanism. We are going to analyses in terms of information entropy, differential attack, statistical analysis and key analysis.

4.1. Information entropy

Information entropy is the analyzing tool which deals

$$H\left(m\right)=-\sum_{i=1}^{255}P\left(m_i\right)\log_2 P\left(m_i\right) \quad (6)$$

with uncertainty and randomness among the cipher image. Information entropy can be explained in Eq (6) where H(m)

is denoted as entropy in this equation and $P(m_i)$ is probability of occurrence at each m_i.

Table 2 information entropy values

Information Entropy from Medical Image	
Plain Image	Cipher Image
5.7676	7.9955

Generally, entropy of the image is 8 it means pixels are behaving uniformity in the cipher images. Table 2 demonstrated that proposed approach has approximately very near to 8 value of entropy which indicated that proposed approach has provided uncertainty and randomness in the cipher images.

4.2. Differential attack

The differential attack examines how well the ciphertexts will influence the difference between plaintexts. Differential attack can be effectively measure in the encryption mechanism with the help of NPCR (number of pixels change rate) and UACI (uniform average change intensity) quantitated values of the image. Let assume C1 and C2 are two

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \tag{7}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100 \tag{9}$$

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{8}$$

encrypted cipher image of medical plain image with a little difference then NPCR and UACI can be defined from Eq (7-9). Table 3 demonstrated NPCR and UACI value of medical image SPIE-AAPM Lung CT Challenge dataset. This indicates that our proposed mechanism has strong ability to resist various types of differiential attacks.

Table 3 NPCR and UACI values

NPCR and UACI from Medical Image	
NPCR	UACI
99.9976	33.3281

4.3. Statistical analysis

Statistical analysis consists of two type of analysis one is histogram analysis and second one is correlation analysis. Concerning histogram analysis, we can see Fig 2 D each cipher images are dispersed uniformly. It means each cipher image is very different from plain image. So, it will be very difficult to guess actual information for attacker or any adversary to see Fig 2. This demonstrated that our proposed approach is very secure from any attacker or adversary.

Concerning correlation analysis, we can measure linear relationship among the adjacent pixel of the image by using Eq (10-15). We can see Fig 2 D Which indicate that there is no relation among the adjacent pixels which is nearly zero whether positively or negatively in the values. This demonstrated that our proposed method has nearly zero correlation coefficient which showed dispersed actual relationship that have plain image.

$$CC_{xy} = \frac{\text{Covariance}(x,y)}{\sqrt{D(x)D(y)}} \tag{10}$$

$$\text{Covariance}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{11}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \tag{12}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - E(y)\right)^2 \tag{13}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{14}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{15}$$

4.4. Key analysis

The key should be more suitable and good in terms of strength to protect any kind of brute-force attack[17]. Our proposed method is used 2^{256} key length to defend any adversary or attack. This 256-bit length key is extremely sensitive as well secure to protect smart healthcare system.

5. Conclusions

The proposed method is highly reliable, efficient and robust encryption nature in smart healthcare IoT system. It is a combination of two process, high speed scrambling and adaptive diffusion method with arithmetic modulo operation.

In which both processes accurately shuffled random neighboring pixel in the cipher images which reflects as a uniformly in the encrypted cipher images. Our simulation results and security analysis acknowledge that proposed mechanism has high security standard to secure any adversary or attacker in the smart healthcare IoT system.

For future work, we will implement some more security aspect to protect digital medical data in smart healthcare system.

Acknowledgments

This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] G. Tripathi, M. Abdul, and S. Paiva, "Healthcare S2HS- A blockchain based approach for smart healthcare system," *Healthcare*, no. November, p. 100391, 2019.

[2] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," *Glob. Heal. J.*, no. xxxx, pp. 0–3, 2019.

[3] S. Tuli *et al.*, "HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments," *Futur. Gener. Comput. Syst.*, 2019.

[4] H. A. El Zouka and M. M. Hosni, "Secure IoT communications for smart healthcare monitoring system," *Internet of Things*, Jan. 2019.

[5] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[6] M. A. Ben Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Opt. Laser Technol.*, vol. 121, p. 105777, Jan. 2020.

[7] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Opt. Lasers Eng.*, vol. 125, p. 105851, Feb. 2020.

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

[9] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, Mar. 2018.

[10] M. Li, Y. Guo, J. Huang, and Y. Li, "Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure," *Signal Process. Image Commun.*, vol. 62, pp. 164–172, Mar. 2018.

[11] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, Nov. 2016.

[12] L. Wang, L. Li, J. Li, J. Li, B. B. Gupta, and X. Liu, "Compressive Sensing of Medical Images With Confidentially Homomorphic Aggregations," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1402–1409, Apr. 2019.

[13] A. Ghoneim, G. Muhammad, S. U. Amin, and B. Gupta, "Medical Image Forgery Detection for Smart Healthcare," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 33–37, Apr. 2018.

[14] M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A New Quaternion-Based Encryption Method for DICOM Images," *IEEE Trans. Image Process.*, vol. 24, no. 11, pp. 4614–4622, 2015.

[15] C. K. Justin Kirby, "The Cancer Imaging Archive (TCIA) Public Access," 2019. [Online]. Available: https://wiki.cancerimagingarchive.net/display/Public/SPIE-AAPM+Lung+CT+Challenge. [Accessed: 08-Dec-2019].

[16] "The National Library of Medicine presents MedPix®." [Online]. Available: https://medpix.nlm.nih.gov/home. [Accessed: 08-Dec-2019].

[17] G. ALVAREZ and S. LI, "SOME BASIC CRYPTOGRAPHIC REQUIREMENTS FOR CHAOS-BASED CRYPTOSYSTEMS," *Int. J. Bifurc. Chaos*, vol. 16, no. 08, pp. 2129–2151, Aug. 2006