IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Survey on Medical Image Encryption

Garima Mathur

Department of Computer Science, UIT, RGPV, Bhopal, India

Corresponding Author: garima41mathur@gmail.com, Tel.: 8871168663

DOI: https://doi.org/10.26438/ijcse/v7i4.128133 | Available online at: www.ijcseonline.org

Accepted: 11/Apr/2019, Published: 30/Apr/2019

Abstract **-** The medical industry has proceeded into the digital age thanks to the development of science and technology. Medicinal pictures which are utilized in their digital form play an important role in every modern hospital. This significant contribution is especially visible in the field of diagnosis and in the treatment of patients. The problem, however, may arise during the application of these digital data. Digital images are linked to image transmission and sharing, which bring about concerns regarding data security. The Digital Image and Communication on Medicine (DICOM) standard was created so as to encourage protected and reliable transmissions and communications. In this paper it has been surveyed about various encryption techniques that can be used for secure transmission of medical images through non-secure medium along with its advantages and disadvantages.

Keywords **-** Encryption, Medical images, DICOM, Key Sensitivity, Known Plaintext attack, Quaternion

I. INTRODUCTION

Nowadays, delivering sensitive digital multimedia contents confidentially over vulnerable public networks is a matter of high importance and encryption is a technique which is widely used for secure communication. Image encryption is one of the vital fields of cryptography and one of the outstanding algorithms used in this domain is the DES (Data Encryption Standard) algorithm which requires less time while considering the computational expenses. The digital images can be considered as a two dimensional matrix or a square array of numbers and elements of this array's are called pixels. The pixel values are digital numbers and since we can show it as a matrix that each pixel can be denoted by a position as (row, column). By encrypting an image, it is intended to apply a symmetric or asymmetric encryption algorithm on an input image in order to convert it to a cipher image using either symmetric or asymmetric keys. Symmetric ciphers uses same key for both encryption and decryption processes while asymmetric ciphers make use of two different key pairs (*i.e.*, public and private keys).

Encryption/decryption algorithms are considered strong if it can resist against most well known attacks such as known-plaintext and cipher-text only attacks. One of the most important topics in exchanging sensitive information among doctors is to provide security for medical images. The Digital Image and Communication on Medicine (DICOM) standard has been developed in order to facilitate safe and reliable transmissions and communication. For securing medical images within the DICOM system currently relies on techniques that include the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (3DES) algorithms. However, implementations of these algorithms for medical images consume substantial processing time. Additionally, a high visual quality of each medical image entails a larger file size. There is a high demand for an architecture that combines security features with a reduced delay on data access.

In this paper we present several encryption algorithms for DICOM images, based on previous work. The main contribution of this paper is to identify, analyze, and address the security flaws of various previously defined algorithms and to identify a superior version out of them.

The purpose of this paper is to present various security issues related to the transmission of medical images through a non-secure medium i.e. over the internet. The structure of the paper is as follows-Various image encryption techniques along with their advantages and disadvantages are listed in section 3. The comparison and analysis of various cryptography algorithms has been discussed in section 4. Conclusions are discussed in section 5. Further studies on the method are necessary and are highlighted in the paper.

II. LITERATURE REVIEW

The first versions of the DICOM standard did not integrate security mechanisms. As a result, sensitive data were transferred in plain text. A requirement for security measures arose during extensive use of the Internet in the medical

sector. Various image encryption techniques along with its advantages and disadvantages has been discussed below, that can be used for encryption of medical images.

In year 2008, Hill cipher algorithm has been developed as an encryption method for images at both gray and color scales [1]. But, this method is not successful on the background of images which were at the same level of color attributes.

Sokouti *et al.* [2, 3], proposed a genetic-based random key in a one-time pad (OTP) encryption system using the image bits. For encryption, the image was first split into row blocks. Because of its double-numerical nature, after the encryption process, no one will recognize whether it is an encrypted image or a text. Regardless of its random keys, OTP encryption system, and numerical nature, it will turned to be a highly secure medical image encryption system in which the security management policies should be complied with the latest security standards to keep it safe forever.

Moreover, another encryption algorithm was presented and the resulted image was significantly decreased the correlation among the elements with high entropy [1]. The method that was implemented is based on Hill cipher and since it uses matrices for encryption, so it is a suitable algorithm to be used for image encryption. In another research [4], a new method by including both permutation and encryption methodologies was proposed. The idea of this algorithm is to break the image into 4 pixels block, the permutation and encryption by RijnDael algorithm process will be performed, respectively. The result shows that the similarity between the original and encrypted images was decreased with an increasing trend on the entropy values.

In **Seyedzade *et al.*** [5], the SHA-512 hash function based on XOR operation was used for image encryption. The proposed method has only few chances of errors and also, it is a very slow algorithm.

In **Ismail IA *et al.*** [6], an algorithm for image encryption was deployed by using two chaotic logistic maps with a large 104-bit key space. This can be used to make more different pixels while the cipher and the plain images are being compared.
Because, the plain pixel depends on key and the output depends on the logistic map and hence, the confusion will be increased.

In **Kamali SH *et al.*** [7], the modified version of AES (MAES) was presented in which the security properties were highly increased in comparison to AES.

In **Indrakanti *et al.*** [8], the method is based on random pixel permutation to maintain the quality of the image with less computation, fast encryption, and high error chance. This method includes three phases which are- the image encryption, key generation, and identification process.

In **Enayatifkr *et al.*** [9], a hybrid algorithm which took the advantages of both genetic algorithm and chaotic function was presented. At the beginning stage, the first population was generated. This population includes the original image on which the chaotic function is applied. Finally, the best encryption result will be chosen.

In **Singh K *et al.*** [10], a cross chaotic maps with the incorporation of DNA was presented which had better results than a default based chaotic maps and counted as an easy and cost effective method.

In **Alsafasfeh QH *et al*.** [11], Lorenz and Rossler chaotic systems is added to their proposed work which had better and robust characteristics in terms of speed, key space, and security.

In **Abuhaiba *et al*.** [12], the encryption of an image using differential evolution is done in this approach as well as analyses was conducted on security properties such as key space analysis and statistical analysis [13].

In **Abugharsa AB *et al.*** **[**14], a method where a new AES based technique was incorporated on shifting blocks of divided images, and applying rows and columns shuffling, and then encrypting by AES algorithm with some errors in a long process.

In **Pareek NK *et al.*** [15], a non-chaos based image encryption method using external 144-bits key was presented. It incorporates the pixel permutation substitution, so, it is strong against the differential attack with a high encryption rate, less computational cost, and less changes in keys.

In **Agarwal A *et al.*** [16], a genetic algorithm based methodology was presented which had really a long process while considering its computational costs and the flowchart.
In **Bhatt V *et al.*** [17], a method comprising of the position permutation, value transformation, substitution, and transposition was represented with very slow process and high entropy.

In **2015 A new quaternion based encryption method for DICOM images** has been implemented, a method that have scrutinized and slightly modified the concept of the DICOM network which significantly improves speed of DICOM images encryption in comparison with those originally embedded into DICOM advanced encryption standard (AES) and triple data encryption standard algorithms (3-DES) [18]. The proposed algorithm splits the DICOM images into two gray-tone images of 8-bit in order to perform encryption. It uses special properties of quaternions

to perform rotations of data sequences in 3D space for each of the cipher rounds. The images are written as Lipschitz quaternions, and modular arithmetic was implemented for operations with the quaternions. This quaternion algorithm is designed to encrypt images (both color and gray-tone), but it can also be used to encrypt textual data.

In **M. Dridi *et al*.[19]**, method used for securing DICOM files is based on a chaotic–neural network. The algorithm uses a combination of a logistic map and a perceptron neural network and is more suitable for image encryption than a one dimensional chaotic system. However, Dridi *et al.* also point out some flaws of the proposed scheme, for example, periodic windows in the bifurcation diagram and a limited range of key space

In **W.Cao *et al.*[20]**, a method that uses edge maps derived from a source image for encrypting medical images. A significantly large key space and strong key sensitive are possessed by the proposed algorithm to protect different types of medical images. Experimental study and security analysis further demonstrate that it has a strong resistance against various security attacks.

In **J. Chandrasekaran *et al.*[21],** This algorithm uses the concept of modular exponentiation and Henon maps for securing DICOM images. Encryption keys are two-dimensional arrays based on modular exponentiation Henon maps are used to permute elements of the arrays. The encryption process is based on a bitwise modulo-2 operation applied to sub-images with permuted key arrays. The proposed scheme eliminates round-off errors in decryption due to modular exponentiation for key generation

In **M. Dzwonkowski *et al.*[22]** , modified version of method proposed in 2015 has been proposed in 2019 ,it is a Secure quaternion Feistel cipher (S-QFC) algorithm holds the idea of a modified Feistel network with modular arithmetic and the utilization of exceptional properties of quaternion's to perform rotations of sequences of data in 3D space for each of the cipher rounds.

A new more secure key generation scheme which is based on quaternion Julia sets is utilized and both-sided modular matrix multiplications are used for the encryption and decryption process. DICOM (Digital Imaging and Communications in Medicine) is the worldwide standard for medical images and related data. It characterizes the configurations for medical images that can be exchanged with the data and quality necessary for clinical use.

The evaluation and comparing of the literature review methods in terms of its advantages, disadvantages and key space is discussed in table 1.

Table 1. Evaluation and comparing with the literature review methods in terms of advantages, disadvantages and key space

S.NO.	Method	Advantages	Disadvantages
1.	Modified AES Based Algorithm 2007	Provide Better performance	It is time taking and risky
2.	Block-Based Transformation Algorithm, 2008	There is no key generator, correlation between the image elements decreased and higher entropy	Image loosing and lower Correlation
3.	Self-Invertible Key Matrix Of Hill Cipher Algorithm, 2008	It is Matrix Based and can Encrypt Gray Scale images	Cannot encrypt image with same gray level or color
4.	A Combination Of Permutation Technique Followed by Encryption , 2008	Provides Higher Entropy but Correlation between image elements decreased	Time taking , Permutation process is too complex, and also chances of mistakes are high
5.	A Novel Image Encryption Algorithm Based On Hash Function, 2010	Encryption Process is done in two phases, so the chances of mistakes is low	Encryption done in two phases so complexity will be increases
6.	A Digital Image Encryption Algorithm Based Composition Of Two Chaotic Logistic Maps, 2010	It is better than all above algorithms because of two logistics maps, uses external sacred keys and strong security	Lot of confusion is there in the process
7.	New Modified Version Of Advance Encryption Standard Based Algorithm For Image Encryption, 2010	Greater security	Because of the algorithm and the secret key, consequently a same data will be ciphered to the same value; which is the main reason for security weakness.
8.	Permutation Based Image Encryption Technique, 2011	It is a three phases process	In key generation process there is high chance of errors
9.	Image Encryption Using Chaotic Maps And DNA Addition Operation And Noise Effects On It, 2011	It is easy to represent	Not a cost effective process
10.	Image Encryption Based On the General Approach for	Larger key space and high-level of security, high obscure level and high computational	Demonstrate process

	Multiple Chaotic System, 2011	speed	
11.	Statistical Analysis Of S-Box In Image Encryption Application Based On Majority Logic Criterion, 2011	Correlation analysis, entropy analysis, contract analysis, homogeneity analysis, energy analysis and mean of absolute deviation analysis	It is complicated and lengthy process because there is lot of analysis done in single technique. Also here time factor will be increases.
12.	The Integration Of A Shifting Technique And The AES Algorithm March 2012	It is improved and effective method	There may be a chance of mistakes while preparing shifting table, it is lengthy and difficult process
13.	Design And Analysis Of A Novel Digital Image Encryption Scheme March 2012	Simple, fast and secured against any attack	It is Large and complicated and also it is very difficult for performance and security analysis
14.	Secret Key Encryption Algorithm Using Genetic Algorithm April 2012	The Encryption algorithm satisfies the desired goal of encrypting the images	This algorithm is complicated and too lengthy
15.	New Advance Image Encryption To Enhance Security Of Multimedia Concept July 2012	Provides best performance, and the lowest correlation with highest entropy	It is a three phase process and every image used is very complicated
16.	Standard GGH	It is a good matrix implementation, Lattice based, easy representation, Correct decryption even with less errors, suitable for high resolution pictures	Low entropy, High correlation, needs more bits after encryption
17.	Padding based GGH	Same as GGH, Lowest correlation, Highest Entropy	It needs more bits for cipher image
18.	A new quaternion based encryption method for DICOM images (F-QFC)	High Computational speed	Weak keys and insufficient key space, no diffusion property and vulnerability to the known plaintext attack
19.	Cryptography of medical images based on a combination between chaotic and neural network	Less complex algorithm	Limited range of key space
20.	Medical Image Encryption using Edge Maps	Large key space, strong key sensitive, strong resistance against various security attacks	Less Computational Speed
21.	A hybrid chaotic and number theoretic approach for securing DICOM images	Provides resistance to brute force attack, high computational speed and key sensitivity	Less efficient
22.	Secure quaternion Feistel cipher (S-QFC) algorithm	High Computational speed than previous method, no diffusion property and vulnerability to the known plaintext attack	Less efficient due to proposed modifications but it can be further used for cloud and mobile environment

The above table compares several encryption techniques that can be used for encrypting medical images. Based on the comparison it can be concluded that secure quaternion feistel cipher (S-QFC) algorithm is best among all, due to its fast computation speed, large key space and robustness to several attacks.

III. COMPARISON AND ANALYSIS

The below table shows the performance analysis and comparison of DES, AES and QFC cryptography algorithms based on the parameters such as speed, Key length, Key sensitivity and its security against Known plaintext attack

Table 2. Performance analysis and comparison of DES, AES and QFC (quaternion feistel cipher) cryptography algorithms

Factors	Encryption Techniques		
	DES	**AES**	**QFC**
Speed	Slow	Faster than DES	Faster than both the techniques
Key Length	56 bits	128,192 and 256 bits	$2^{8.(m^2+4n)} \sim 10^{2.4.(m^2+4n)}$
Key sensitivity	weaker key sensitivity	Stronger key sensitivity than DES only	Strong Key Sensitivity
Known Plaintext attack	Vulnerable to known plaintext attack	Vulnerable to known plaintext attack	Robustness to known plaintext attack

The analysis of computation speed of the S-QFC algorithm in comparison to the F-QFC and AES algorithms is presented in [3]. These algorithms were tested on the same

machine and on the same simulation software environment (MATLAB). The expected values with confidence intervals which are calculated from 20 simulations are presented. Because of the number of performed simulations, *t*-Student estimation is used. The expected values shown in Table 3 are an estimation of the expected value μ.

$$P\left(\overline{X} - t_{\alpha}\frac{S}{\sqrt{N-1}} < \mu < \overline{X} + t_{\alpha}\frac{S}{\sqrt{N-1}}\right) = 1 - \alpha$$

Where, $\overline{X}$ is the expected value of the sample, S is standard deviation of the sample, N is size of the sample (20 simulations), t_{α} is obtained from the *t*-Student table for $N-1$ degrees of freedom and α is the confidence coefficient equal to 5%.

Table3. Computational speed of AES, F-QFC and S-QFC Algorithms (for 512 X 512 px)

AES-ECB	$\overline{X}$	$\frac{t_{\alpha}S}{\sqrt{N-1}}$
Initialization time [s]	6.294e-01	2.999e-02
Encryption time [s]	1.002e-02	1.561e-01
Decryption time [s]	1.446e+02	2.276e-01
Total time [s]	2.454e+02	-
F-QFC	$\overline{X}$	$\frac{t_{\alpha}S}{\sqrt{N-1}}$
Initialization time [s]	2.516e-03	2.894e-04
Encryption time [s]	9.662e-01	1.166e-03
Decryption time [s]	9.620e-01	2.167e-04
Total time [s]	1.931e+00	-
S-QFC	$\overline{X}$	$\frac{t_{\alpha}S}{\sqrt{N-1}}$
Initialization time [s]	6.586e-02	8.855e-03
Encryption time [s]	9.065e+00	7.649e-02
Decryption time [s]	8.945e+00	8.876e+02
Total time [s]	1.807e+01	-

According to the results as shown in Table 3, the S-QFC algorithm is slower than the F-QFC algorithm, but still much faster than the AES algorithm. The degradation in the computation speed of the S-QFC algorithm is primarily due to additional matrix multiplications introduced in the encryption and decryption processes.

IV. CONCLUSION

Cryptography is a technique widely used for secure communication. The problem received much attention, however the number of possible methods which enable the transmitted data interception, is increasing rapidly. Medical pictures are viewed as critical and delicate information in the medical informatics systems. For exchanging medical images over an insecure system, development of a secure encryption algorithm is necessary In this paper we survey and analyze several image encryption and decryption techniques that can be used for securing medical images, as well as comparison is done based on the parameters such as key space, computational speed and there security from various well known attacks. After comparing various encryption algorithms it can be concluded that quaternion based algorithms are best among all, because of its large key space, greater key sensitivity, robustness to known plaintext attack and fast computational speed. Quaternion algorithms can be further used for cloud and mobile environments.

REFERENCES

[1]. Panigrahy S., Acharya B., Jen D. Image encryption using self-invertible key matrix of hill cipher algorithm. In: 1st International Conference on Advances in Computing, 21-22 February, Chikhli, India, . 2008; pp: 1-4.

[2]. Sokouti M., Pashazadeh S., Sokouti B. Medical image encryption using genetic-based random key generator (GRKG).; In: National Joint Conference on Computer and Mechanical Eng. (NJCCEM2013); May 8; Miandoab, Iran. 2013. pp. 1–6.

[3]. Sokouti M., Sokouti B., Pashazadeh S., Feizi-Derakhshi M-R., Haghipour S. Genetic-based random key generator (GRKG): a new method for generating more-random keys for one-time pad cryptosystem. Neural Comput. Appl. 2013;22(7-8):1667–1675. doi: 10.1007/s00521-011-0799-8.

[4]. Younes MAB, Janatan A. "An image encryption approach using a combination of permutation technique followed by encryption". IJCSNS. 2008;8(4):191–7.

[5]. Seyedzade S.M., Atani R.E., Mirzakuchaki S. Novel image encryption algorithm based on hash function.; 6th Iranian Conference on Machine Vision and Image Processing; October 27-28; 2010. pp. 1–6.

[6]. Ismail I.A., Amin M., Diab H. Digital image encryption algorithm based on composition of two chaotic logistic maps'2010. Int. J. Netw. Secur. 2010;11(1):1–5.

[7]. Kamali SH, Shankeria R, Hedayati M, Rahmani M. New modified version of advance encryption standard based algorithm for image encryption.; In: International Conference on Electronics and Information Engineering (ICEIE); August 1-3, 2010. pp. v1-141–v1-5.

[8]. Indrakanti S.P., Avadhani P.S. Permutation based image encryption technique. Int. J. Comput. Appl. 2011;28(8):45–47.

[9]. Enayatifkr R., Abdullah A.H. Image Security via genetic algorithm.; In: International Conference on Computer and Software Modeling IPCSIT;

[10]. Singh K., Kaur K. Image encryption using chaotic maps and DNA addition operation and noise effect on it. Int. J. Comput. Appl. 2011;23(6):17–24.

[11]. Alsafasfeh Q.H., Arfoa A.A. Image encryption based on the general approach for multiple chaotic system. J Signal Inform Process. 2011;2(3):238–244. doi: 10.4236/jsip.2011.23033.

[12]. Abuhaiba I.S., Hassan M.A. Image encryption using differential evolution approach in security Domain. Signal Image Process. Int. J. 2011;2(1):51–69. [SIPIJ].

[13]. Patel K.D., Belani S. Image encryption using different techniques: A review. Int. J. Emerg. Technol. Adv. Eng. 2011;1(1):30–4.

[14]. Abugharsa A.B., Basari A.S., Almangush H. A new image encryption approach using the integration of a shifting technique and the AES algorithm. Int. J. Comput. Appl. 2012;42(9):38–45.

[15]. Pareek N.K."Design and Analysis of a novel digital image encryption scheme". Int J Net secure Appl. 2012;4(2):95–108.doi: 10.5121/ijnsa.2012.4207.

[16]. Agarwal A. Secret key encryption algorithm using genetic algorithm. Int J Adv Res Comp Sci Soft Eng. 2012; 2(4): 216-8
[17]. Bhatt V. Implementation of new advance image encryption algorithm to enhance security of multimedia component. Int J Adv Technol Eng Res. 2012;2(4):13–20.
[18]. 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, Nov. 2015.
[19]. M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," IET Image Process., vol. 10, no. 11, pp. 830–839, 2016.
[20]. W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," Signal Process., vol. 132, pp. 96–109, Mar. 2017.
[21]. J. Chandrasekaran and S. J. Thiruvengadam, "A hybrid chaotic and number theoretic approach for securing DICOM images," Secur. Commun. Netw., vol. 2017, Jan. 2017, Art. no. 6729896, doi: 10.1155/2017/ 6729896.
[22]. M. Dzwonkowski and R. Rykaczewski, "Quaternion feistel cipher with an infinite key space based on quaternion Julia sets," J. Telecommun. Inf. Technol., vol. 4, pp. 15–21, Dec. 2015.

