Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02028-5

ORIGINAL RESEARCH

A secure medical image transmission algorithm based on binary bits and Arnold map

K. N. Madhusudhan[1] · **P. Sakthivel**[1]

Received: 20 February 2020 / Accepted: 24 April 2020

Abstract
The responsibility of maintaining patient's records is with medical personnel. The medical personnel are supposed not to disclose any kind of medical information related to the patient. This is also applicable for the medical information discovered by medical personnel in connection with the treatment of the patient. With the advent of technology and its penetration into the medical field in the form of telemedicine and e-health, the challenge of maintaining confidentiality is becoming complex. The confidentiality needs to be protected from storage of medical image or transmission of image from a medical database center to other. Nowadays, the information of patient is printed in the corner of the medical image. This can be accessed by anybody or even the machine can access and store the information. During an electronic transmission, the patient information may be intercepted by a third party. This may lead to big lawsuit. Apart from these security issues, for scenarios such as medical research, the image should be used but patient information should be hidden. Also for diagnostic purposes, the information of the patient should be readily accessible to the medical personnel. These constraints lead to the necessity of suitable security techniques for medical image storage and transmission. If suitable security techniques are not applied, privacy of patients will be stake. Hence, numerous methods are being implemented by individuals, governments and businesses for secured transmission of patient's data. For patient's privacy protection, secured transmission requires techniques like cryptography and watermarking. These techniques achieve confidentiality and integrity. In this work, a new approach has been developed for secured transmission of medical images.

Keywords Machine interaction · Image transmission · Security · Arnold maps

1 Introduction

Secure and fast diagnosis is important in the medical field for saving the lives of people. Diagnosis involves generation of medical images. Medical images get generated using many ways like magnetic resonance imaging (MRI), radiography, ultrasound, nuclear medicine, tactile imaging, thermography, photo acoustic imaging and electroencephalography (EEG). Images are also generated during medical tests like electro cardio graphy (ECG) and Magneto Encephalography (MEG). As the size of these images is large, it requires a huge space for storage and good bandwidth for transmission in the original status. In current scenario, image transmission is becoming a daily routine and because of this, there is a necessity of efficient way for transmission (Lo-Varco et al. 2003; Norcen et al. 2003; de Carvalho 2008). Image transmission over the internet is a challenging task. Encryption is the available option for secured transmission. The image is secured when cryptography is used and also communication channel is better utilized. For transmission of images, two techniques are being practiced. First method is the protection of content using encryption as discussed by McEliece (1978), Berlekamp et al. (1978), Pareek et al. (2006). Data decryption requires a key. The second method is based on data hiding or watermarking. This process involves embedding a message secretly into the data. For image compression, there are some methods in practice. For reduction of image size, the image compression method is used primarily which does not cause any affect to image quality. The procedure results in storing more data in a file, thus increasing the memory. It results in reducing the speed of image access during its transmission over the internet. The commonly used compression formats are GIF and JPEG. For photographic

✉ K. N. Madhusudhan
madhusudhank.aut@gmail.com; krgirimadhu@gmail.com

[1] Department of ECE, CEG, Anna University, Chennai 600025, India

Published online: 13 May 2020

images, the JPEG formats are used frequently whereas the GIF formats are used for arts in which geometric figures are simple. Fractals and wavelets are the other methods being used for compression. The secured transmission of medical images is based on authentication, confidentiality and integrity. Confidentiality involves the data protection from access of unauthorized sources. Only authorized users can get an access to information. The data sent and the data received should be same. There should not be any modification, deletion or insertion. This process is called integrity. Authentication is the process of ensuring that the entity which is in communication is the same which it claims to be. It confirms that the data is related to same patient. Cryptography is a security concept that is intended to provide security to any kind of message either text or image. Encryption keys are used by cryptographic methods which change general algorithm to a specific technique of encryption. The purpose of encryption is to make the data to be secured in an unintelligible format. Hence, the substance of the data cannot be sniffed by the intruders, unless some complex manipulations are done. Understanding the importance of security, this work contributes a secure data transmission scheme for medical images that fights against privacy breaches.

The rest of the article is arranged in the following way. Section 2 discusses the related review of literature with respect to secure medical image encryption. The proposed work is described in Sect. 3 and the attained results are discussed in Sect. 4. Finally, Sect. 5 concludes the paper.

2 Related work

Soleymani et al. (2012) presented the problem related to security of medical image transmission in wireless sensor networks. The researchers opine that the remote healthcare system is already in place in developing and developed countries. For image processing, there exist several algorithms. This work provides information on how various methods are used to provide security to medical images transmission. The methods discussed include the partial encryption, compression and watermarking. The reversible watermarking method with encryption is also discussed. The authors conclude the work by saying that in all the methods, patient information and image is embedded and encrypted during data transmission. During embedding, a problem of slow transfer and noise arises. For resolution of these problems, segmentation and compression techniques are used.

Kester et al. (2015) opine that medical images are stored in cloud and other health information systems. Hence, providing security to the medical data is important. Using encryption and authentication procedure, security and privacy needs to be guaranteed. In this research work, the authors have proposed watermarked and recoverable encrypted method for image processing. The approach is useful for security and authenticity of images related to patients.

Rohini and Bairagi (2010) state that security of medical image is significant during transmission across public networks. The management system for storing distributed medical data is called PACS-picture archiving and communication system. In PACS, the medical image transmission is generally done over the intranet of hospitals. The intranets are usually protected by a firewall. This restricts outsider's access to medical data. This work presents existing methods, previous works, and the need for security mechanism with respect to medical image. The problem with the existing techniques like watermarking is that the lack of robustness against various types of image manipulations or attacks. Also, it is complex to implement these techniques in real-time. With respect to digital fingerprints, the concerns are technological compatibility, legal issues, secured storage and transmission. The authors conclude by saying that there is a need for special method for processing of medical image communication which includes security aspects.

Ahmed et al. (2018) proposed a robust technique for medical image watermarking for verification and authenticity of medical images in telemedicine applications that are computer-aided diagnosis. For achieving imperceptibility with watermark transparency and robustness, a method based on fast curvelet tansform (FCT) and robust principal component analysis (RPCA) has been proposed.

Pande and Thakur (2018) surveyed various mage security techniques and presented a summary. Various parameters such as basic concept used, image types, parameters used for performance evaluation, remark about the work and findings are tabulated. Image security techniques such as image encryption, image transmission, image steganography etc. are discussed. Image transformation includes the process of taking digital image as input and producing another image as output for security enhancement. Conversion of input image file into other random image which is difficult to understand is termed as Image encryption. This is accomplished with or without a key. For securing image transmission, there exists various mechanisms such as selective image encryption, chaos based cryptography, public key image encryption, private key image encryption, visual cryptography etc. The authors conclude that there exists various encryption techniques presented in the 1990s and each of the techniques is unique in its way. Some techniques provide good quality at the receiving end while some other techniques produce degraded images. The techniques vary in processing speed also.

Kamble and Patil (2018) suggested a technique for medical image security with tamper detection. In first step, record of patient which is in electronic form is encrypted by DNA cryptography. Later it is submitted to secret sharing algorithms which are shared with participants. At the receiving side, the created

shares are verified. By combining these shares, secret can be uncovered. By verifying the shares, the changes can be detected.

Junaid and Ravindran (2012) presented the research work in which the enhancement of images done using local adaptive filter and POI—pixels of interest. This is done for reducing the size of the medical images to be transferred. For compression of data with minimum storage space, discrete wavelet transform (MDWT) technique is used. The image is reconstructed at the receiving end. The objective of the work include design and development of modified DWT method using reduced sub band coding and uniform quantizer for image band splitting and then for coding each sub band using a coder. To achieve reduction in storage, the proposed mechanism uses dimension reduction that implements intermediate co-efficient storage. At the receiving end, by decoding every sub band, intermediate co-efficient is obtained.

Deepa and Sutha (2017) discussed the security of medical images when transmission occurs in mobile Adhoc network. Doctors form a group for communication wherein they transfer medical images as well as data related to patient. This research work designs the self-adjustment property in Adhoc network. Each node receives the intended message from its neighbour and also checks the signal strength of the node that transmits it. If the signal strength is less, assuming that the sending node is moved from its location, receiving node adjusts its location to receive the signal.

John and Cherian (2015) proposed an innovative method for transformation of the secret image into secret fragment-visible mosaic mage. The size of the secret image and mosaic image is same. Mosaic image gets created by dividing target image and secret image into parts of similar size and these tile blocks are fitted into target blocks. Genetic algorithm (GA) is used for tile image hiding thus providing improved quality in retrieved secret image.

Umamageswari and Suresh (2013) developed a method wherein ROI i.e., region of interest (ROI) defined data is embedded in it. For compression purpose the researchers proposed the JPEG2000 algorithm. Arnold's cat map is proposed for maintaining reliability, accessibility and secrecy of the embedded data. Zhang et al. (2016) proposed an image encryption algorithm, which is based on the techniques such as dynamic DNA coding and Chen's hyperchaotic system.

Sneha et al. (2020) presented a chaotic color image encryption scheme by combining Walsh-Hadamard transform with Arnold-Tent maps. The images are treated with respect to channels and two chaotic maps such as Arnold and Tent maps are utilized for enciphering.

Gupta et al. (2020) proposed an efficient image encryption scheme by employing non-dominated sorting genetic algorithm-III based four dimensional chaotic maps. This work follows the principle of master–slave model. Initially, the mutation and cross-over operations are performed, followed by which the jobs are separated for master and slave nodes. Communication between the master and slave nodes is made possible with the help of message passing interface.Based on these existing works, this paper presents a medical image transmission algorithm based on Arnold map and binary bits. The proposed methodology is described in the following section.

3 Proposed methdology

3.1 Arnold map

Arnold proposed Arnold map in the research related to ergodic theory in 1960s. It is also known as cat map. It is an invertible map represented by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod 1) \tag{1}$$

where (x mod 1) indicate x's fractional part for any given real number x. In Arnold map, the Lyapunov exponent is greater than 1 that means that the map is chaotic. Here, map (1) is not used straight in encryption of image which is in digital format, as Arnold map security depends on the initial value. To overcome this drawback, Arnold map that is generalized is presented with two parameters a and b as given below.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod 1) \tag{2}$$

a and b are control parameters which are real numbers. It can be concluded that the largest Lyapunov exponent in map (2) is greater than map (1). This is when a > 1 and b > 1. This means that map (2) can perform better in data shuffling operation.

3.2 Methodology

3.2.1 Permutation

In a classical image encryption method, for changing the pixel position in the plain image, permutation procedure is used. For altering the pixel value, a diffusion procedure is used. Permutation can be either at pixel level or bit level. A pixel is identified as the smallest element even though the positions of pixels are scrambled. Generally, image gray-scale distribution remains unchanged. A pixel can be divided further into a number of bits. A considerable diffusion effect happens because of the random rearrangement of bits of the pixels. This effect is not applied for the permutation effect in the bit-level permutation method. The overall flow of the proposed work is depicted in Fig. 1.

The plain image of size $h \times w$ is taken and each pixel a_{ij} is changed into a binary sequence of 8 bits. From this,

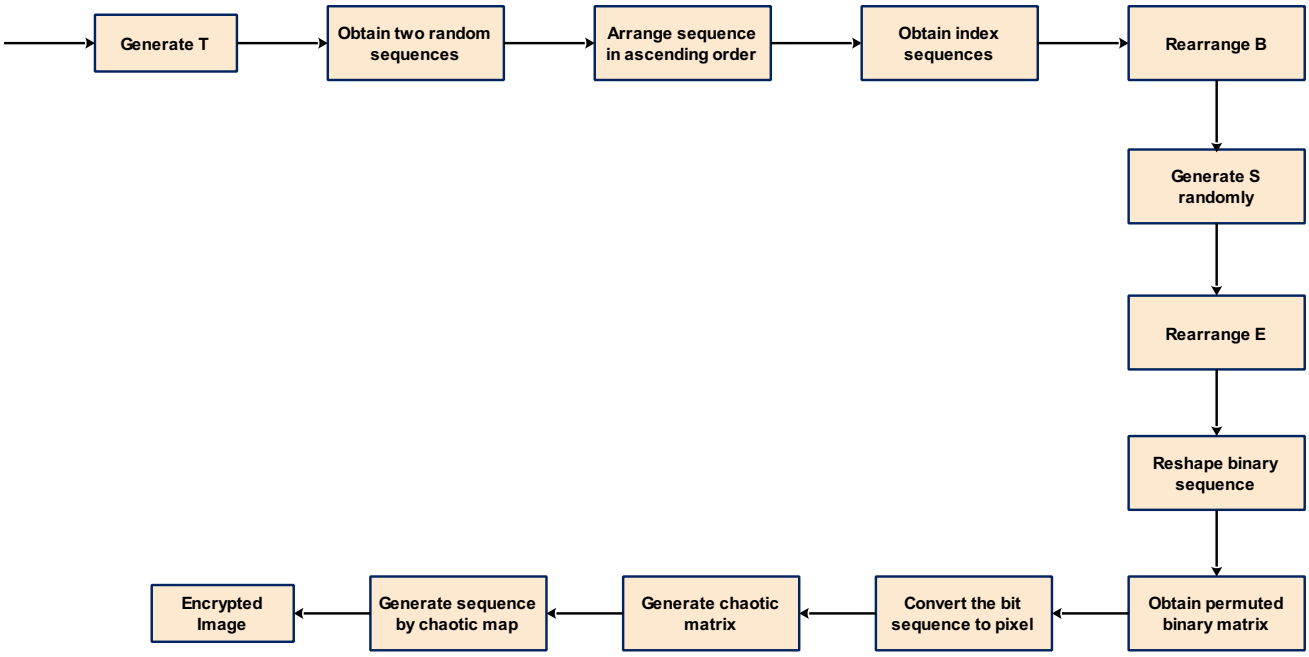

Fig. 1 Overall flow of the work

2 dimensional binary matrix with size $h \times 8w$ is obtained. Permutation process at the bit-level is introduced with row and column relocations. At first, in the row direction, bit-level permutation is executed and the proposed algorithm is presented as follows.

Proposed Algorithm

Input – Medical Image
Output – Encrypted image
Begin

1. Generate an integer sequence $T = (t_1 K t_h)$ randomly; (T represents integer permutations).
2. Obtain two random sequences with $h_0 + 8wh$ elements by generalized Arnold map iteration.
3. If (output is similar to previous value)
4. Discard the value;
5. Discard the initial h_0 elements;
6. Obtain two sequences namely R_x, R_y;
7. Arrange the sequences in ascending order and obtain two index sequences (I^x, I^y) by eqn.(3);
8. Extend 2D binary matrix to 1D binary sequence B with row order $(t_1 K t_h)$;
9. Rearrange B as $B_k^{'}$ by eqn.(4);
10. 2D-binary matrix is extended to 1D binary sequence B with row order $(t_1 K t_h)$;
11. Generate an integer sequence $S = (s1 K s_{8w})$ randomly; (S indicates permutation of integers 1,2,…,8w);
12. Extend the row permuted matrix to one dimensional binary sequence E with column order $(s_1 K s_{8w})$;
13. Rearrange E as $E_k^{'}$ by eqn.(5);
14. Reshape the binary sequence E' to attain 2D matrix;
15. Obtain permuted binary matrix out of row and column permutation;
16. Convert the bit sequence into pixel M;

End;

The index sequences (I^x, I^y) are generated by the following Eq. (3).

$$I^x = \left\{ I_1^x K I_{8wh}^x \right\};\ I^y = \left\{ I_1^y K I_{8wh}^y \right\} \tag{3}$$

The reason for eliminating the initial h_0 elements is to escape from the harmful effect of generalized Arnold map.

$$B_k' = \left\{ B_{I_k^x} \right\};\ k = 1, 2, \ldots, 8wh \tag{4}$$

Here, B' is the binary sequence that is reshaped to the row-permutated image matrix. The execution of the row direction permutation then happens. After the row direction, the bit-level permutation in the column direction is done. The procedure is same as row direction. Similarly, the column-wise permutation is represented as follows.

$$E_k' = \left\{ E_{I_k^x} \right\};\quad k = 1, 2, \ldots, 8wh \tag{5}$$

The diffusion procedure is presented in the following section.

3.2.2 Diffusion procedure

To maintain the property of chaotic sequences, the XOR is operated between M, the confusing image matrix which is obtained in step 16 (as presented in the algorithm). The chaotic matrix C is used to get the matrix N, where $N = M \oplus C$. Here, C is the chaotic matrix computed by Eq. (6).

$$C = int\left(y \cdot 10^{20}\right) mod 256 \tag{6}$$

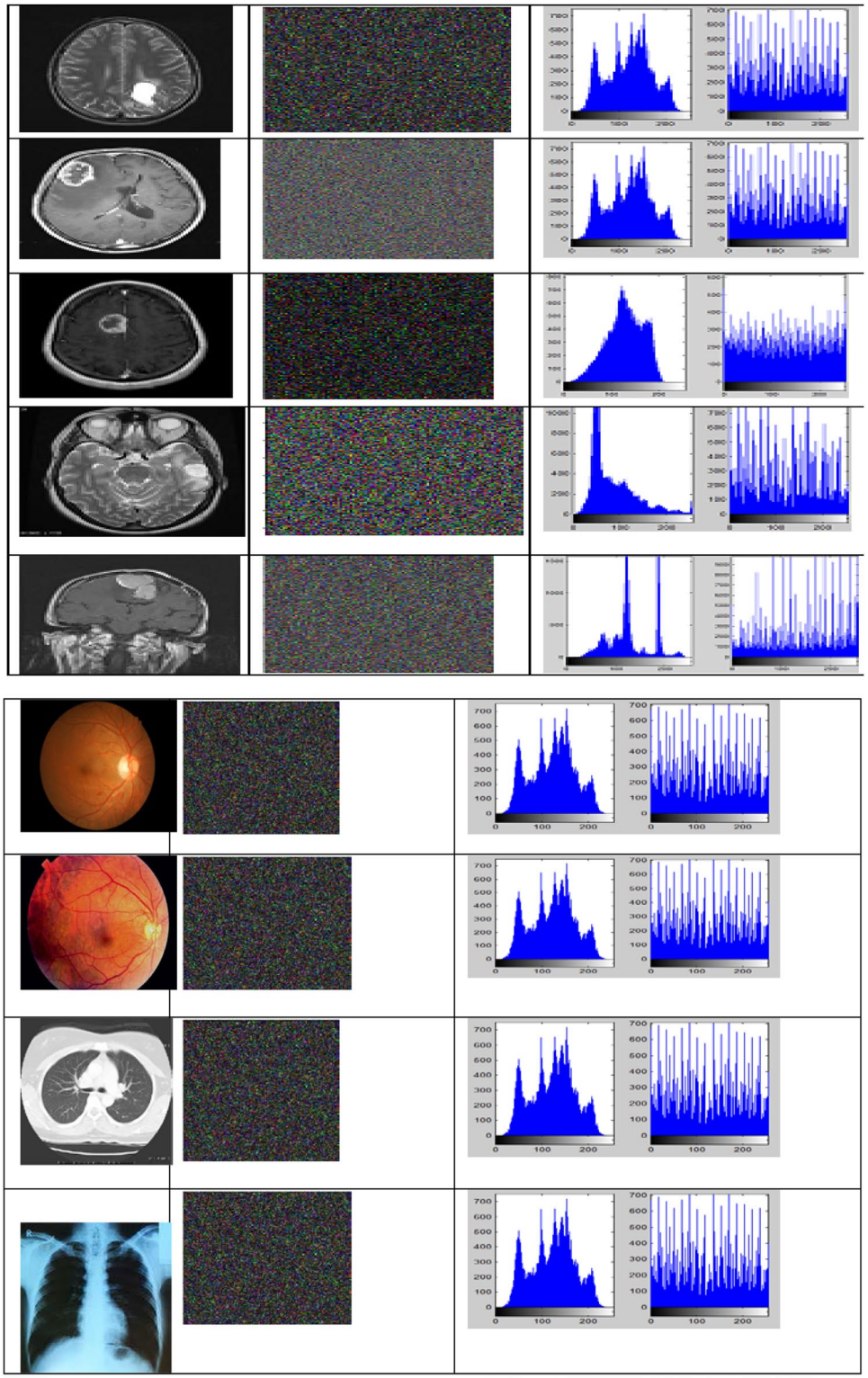

Fig. 2 Col.1—Col. 3 indicates Original image, cipher image and histogram of original and cipher image respectively

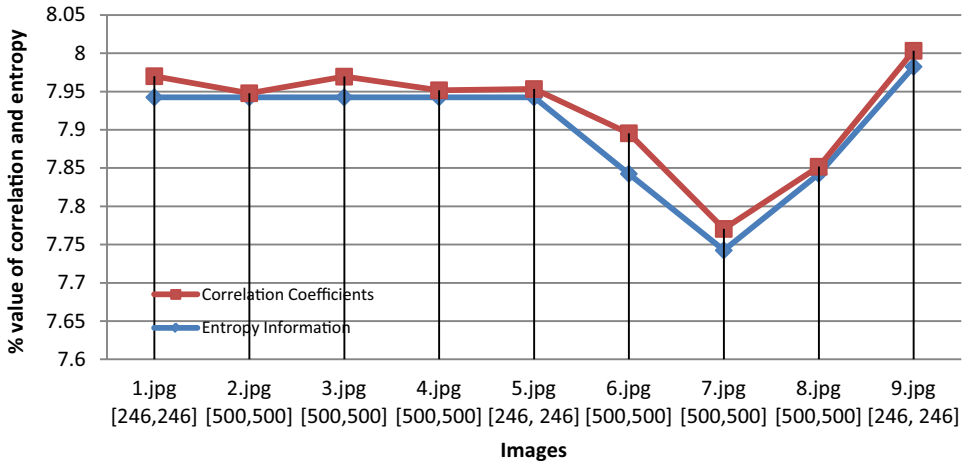

Fig. 3 Consistency of the algorithm (correlation and Entropy values)

The sequence y is generated using the chaotic map

$$y_{n+1} = dy_n(1 - y_n)K \cdot K; \quad b \in [3.5699456, 4]$$
$$y_n \in (0, 1); \quad n = 1, 2, \ldots \tag{7}$$

The results attained by the proposed work are discussed in the following section.

4 Results and discussions

This section presents results with performance evaluation with standard metrics explained in the previous section.

4.1 Performance metrics

In the field of information security, a perfect encryption method needs to be very sensitive to the cipher key, cipher text and plain text. In addition, a good encryption method needs to be having robust capability to tolerate cryptography analysis and malicious attacks that are directed to break the system. In this section different tests have been discussed related to analysis of the security of proposed cryptosystem.

Histogram analysis presents values of pixel distribution in the image. The histogram of cipher image must be uniform and varies with plain image. This prevents attack that may steal valuable statistical information. Figure 2 shows the original image, cipher image and histograms of both original and cipher images.

The measure of the uncertainty linked with a random event is termed as Information entropy analysis. Let $H(X)$ represents the entropy of information of source X with length L as follows.

$$H(X) = -\sum_{i=0}^{L-1} p(x_i) \log_2 p(x_i) \tag{8}$$

where $p(x_i)$ is the probability of symbol x_i.

In plain image, a scheme that is ideal must overcome obvious correlations. Correlation analysis is used to compare and quantify the pixels which are adjacent in the cipher and plain image with more accuracy. By using the following equation, the correlation coefficient of cipher image and plain image can be obtained.

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{9}$$

where $E(x)$ is the expectation and $D(x)$ is the variance of variable x. Figure 3 demonstrates the consistency of the proposed algorithm with correlation and Entropy factor.

In differential attack analysis, for investigating the influence of a 1-bit change in the plain image to the respective cipher image, two performance indices are used. UACI (unified average changing intensity) and NPCR- number of pixels change rate are the performance indicators. They are defined as below.

$$NPCR = \sum_{i,j} \frac{d(i,j)}{h \times w} \tag{10}$$

$d(i,j)$ takes the value 0 or 1 depending on $C_1(i,j), C_2(i,j)$.

$$UACR = \frac{1}{h \times w} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \tag{11}$$

where h is the height and w is the width of the cipher image, respectively.

4.1.1 Key sensitivity analysis

By slightly altering the initial values of the Arnold map, sensitivity analysis of encrypted images can be done. The

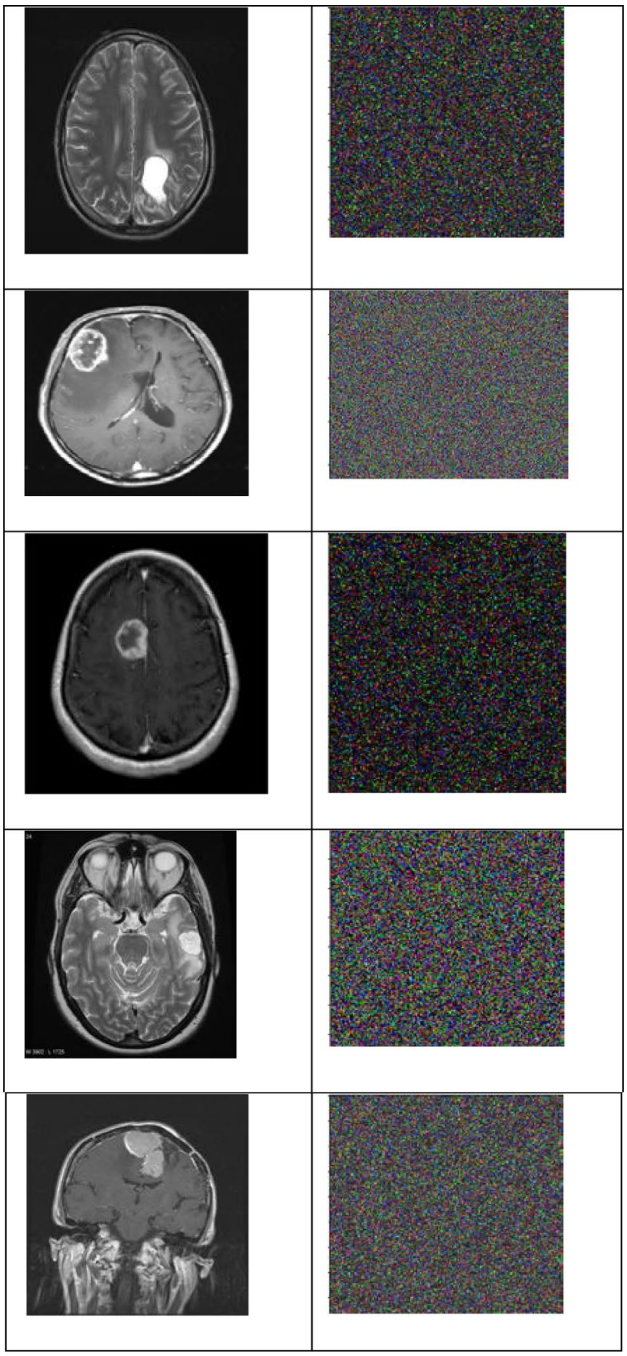

Fig. 4 Key sensitivity performance analysis (key sensitivity performance analysis for original key = 1234, modified key = 1235)

Table 1 Correlation coefficients and entropy information of cipher image

Image with dimensions	Entropy information	Correlation coefficients
1.jpg [246, 246]	7.9425	0.0276
2.jpg [500, 500]	7.9425	0.0053
3.jpg [500, 500]	7.94251	0.0270
4.jpg [500, 500]	7.9425	0.00918
5.jpg [246, 246]	7.94251	0.0108
6.jpg [500, 500]	7.8425	0.053
7.jpg [500, 500]	7.74251	0.0280
8.jpg [500, 500]	7.8425	0.00928
9.jpg [246, 246]	7.98251	0.0208

following are the results of the decryption operation by slight change in the key values of the Arnold cat map.

Hence, the performance of the proposed work is proven to be better and the conclusions of the article are presented in the following section (Fig. 4).

5 Conclusion

The information pertaining to patient plays a very vital role in telemedicine and tele-diagnosis. Authentication of medical image content is crucial as images are more and more distributed. In literature, it can be found that there exist several methods for security of medical images. The techniques include compression, watermarking and new algorithms for secured transmission. The proposed approach converts the image pixel into binary bits. Later Arnold map is used to generate random numbers. Image scrambling has been performed on the binary bits of the pixels. Finally, diffusion procedure has been performed for secured transmission of medical images. The implementation results are promising and this method can be a good contribution to research in this area (Tables 1, 2, 3).

Table 2 NPCR and UACI of some ciphered images

Images	1.jpg [246, 246]	2.jpg [500, 500]	2.jpg [500, 500]	3.jpg [500, 500]	4.jpg [246, 246]
NCPR	0.996	0.9956	0.9962	0.9958	0.99411
UACI	0.3346	0.33463	0.33463	0.33463	0.33463

Table 3 NPCR and UACI comparison with different methods

Images	Average % (proposed)	Avg % [16]	Avg % [17]
NCPR	99.6	99.50	88.9
UACI	33.46	28.29	30.21

References

Ahmed R, Hassan B, Li B (2018) Robust hybrid watermarking for security of medical images in computer-aided diagnosis based telemedicine applications. In: 2018 IEEE international symposium on signal processing and information technology (ISSPIT), pp 1–5

Berlekamp E, McEliece R, Van Tilborg H (1978) On the inherent intractability of certain coding problems. IEEE Trans Inf Theory 24(3):384–386

de Carvalho DF, Chies R, Freire AP, Martimiano LA, Goularte R (2008) Video steganography for confidential documents: integrity, privacy and version control. In: Proceedings of the 26th annual ACM international conference on design of communication, pp 199–206

Deepa R, Sutha J (2017) Efficiently multicasting medical images in mobile Adhoc network for patient diagnosing diseases. Biomed Res 2017:315–320

Gupta A, Singh D, Kaur M (2020) An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps. J Ambient Intell Human Comput 11(3):1309–1324

John RM, Cherian JP (2015) Secure image transmission via mosaic images using genetic algorithm. Int J Innovat Res Sci Technol 2(5):208–213

Junaid KM, Ravindran G (2012) Modified DWT based medical image transmission using reduced storage space. Asian J Biomed Pharmaceut Sci 2(10):24–32

Kamble P, Patil S (2018) Medical image security with cheater identification. In: 2018 fourth international conference on computing communication control and automation (ICCUBEA), pp 1–6

Kester QA, Nana L, Pascu AC, Gire S, Eghan JM, Quaynor NN (2015) A security technique for authentication and security of medical images in health information systems. In 2015, 15th international conference on computational science and its applications, pp 8–13

Lo-Varco G, Puech W, Dumas M (2003) DCT-based watermarking method using error correction coding. In ICAPR'03: international conference on advances in pattern recognition, pp 347–350

McEliece RJ (1978) A public-key cryptosystem based on algebraic. Coding Thv 4244:114–116

Norcen R, Podesser M, Pommer A, Schmidt HP, Uhl A (2003) Confidential storage and transmission of medical image data. Comput Biol Med 33(3):277–292

Pande AP, Thakur NV (2018) A survey on different ways of secure image transmission. Int Res J Eng Technol 5(2):407–413

Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24(9):926–934

Rohini S, Bairagi V (2010) Lossless medical image security. Int J Appl Eng Res 1(3):536–541

Sneha PS, Sankar S, Kumar AS (2020) A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. J Ambient Intell Human Comput 11(3):1289–1308

Soleymani A, Ali ZM, Nordin MJ (2012) A survey on principal aspects of secure image transmission. Proc World Acad Sci Eng Technol 66:247–254

Umamageswari A, Suresh GR (2013) Security in medical image communication with arnold's cat map method and reversible watermarking. In: 2013, international conference on circuits, power and computing technologies (ICCPCT), pp 1116–1121

Zhang J, Hou D, Ren H (2016) Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system. Math Probl Eng 2016:1–11