INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE TRANSMISSION OF MEDICAL IMAGES USING POSITION AND VALUE PERMUTATION

SACHIN KAILAS BHOPI[1], NILIMA M. DONGRE[2], RESHMA R. GULWANI[2]

1. ME Student: Department of Information Technology, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India.
2. Ass. Prof, Department of Information Technology, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Health Insurance Portability and Accountability Act(HIPPA), says health organizations should take required measures to ensure that patient information is only provided to individuals who has a professional need. The patient information such as x-rays, CTs and MRIs needs a security to protect from unauthorized access. To provide security image encryption algorithm is proposed. Here chaotic logistic maps are used to generate pseudorandom numbers which can work as a key to encrypt the image. The proposed algorithm first performs position permutation on the image to change the pixel location and then value permutation is used to change pixel values. The resultant image is encrypted image which is further compressed by efficient lossless compression algorithm.

Keywords: Image Security; Pixel Permutation; Logistic Map; Image Compression

.

Corresponding Author: MR. SACHIN KAILAS BHOPI

Access Online On:

www.ijpret.com

How to Cite This Article:

Sachin Kailas Bhopi, IJPRET, 2016; Volume 4 (9): 379-389

PAPER-QR CODE

INTRODUCTION

Nowadays, People often take second opinion from other doctors who suggest them same kind of tests which include x-rays, CTs, and MRI and so on which generate redundant data. This will waste lots of resources as well as time and money of the patient. To overcome this problem, many experts suggest using storage infrastructure where every doctor can store and retrieve the data of his own patient and the other patients as well. To provide security to such important data is necessary to protect it from unauthorized access.

Image encryption is an intelligent way of hiding information [1]. The image data is significantly different than that of text data as it has properties such as high correlation between the nearby pixels, large size, and high redundancy that imposes special requirements on any encryption technique [2]. There are several approaches to achieve image encryption such as Steganography, Compression, Digital Watermarking and Cryptography.

The different encryption algorithms like AES, DES etc. are fails for image encryption [3]. Chaotic maps are more suitable for image encryption because of its properties like systems depend completely on initial condition; it has lower mathematical complexity and provides better security [4].

Compression is a reduction in the number of bits needed to represent data in order to store or transmit data in an efficient form. The image compression techniques can be of two types lossy and lossless compression. The lossless compression algorithm is one who can generate exact replica of the original image and lossy compression could loss some of the information [5].

The image encryption using chaotic maps can have applications in the areas like Tele-medicine, military, government documents etc. Towards this direction, we design an efficient chaos based symmetric cryptography system for medical image encryption.

The remainder of this report is organized as follows. Section II presents Literature survey. Section III briefly addresses the issues in current systems and how it can be overcome. Section IV reports methodology in which position permutation and value permutation is used to encrypt the image and compression is used to reduce size of image file, and Finally, Section V concludes the topic.

LITERATURE SURVEY

Literature involves techniques for providing image security through block permutation, pixel permutation and use of chaos function along with their merits and demerits.

Block-based Transformation Algorithm

Block based transformation algorithm consist of image transformation as we as Blowfish algorithm. The image is decomposed into the sub blocks. The sub blocks can be reposition to get possible scrambling then the image is again encrypted using blowfish algorithm to provide resultant encrypted image. The correlation between image elements is significantly reduced. Drawback of this technique is too much memory utilization for execution of image encryption and its correlation and entropy value can be reduce further.[6]

Permutation Technique followed by Encryption

Permutation technique followed by encryption consists of image permutation as well as AES algorithm. In this original image is process to transform into sub blocks of size 4*4 pixels block each. These sub blocks can be rearranged into scrambled image using a permutation process, and then encrypted using the AES algorithm. The correlation between image elements is significantly reduced and higher entropy is achieved but permutation process is very complicated and also time taking process [7].

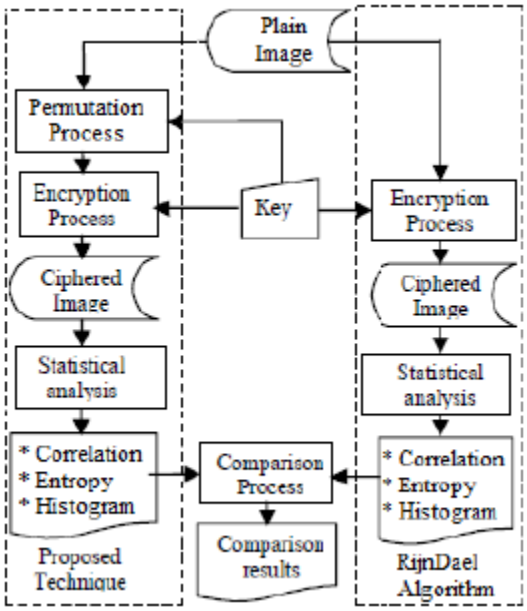

Fig. 1. Permutation followed by encryption[7]

Chaos and DES

Chaos and DES is a combination of two encryption algorithms. This technique uses the logistic chaos map to generate the pseudo-random numbers which applied to the RGB to encrypt image chaotically and then encrypt using DES. Their result show high starting value sensitivity, and high security but because of the characteristics of image information, DES algorithm is not the ideal choice for digital image encryption.[8]

Chaotic maps and DNA addition operation

Chaotic maps and DNA addition operation are compared four chaotic maps such as Cross chaotic, Logistic, Ikeda and Henon map and noise effects are observed on image. Encrypt original image using chaotic maps to get desired encrypted image. Apply noise on encrypted image which means try to decrypt using random key which will give desired encrypted image. It is sensitive to the secret keys, it has larger key space but the quality of image degrades due to the effect of noise but not to an extend that image cannot be recognized.[9]

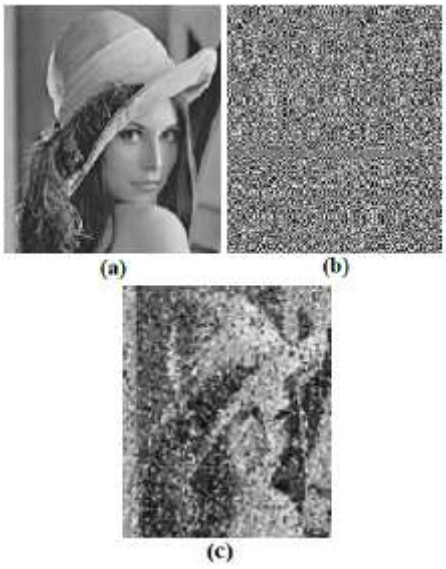

Figure 2. Chaotic Maps and DNA addition: (a) Original Image, (b) Encryption Image, (c) Decrypted Image

PROBLEM STATEMENT

The current trend of medical image transmission through the wired and wireless network is more and more increasing. Telemedicine and e-health especially, have a basic need of data transmission. However, the security problems during transmission also increase. There is a

basic need to secure the data during transmission. In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In this communication, the proposed approach for image encryption based on chaotic logistic maps in order to meet the requirements of the secure image transfer. Input image of is decomposed into eight times smaller blocks. Each sub blocks are then encrypted with row wise rotation and column wise rotation with respect to key bits taken from chaotic logistic map. The resultant blocks are recomposed into image which again decomposed into four times smaller blocks than that of the original image for diagonal rotation. Then 2D image is converted into 1D array from which every one byte is taken for encryption using value permutation algorithm. For compression, Image file is converted into text file and find the count to assign a code for each character. The resultant file will be encrypted as well as compressed to travel over the unsecured network.

METHODOLOGY

In proposed method, there are two phase. In first phase Fig. 3, Position permutation is perform on input image by dividing image into sub blocks and applying row wise, column wise and diagonal rotation on each block. In second phase Fig. 4, Value permutation is perform on output image of the position permutation. In this, Image is read as a 1D array and each byte is extract to apply value permutation algorithm. The resultant image is final encrypted image. To transmit over the unsecure network encrypted image is compressed using adaptive coding.

Position Permutation Algorithm

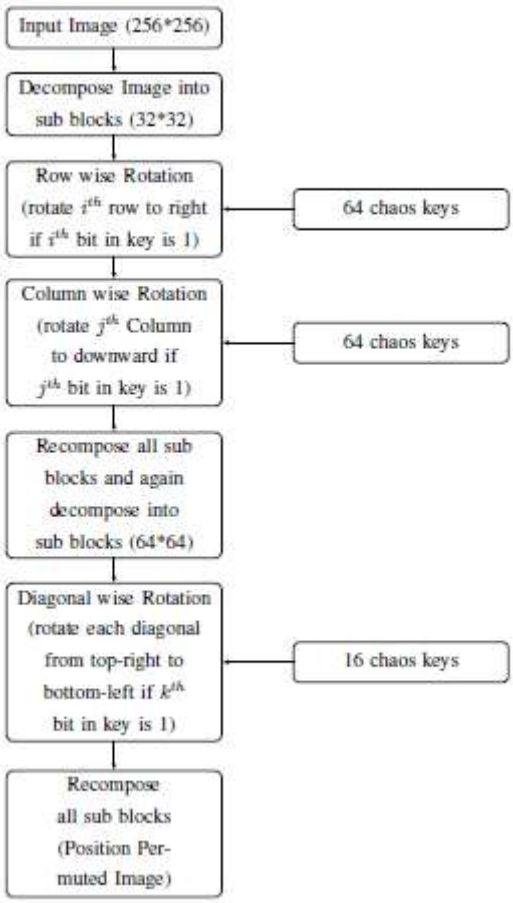

Figure 3. Position Permutation

Step 1: Input image (256*256 pixels) is decomposed into 32*32 pixels sub blocks to perform further operation on each block separately.

Step 2: Each sub block of size 32*32 pixels is permuted by row wise and column wise rotation using a key provided by chaotic logistic map.

– Horizontal rotation: If the ith bit in key is 1 then single right rotary shift on ith row and if the bit is 0 then single downward rotary shift on first column.

– Vertical rotation: If the jth bit in key is 1 then single downward rotary shift on jth column and if the bit is 0 then single right rotary shift on first row.

Step 3: Recompose all the sub blocks which is again decompose into little bigger blocks such as 64*64 pixels sub blocks to perform diagonal wise rotation.

Step 4: Diagonal wise rotation: If kth bit in key is 1 then all diagonal in sub block is rotated by one position from top-right to bottom-left otherwise each diagonal in sub block is rotated by one position from top-left to bottom-right.

Step 5: Recompose all the sub blocks to get resultant image with position permutation algorithm.

Value Permutation Algorithm

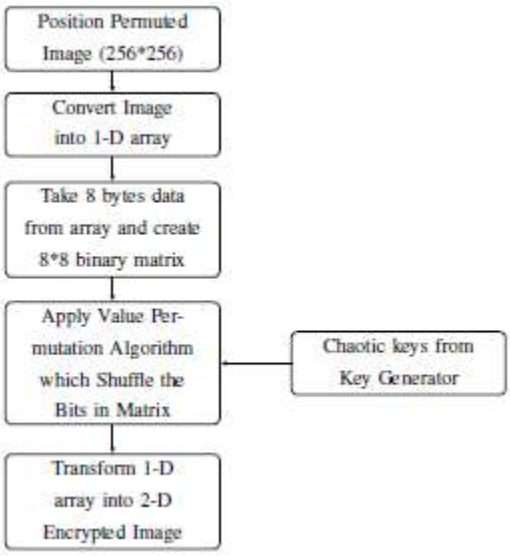

Figure 4. Value Permutation

Step 1: Take position permuted image and convert it into 1-D array.

Step 2: Take eight 8-bit values from an array and create binary matrix of size 8*8.

Step 3: Let M denotes binary matrix of size 8*8 and M0 denotes encryption result of M.

– RotateXpr i (M): M M' is define as rotate all bits in the ith row of M, 0 ≤ i ≤ 7, r bits in the left direction if p=1 or r bits in the right direction if p=0.

– RotateYqs j (M): M M' is define as rotate all bits in the jth column of M, 0 ≤ j ≤ 7, s bits in the up direction if q=1 or s bits in the down direction if q=0.

Step 4: Perform encryption using keys generated from chaos key generator.

Step 5: Convert encrypted array into image.

Step 6: Decrypt image using same and exactly opposite procedure as that of encryption using same keys.

Chaotic Logistic Map

The logistic map is very simple non-linear dynamical equation used to generate complex and chaotic behavior. Chaotic logistic map is written as follows:

xn+1 = rxn(1-xn)

Key Generator

Choose m maps M0, M1, Mm-1 from the map bank and set the order of the chosen maps to hop. From every chosen map, s orbits S0, S1, Ss-1 are generated and from individual orbit, n points N0, N1, Nn-1 are generated. Parameters m, s, n are expressed in a key.

Example : Here is the key, it consists of 58 random numbers (0 to 15, i.e., 0 to F in hexadecimal). Notice that the first two numbers determine the #maps, and are generated separately.

Here 1 2 is hex will be (12)h = (18)d. We calculate 18 (mod 7) = 4. So the #maps = 4. Each map needs a 56 bit sub key, so we need another 56 x 4 = 224 bits, i.e., 56 hex numbers for the rest of the key. Suppose those random numbers are as follows.

1 2 11 13 1 4 4 11 3 10 8 14 6 9 7 7 1 14 10 14 6 2 14 15 9 7 1 7 11 0 8 10 7 1 6 11 8 4 11 9 14 5 3 4 3 7 1 10 14 7 5 9 5 6 5 15 8 11

Represented in hexadecimal format, the key will be: “11 BD144B3A8E6977 1EAE62EF9717B0 8A716B84B9E534 371AE759565F8B”

Here are the four chaotic maps. The coefficients of those dynamical system difference equations are well tuned, and equations all lead to chaos.

0th Logistic map: xn+1 = 3:901xn(1-xn); xn Є (0, 1)

1th Logistic map: xn+1 = 3:931xn(1-xn); xn Є (0, 1)

2th Logistic map: xn+1 = 3:961xn(1-xn); xn Є (0, 1)

3th Logistic map: xn+1 = 4xn(1-xn); xn Є (0, 1)

According to the key, there are four maps involved. Each of them has its own seed, offset, #orbits, #samples. The details are in the above table 1.

Table 1: Chaotic Maps

	Seed	Offset	#Settles	#Orbits	#Sample
Map #0	0.0012391499	0.00001499	135	11	11
Map #1	0.002010722	0.000061335	53	15	4
Map #2	0.009073003	0.000033977	259	7	8
Map #3	0.003611367	0.00002287	125	12	15

We extract the lowest digits from a specific chaotic orbit point xn by the following steps:

Step 1: Removes the decimal point from xn (|xn | is less than 1).

E.g., 0.33461→33461, 0.9442345679457→9442345679457

Step 2: Makes the number 8 digits. If the original number is shorter than 8 digits, we add zeros at the end. If the original number is longer than 8 digits, we chop off the extra digits from the left side.

E.g., 33461 → 33461000, 9442345679457 → 45679457

Step 3: Gets the remainder from the 8 digits number by mod 256, it will be the generated pseudo random number.

E.g., 33461000(mod 256) = 8, 45679457(mod 256) = 97 The generated random numbers are in between 0 and 255 which can give 8-bit binary key in value permutation algorithm.

Compression Algorithm

Image compression is perform using adaptive coding and it can be successfully reconstructed. First, convert the image in text file and generate and update a tree based on each occurrence of

character. If character count increases it moves upward by updating tree. Repeat the process until last character and perform a traversal of tree to generate code table. Data may be encoded by simply by replacing each symbol with its code. The original image is reconstructed. Once the bits read match a code for symbol, write out the symbol and start collecting bits again.

Performance Parameter

PSNR

$$PSNR = 10\log_{10}\frac{h_w\left[\max_{1<i\le m,1<j\le n}\left\{p'_{i,j}\right\}\right]^2}{\sum_{i=1}^{h}\sum_{j=1}^{w}(p_{i,j}-p'_{i,j})^2}$$

Where h and w are the width and height of original image, while Pij and P'ij are pixel values of encrypted image.

Correlation Coefficient Analysis

Correlations between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where x and y are the values of two adjacent pixels in the image.

Histogram analysis

Calculate the histogram of plain image and cipher image to check for similarity. Histogram of cipher image should be significantly different from that of original image, and bears no statistical resemblance to the plain image.

CONCLUSION

The proposed scheme is an efficient encryption scheme for confidential storage and transmission of medical images to produce a high computation speed and high security. Chaotic maps are computationally economic and fast. Chaotic logistic map is used for two phase encryption. In first phase position permutation is applied on decomposed sub blocks of images

and value permutation in second phase gives additional security to resist attack on confidentiality Furthermore lossless compression is also applied to reduce required bandwidth to travel over the network. In future, this technique can be used to encrypt video efficiently.

REFERENCES

1. Bruno Apolloni, Robert J. Howlett, Lakhmi Jain, "Image Information Hiding Encryption Using Chaotic Sequence", 11th International Conference, KES 2007, XVII Italian Workshop on Neural Networks, Vietri sul Mare, Italy, September 12-14, 2007.
2. Neha D Parmar, Neha Pandya, "Analysis Of Encryption And Watermarking Techniques For Secure Bluetooth Transmition Of Image Files", International Journal of Engineering Research and Technology, Vol.2 - Issue 1 (January - 2013).
3. Tapas Bandyopadhyay, B Bandyopadhyay, B N Chatterji, "Secure Image encryption through key hashing and wavelet transform techniques", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.
4. Shoaib Ansari, "Cryptography Technique using Chaotic Map", International Journal of Innovative Research in Engineering and Multidisciplinary Physical Sciences (IJIRMPS) Volume 1, Issue 2, December 2013.
5. Munish Kumar, Anshul Anand,"An Introduction to Image Compression", International Journal of Computer Science and Information Technology Research, Vol. 2, Issue 2, pp: (77-81), Month: April-June 2014.
6. Mohammad Ali, Bani Younes and Aman Jantan, "Image Encryption Using Block Based Transformation Algorithm", IAENG International Journal of Computer Science, 19 February 2008.
7. Mohammad Ali, Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.
8. ZHANG Yun-peng, LIU Wei and CAO Shui-ping, "Digital Image Encryption Algorithm Based on Chaos and Improved DES", Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.
9. Kuldeep Singh and Komalpreet Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", International Journal of Computer Applications (0975 8887) Volume 23 No.6, June 2011.