International Journal of scientific research and management (IJSRM)
||Volume||4||Issue||09||Pages||4607-4611||2016||
Website: www.ijsrm.in ISSN (e): 2321-3418

Medical Image Security Based On Diffusion- Substitution Method

Jeannine Nithya M D, Prabhavathi K
M.Tech (VLSI Design and Embedded System),
Dept. of Electronics and Communication Engineering,
BGS Institute of Technology.
Assistant Professor,
Department of Electronics and Communication Engineering,
BGS Institute of Technology.

Abstract—**In modern applications pertaining to transmission and receiving of multimedia data, the demand for data privacy has never been more significant. Hence, encryption of data becomes very much essential. Many encryption algorithms had been proposed, however, algorithms with high security, good efficiency and high performance are the demands of today's applications. The work proposed in this paper is a diffusion process involving position based transformation with respect to pixels in two stages of encryption. The first stage involves dividing the image into non-overlapping blocks for which the image size is decided by a key. The second stage involves pixel shuffling with a particular pattern within each block in an image. The encryption algorithm implemented in this paper also validates for colour images of RGB format.**

Keywords: diffusion, substitution, position transformation, key

I. INTRODUCTION

With the advancement in the field of wireless technology, transmitting and receiving of multimedia data has created many new applications in areas such as military, biomedical and research areas to name a few. Due to the advancement s in such areas the necessity for privacy of data has become more prevalent. Thus there is a need for securing the multimedia data over the transmission channel from unauthorized use. Hence, encryption of image has become more prevalent in present day and its significance could not be termed trivial. Therefore, a need for better, highly secured, more efficient and high performance encryption technique is required. Some of the encryption methods to provide maximum security are chaos-based encryption, diffusion based encryption, substitution based encryption, etc. In this work, an image encryption technique based on diffusion and substitution is performed. The diffusion process performs position based transformation of block pixels within the block in an image by zigzag approach while the substitution process replaces the block pixels by computing the differences between row and column. i.e., row and column transformation. The combined (diffusion-substitution) method of encryption intends to provide high security.

II. DESCRIPTION OF METHODOLOGY

An image will have high correlation rate among its neighbouring pixels which has intelligible information. Thus, the primary objective of any encryption process based on image is to reduce the correlation factor as much as possible. The following section mentions the basic concepts involved in the process of image encryption.

In this process, the image pixels is divided into several non-overlapping squared and their size (Bs), which is independent based on their secret key.

A. Image diffusion: In the diffusion process each pixel is performed position based transformation on pixel location in a pattern which corresponds to zigzag manner. Prior to this rearrangement of the pixels in the image, the image is divided into blocks which are non-overlapping, So, for each iteration of image encryption process, the block size defined for the image keeps changing, The block size is selected based on the mathematical notation as follows

$$B_s = \sum_{p=1}^{4} K(4(r-1)+p) \qquad \ldots\ldots\ldots\ldots (1)$$

Where,B_s is the Block size, K is the sub-key, p is pixel in an image, r is the rounds of iterations.

B. Image substitution: The image substitution process is carried out by performing simple computation on pixels to change its properties. The separated channels are passed through 8 rounds, after deciding the block size. These non-overlapping squared blocks are passed through column and row transformation. The block size for substitution is selected as shown below

$$B_s = \sum_{p=1}^{4} K(4(8-r)+p) \qquad \ldots\ldots\ldots\ldots .. (2)$$

Where, $\boldsymbol{B_s}$ is the Block size, K is the sub-key, p is pixel, r is the rounds of iteration.

The paper is organized as follows, the first section explains about the encryption process pertaining to the paper. The section gives a review of literature pertaining to the many encryption schemes. The third section explains about the implementation process associated with the proposed system. The fourth section gives the simulation results obtained by implementing the proposed system and the last section gives the conclusion with respect to the overall proposed encryption method.

III. PROPOSED METHODOLOGY

A. IMAGE ENCRYPTION

An object that depicts a visual perception of an object is called as an Image. An image may be of two-dimension and three-dimension. The method in which full encryption that encodes a complete section of an image is said to be as complete image

encryption. The method is used in places where the information is to be kept very confidentially and used for security purposes. Here we use both gray-scale and color images as input. A 128 bit key is generated using the block size in which image, that is to be encrypted is divided into several squared non-overlapping blocks. After the key is generated, pixels are re-arranged with the same block by property mixing. Later, after 16 rounds of iteration we get an encrypted image. The image encryption process is as shown in figure 1.

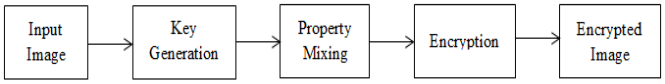

Figure 1: Image Encryption.

Encryption Algorithm:
Step 1: Select a key of 128-bit size. The key should be divided into blocks of 8-bits each called as the session keys.
Here K is referred to as session keys.
Step 2: Let a plain image pass through mixing process by which it decreases the quality of the original image and disturbs the image.
Step 3: The mixing process is as follows:
ipsition of the first session key i.e., 1
for x=1 : H do
for y=1 : W do
$P_{x,y} \leftarrow (P_{x,y} \oplus P_{x,y-1} \oplus K)$
i ← position of next session key i.e., (I mod 16) + 1)
Endfor
Endfor
Step 4: The mixing process continues for 16 times and finally we get an image that is completely encrypted.
Step 5: We get an Encrypted Image of the original image that is taken as an input.

3.2 IMAGE DECRYPTION

Decryption is the reverse method of encryption process. It defines the recover of original data from the encrypted thing. Some of image encryption techniques are used traditionally is data encryption standard. The decryption process flow diagram is as shown on figure 2

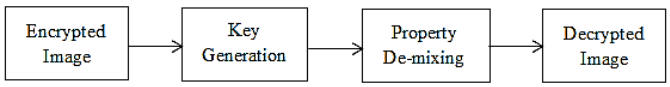

Figure 2: Image Decryption.

Decryption Algorithm
Step 1: Select the encrypted image as input for the decryption process.
Step 2: Select a key of 128-bit size. The key should be divided into blocks of 8-bits each called as the session keys.
Step 3: Perform de-mixing process for 16 iterations.
Step 4: Obtain the original image I (decrypted image).

III. IMPLEMENTATION

The objective of the proposed system is to perform diffusion based encryption and decryption process for a given set of images. The encryption/ decryption process is divided into two parts individually, the first part is called the image property mixing and the second block is the image block reshuffling (which is based on the position based transformation of the image encryption/ decryption process). The block diagram concerning the general system architecture of the proposed system is shown in figure 3 below.

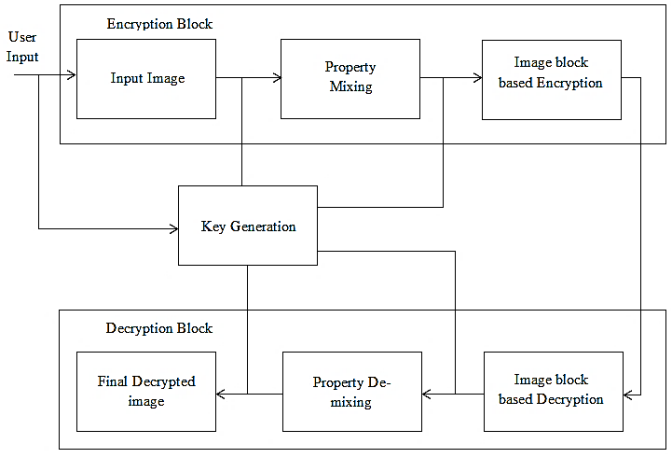

Figure 3: Proposed System Architecture

Initially an input image (plain image) is resized to have an equal dimension of square matrix. A random key is generated which is of the size of the total number of bytes of the corresponding input image.

Decision with respect to size of the block (Block based encryption process)

The image (plain image) to be encrypted is first divided into number of blocks (with respect to pixels) having equal dimensional size (i.e. number of rows and columns are equal).The pixels which do not belong to any blocks are combined to their adjacent blocks. The size of each block in each iteration is decided by a session key (K_i). Different values corresponding to the block size is given in table 1 as shown below.

Table 1 : block size table for image encryption.

$K_i mod\ 10$	0	1	2	3	4	5	6	7	8	9
Block size (B_i)	16	24	32	40	48	56	64	72	80	96

Diffusion process

After the deciding the image block size for that particular iteration, the pixels in that block are rearranged by following the zigzag pattern. The pattern is represented in figure 4 as shown below. Location of the initial pixel which travels in a block is made to be completely dependent on the key. The property of the pixel in the block is changed with their adjacent or neighboring pixels. the location around the pixel is represented in figure5 as shown below.

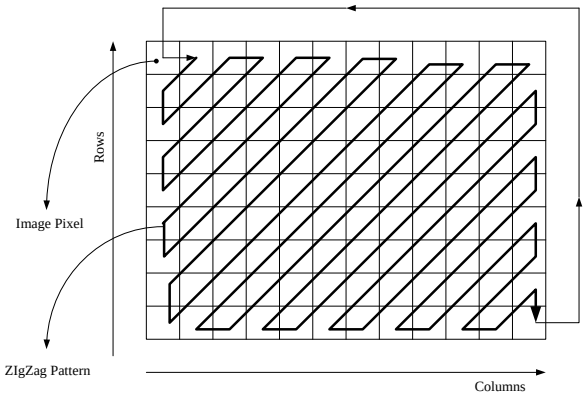

Figure 4 : Zig-Zag pattern for pixel reshuffling (for a single block) for the purpose of image encryption.

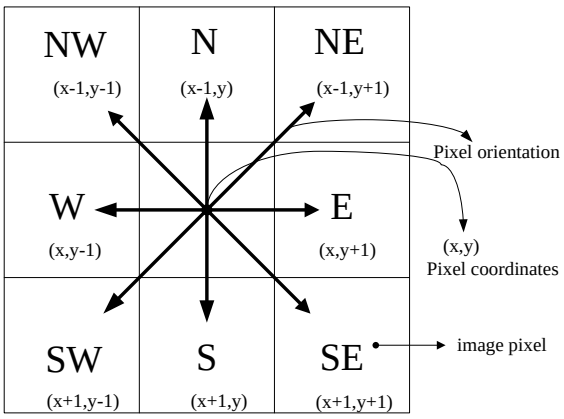

Figure 5: Pixel Location around the Pixel of Interest in the Image.

Property Mixing

In this stage as shown in figure 4.6, every pixel in the plain image is replaced by a new pixel which is obtained as a result of the diffusion process which is mentioned in the above section. In the mixing process, the position of current pixel is defined ($P_{x,y}$). The position previous to this pixel is also considered ($P_{x,y-1}$) and is XORed with the current pixel position, which is given as

$$R_{x,y} = P_{x,y} \oplus P_{x,y-1}$$

Where, $R_{x,y} \rightarrow$ resultant pixel obtained by the mixing process.

The resultant pixel $R_{x,y}$ is again XORed with the value in the respective position of the key (K_i) which is given in the equation below.

$$S_{x,y} = R_{x,y} \oplus K_i$$

Where, $S_{x,y} \rightarrow$ Final resultant image obtained after performing XOR operation with the key K_i

The next position of the session key is computed by calculating i with mod 16 and incrementing by a value of 1, which is given as,

$$i = (i \ mod \ 16) + 1$$

IV. PERFORMANCE ANALYSIS

A. Histogram Analysis.

A Histogram is a pictorial chart that depicts the distribution of a set of data. Unlike Run Charts or Control Charts, which are discussed in other modules, a Histogram does not reflect process performance over time. It's helpful to think of a Histogram as being like a snapshot, while a Run Chart or Control Chart is more like a movie. When user is unsure what to do with a large set of measurements presented in a table, they can use a Histogram to organize and display the data in a more user friendly format. Histogram will make it easy to see where the majority of values fall in a measurement scale, and how much variation there is.

Quality Measurement

This section briefly explains about the performance and security analysis. An encryption scheme must resist any kind of attacks such as cryptanalytic, statistical and brute-force attacks. Here the number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) have been measured to see the influence of changing a small percentage of pixels in the plain image on the ciphered image. Measurement of NPCR is the percentage of different pixel numbers between two ciphered images. UACI measures the average intensity difference between the pixels of two ciphered images. The correlation between the original and encrypted image is also measured, correlation between pairs of the images are produced using the proposed image encryption algorithm by computing correlation coefficients.

B. Number of Pixel Change Rate (NPCR)

The NPPR method is used to evaluate the strength of the image with respect to its encryption and decryption techniques. It defines the rate at which the pixel changes in the image during each iteration. The mathematical definition of the NPCR is given as shown in equation (1),

$$N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\ \% \quad \ldots\ldots\ldots\ldots\ldots\ldots \ (1)$$

$$\text{Where, } D\ (i,j) = \begin{cases} 0, if\ C^1(i,j) = C^2(i,j) \\ 1, if\ C^1(i,j) \neq C^2(i,j) \end{cases}$$

C^1 is the cipher image before pixel change, C^2 is the cipher image after pixel change, T is total number of pixels in the cipher text, i, j is pixel coordinates.

The NPCR focuses on the absolute number of pixels in the image which changes during the differential attacks.

C. Unified Average Changed Intensity (UACI)

The UACI method is defined as the difference between two paired images with respect to its cipher text image. The UACI is mathematically defined as in equation (2),

$$U(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\ \% \quad \ldots\ldots\ldots\ldots\ldots\ldots \ (2)$$

Where, F is the highest supported pixel value which is compacted with a cipher text image format.

D. Correlation coefficient

Correlation coefficient is computed to find the measure of relativity between two samples of interest. The mathematical representation is as shown in equation (3).

$$r = \frac{n(\sum_i xy) - (\sum_i x)(\sum_i y)}{\sqrt{[n\sum_i x^2 - (\sum_i x)^2][n\sum_i y^2 - (\sum_i y)^2]}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \ (3)$$

Where, r is the correlation coefficient, n is the total number of elements, i is the number of elements in x and y (individually), x is the first sample, y is the second sample.

V. EXPERIMENTAL RESULTS

This session deals with the simulated results obtained from the implementation of the project with respect to image encryption/ decryption process. The following sections are mentioned as follows. Table 2 deals with the brief mentioning of the structure and attributes of the database with respect to images. Table 3 shows the obtained results from the proposed system

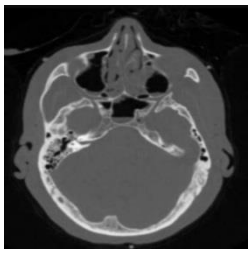

Figure 6: Input Image.

Figure7: Complete image encryption and decryption

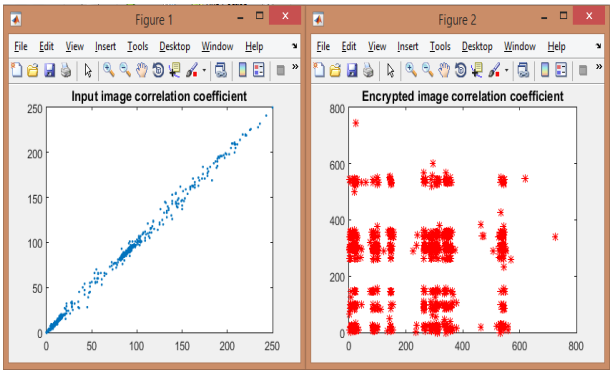

Figure 8: Correlation coefficients of the original and encrypted image.

The database considered for implementation in this project consists of five images of type unsigned integer (8 bits) with the following attributes mentioned in table 2.

Table 2: Database for the implementation of the project.

Input	Image size	Bytes	Class	Min & Max value
Backbone	400 X 400	160000	Uint (8 bits)	0 – 255
Brain	720 X 720	518400	Uint (8 bits)	0 – 255
Ultrasound	512 X 512	262144	Uint (8 bits)	0 – 255
Baboon	298 X 298	88804	Uint (8 bits)	0 – 255
Leena	512 X 512	262144	Uint (8 bits)	0 – 255

Table 2 represents the database implementation for the project in terms of Image size, Bytes, Class, Minimum and Maximum values.

Table 3: Measurement of the simulation results

IMAGE	NCPR	UCAI	CC (Input Image)	CC (Encrypted Image)
Backbone	0.9979	0.4754	0.9984	-0.03477
Brain	0.9952	0.5539	0.9988	-0.04294
Ultrasound	0.9980	0.6243	0.9979	-0.04160
Baboon	0.9986	0.4334	0.9879	-0.04025
Leena	0.9986	0.4344	0.9913	-0.04467

Table 4: NPCR and UACI values.

Input Image	NPCR Score	NPCR Pixel Value	NPCR Distance	UACI Score	UACI Pixel Value	UACI Distance
Backbone	0.997	1	[0.996 1.407]	0.475	0	[0.334 2.025]
Brain	0.995	1	[0.996 1.407]	0.556	0	[0.334 2.025]
Ultrasound	0.998	1	[0.996 1.407]	0.624	0	[0.334 2.025]
Baboon	0.998	1	[0.996 1.407]	0.433	0	[0.334 2.025]
Leena	0.998	1	[0.996 1.407]	0.434	0	[0.334 2.025]

Table 3 represents the performance analysis of the project. The correlation coefficients of the original and the encrypted images. The given table 4 shows the obtained results after evaluating the results.

VI. CONCLUSION

The diffusion based encryption and decryption methods are successfully performed by applying position based transformation in two stages respectively. The key generated is of random in nature represented in a hexadecimal format. Individual keys are generated for the above encryption operations. It is observed that good encryption was performed with respect to images of all types and formats; however the constraint of image dimensionality still persists. The proposed system also performed good encryption for color images pertaining to RGB (Red, Green and Blue) component along with the gray scale images. By using diffusion based encryption and decryption algorithm for complete image we have got a secure algorithm but in future work we have to adopt other encryption and decryption techniques which consume even more less time for its computation.

REFERENCES

[1] "Narendra K. Pareek, Vinod Patidar, Krishan K. Sud, Diffusion-substitution based gray image encryption scheme", Digital Signal Processing, Volume 23, Issue 3, May 2013.(Base Paper)

[2] "A. Awad and A. Miri, A new image encryption algorithm based on a chaotic DNA substitution method," *Communications (ICC), 2012 IEEE International Conference on*, Ottawa, ON, pp. 1011-1015, 2012.

[3] "J. m. Liu and Q. Qu, Cryptanalysis of a Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Map," *Information Processing (ISIP), 2010 Third International Symposium on*, Qingdao, pp. 67-69, 2010.

[4] "X. Fei and G. Xiao-cong, An Image Encryption Algorithm Based on Scrambling and Substitution Using Hybrid Chaotic Systems," *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, Hainan, pp. 882-885, 2011.

[5] "A. J. Paul, P. Mythili and K. Paulose Jacob, Matrix based cryptographic procedure for efficient image encryption," *Recent Advances in Intelligent Computational Systems (RAICS), IEEE*, Trivandrum, pp. 173-177, 2011.

[6] "J. Bhaumik and D. R. Chowdhury, Design and implementation of Cellular Automata based diffusion layer for SPN-type block cipher," *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on*, Dhaka, pp. 828-831, 2012.

[7] "A. Jain and N. Rajpal, A two layer chaotic network based image encryption technique," *Computing and Communication Systems (NCCCS), 2012 National Conference on*, Durgapur, pp. 1-5, 2012.

[8] "J. S. Khan, A. ur Rehman, J. Ahmad and Z. Habib, A new chaos-based secure image encryption scheme using multiple substitution boxes," *2015 Conference on Information Assurance and Cyber Security (CIACS)*, Rawalpindi, pp. 16-21, 2015.

[9] "J. Khan, J. Ahmad and S. O. Hwang, An efficient image encryption scheme based on: Henon map, skew tent map and S-Box," *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*, Istanbul, pp. 1-6, 2015.

[10] "Naveenkumar S K, Panduranga H T and Kiran, "Chaos and Hill Cipher Based Image Encryption for Mammography Images," *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*, Coimbatore, pp. 1-5, 2015.

[11] "M. S. Elpeltagy, M. M. Abdelwahab and M. S. Sayed, Image encryption using Camellia and Chaotic maps," *2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Abu Dhabi, pp. 209-214, 2015.

[12] "S. Rohith and B. K. Sujatha, Image encryption and decryption using combined key sequence of Logistic map and Lozi map," *Communications and Signal Processing (ICCSP), 2015 International Conference on*, Melmaruvathur, pp. 1053-1058, 2015.

[13] "T. Sukumar and K. R. Santha, An approach for secret communication using adaptive key technique for gray scale images," *Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on*, Nagercoil, pp. 1-5, 2015.

[14] "M. Bertilsson, E.F. Brickell, and I. Ingemarson, Cryptanalysis of video encryption based on space-filling curves," in Proc. *Advances in Cryptology–EuroCrypt'88, Lecture Notes in Computer Science*, vol. 434, Springer, Berlin, pp. 403–411, 1989.

[15] "M. Kuhn, Analysis for the Nagravision video scrambling method," *1998, online document*, available at: http://www.cl.cam.ac.uk/ mgk25/ nagra.pdf.

[16] "J. McCormac, European Scrambling Systems 5: Circuits, Tactics And Techniques" – The Black Book, Waterford University Press, 1996.

[17] "W. Li, Y. Yan, and N. Yu, Breaking row-column shuffle based image cipher," in Proc. *20th ACM international conference on Multimedia (MM'12), New York, NY, USA*, pp. 1097–1100, 2012.