RESEARCHERID
THOMSON REUTERS

[Kumari, 4(10): October 2017]
DOI- 10.5281/zenodo.1006761

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

AN EFFICIENT METHOD FOR SECURED TRANSFER OF MEDICAL IMAGES

M. Sharmila Kumari[*1] & Sudarshana[2]

[*1]Professor, Department of Computer Science and Engineering, P A College of Engineering, Mangalore
[2]Department of Computer Science and Engineering, P A College of Engineering, Mangalore

ABSTRACT

Transmission of multimedia data is in a secured manner in different channels is found to be one of the complex tasks. Due to heavy traffic in the network,chances of data drop are also very high. In such cases, intruder or any third party can tap the information where the security is compromised. Hence to reduce the transmission time, a novel method is introduced here that provides security of the data as well as compression for faster transmission of data. We have seen substitution cipher scheme has gained prominence in the cryptographic system. The proposed technique considers two arrays namely row array and column array where encrypted data is stored. Encryption is based on the key of random array. All color components of the pixels of the image are encrypted individually. Addition modulo 256 is applied one pixel values using a random number. Individually encrypted colors are combined together to form an encrypted image. This encrypted image is compressed using Deflate compression technique. Performance of the proposed method is evaluated on many images and comparative study with the existing system revealed that the proposed system possess better performance.

Keywords*: Encryption, Decryption, Compression, Medical Image Transfer*.

I. INTRODUCTION

Digital communication via secured media is one of the fundamental research problems in the current technological advancements in the field of computer networks. People use diverse transmission methods to communicate with one another. The data or information exchanged between the communicating parties can be wired or wireless. Information sharing is the important issue in any communication system. Transmitted data can be textual or multimedia. Hence the information or data transmitted between communications parties should be secured enough. When image is the source of information, the security of the image is essential. We here focus on transmission of images. Some of the applications of image transmission are patients' X-Ray/MRI images in hospitals, defense, satellite communications, astronomical data, weather forecast, industries, etc. In all these areas, image transmission plays a vital role where providing security for these images it is considered utmost important.

In this work, medical image is taken as the information source for the transmission. At the sender side, image is encrypted and sent through the transmission channel. The original image is obtained by the appropriate decryption process.Image encryption is the process where a suitable encryption algorithm and keys are used to convert an original image in to cipher image. Using the decryption algorithm and key original image can be obtained back. In this work, along with security, compression of image too is addressed. To accomplish this, an efficient compression technique is applied by which transmission time is reduced. By encrypting and compressing the encrypted data, the objective of the work is achieved.

II. LITERATURE SURVEY

BibhudendraAcharyaet. al. [1] proposed an algorithm with usage of involutory key matrix. Process starts with accepting an image as input, the RGB components should be decomposed from image, each pixels should be encrypted with advances hill cipher method, first step is to find the involutory key matrix, symmetric blocks can be made via image. Then pixels of every block can be taken, using that construct temporary block. On each newly

created temporary block apply the hill cipher procedure. A matrix can be obtained after applying hill cipher. For that matrix transpose matrix is calculated, transposed matrix got after encryption which is put in i^{th} spot block associated with the encrypted image. Advanced process is better than normal hill cipher which provides better security against attacks and also is reliable.

Ganesh Kumar et. al. [2] proposed a new method to secure the image from different attacks, colors of the image will be braked using the procedure of coloring algorithm, which divides the RGB colors present in the image. As a result of division, different blocks are created. These blocks contain different individual color blocks of vertical as well as horizontal are there. These colored blocks are shuffled depending on the position and encrypted using blow fish method of encryption. For more secured encryption a 128 bit public key is added. Using three different color images a single image is created by merging them. This provides more correlation effect. Hacker cannot find the correct image as the image size is dependent on the block created.

Fahoum and Harb B [3] proposed a new compression technique with combination of fractal and wavelet algorithm. Using wavelet transformation process, the read image is decomposed. Fractal coding is applied on the low frequency components of the image and high-frequency using threshold coding process, which is called as Adaptive Wavelet. Low-resolution parts can be compressed using fractal process and high resolution parts using Wavelet process. In encoding process segmentation, segmentation will be done first, after which block pool is created. Then affine mapping will be done and non-similar parts are removed. After the encoding process, the bits are sent to the decoder process, to decode. Here inverse fractal and inverse wavelet process is used after which finally original image is reconstructed.

Rawat and Maher [4] proposed hybrid process of compression using fractal and DCT. A colored image is taken as input and divided into portions and then DCT method is applied. This is followed by the quantization zigzag scan. Fractal encoding and Huffman coding is applied to the scanned image that results in a compressed image. For decompression, Huffman decoding and fractal decoding will be applied for compressed image. Then, inverse quantization process is done followed by inverse DCT. Finally we get back the original image. By using this hybrid method, artifacts are easily overcome and analogous blocks which appear continuously for compression will be eliminated.

Sharma and Kaur [5] proposed a combined image compression method using DCT and DWT as well as Huffman coding. The process starts by loading an image of size 256×256 followed by extracting and separating the RGB component from the image. Then, DWT compression is applied which contains two major step which decides the threshold values that are known as hard threshold and another referred to as soft threshold. DCT compression is then applied to individual RGB components. The histogram probability reduction function is applied on every RGB components followed by image quantization. Finally it is Huffman coded.

Kurihara et.al. [6] proposed to compress image after encryption. This can provide compression performance nearly same as that of compression provided by jpeg. Encryption process has mainly four blocks. Here image pixels are separated into non overlapped serial blocks. Then, block scrambling process is done where each block is randomly permuted followed by block rotation and block inversion. Block rotation is the process where each block is randomly rotted either 0, 90, 180, 270 degrees. After block rotation, negative positive transformation takes place where pixel values are reversed in each block using a random numbers. Then, color component shuffling is done for each block using a random integer to permutes the values along the RGB components. Finally they are integrated.

Radha [7] proposed compound image compression process using encryption techniques. This method combines the encryption process and compression process. The method has three steps. First is conversion of color space, where color is converted into one luminance and two chrominance, i.e. YUV. Next step is the scrambling process where plain image will be scrambled, then mixing process is done where scrambled image is mixed using a chaotic map. This scrambling process provides high security from the different attackers. Next step is compression where jpeg compression is adapted. The proposed method is fast as well as secured process because of key space is very huge.

Agrwal [8] proposed pixel shuffling method to simultaneously perform encryption, compression which is related to steganography oriented process. DCT method is used for compression and encryption is based on pixel shuffling process. Input image is divided into blocks and then applied DCT for each block followed by quantization. Quantized data is entropy encoded. Finally obtained image is of reduced size. Then encryption in column and pixel with row are changed resultant image obtained. Then pixel shuffling decryption process will take place where encrypted image is taken as input and row as well column pixels are swapped. The original image obtained after decryption process. For obtained image, steganography process will be applied. This method lessens the bandwidth for transferring the image over the network.

III. PROPOSED WORK

Fig 3.1 represents the overall procedures which are carried out with the proposed system. Image data is read from the source and is forwarded to the encryption module. Encryption moduleuses transposition method with additive modular operation.

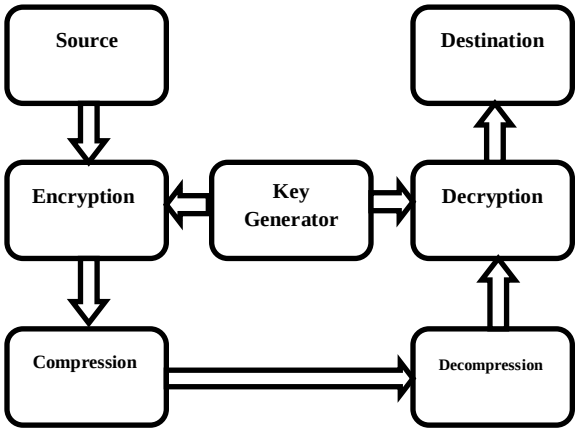


Fig 3.1: Block diagram of the proposed system

First, the image contents are stored in a two arrays. Column array stores column elements and row array stores the row elements. First, row elements are shifted, then column elements followed by encryption. Using a suitable key generator, different keys are generated. Additive modular encryption is applied to the encrypted column elements where each colors of the pixels is individually encrypted. Finally individually encrypted colors are merged, which results in an encrypted image.The encrypted image is then compressed. Deflate is used for compression. Using this, image is compressed and stored in an array which is then transmitted. In the destination side, received data is un-compressed using inflator function followed by decryption using inverse transposition where inverse additive function is applied. Encrypted column array is decrypted first, then row decryption, then finally decrypted row pixels form the original image.An image can be thought as two-dimensional arrays of pixels. The length of these arrays is identical to image width and respective height. This particular property is considered in proposed method. The process of encryption has the following set of steps:

Step 1: Random Numbers generation
Two arrays namely row Array, and columns Array are used for shifting the pixels, one for row shifting and another for column shifting. Unique values are generated randomly for these arrays. The size of row Array is equal to image width and the height is considered for the size of the column Array. That is, Array which is respect to row it is in between 0 and image width and array values with respect to column in between 0 and image height. Unique values are considered for each.

Step 2: Extraction process of pixels
Pixels of the input image are extracted and stored in a 2D which is then used for encryption process.

ISSN 2348 – 8034
Impact Factor- 4.022

Step 3: Row Encryption

In this step, a row of pixels is taken at a time. Each pixel shifted in random procedure. Based on the values present in the row array, column array is created which is two dimensional and it holds the encrypted pixels values.

Step 4: Column Encryption

In this step, a column of pixels from encryptedRowArrayis taken at a time. Each of these pixels has been shifted randomly based on the values in the respective column Array. For these shifted pixels a new array is created.

Step 5: Additive Encryption

Encrypted column array contains the reordered pixels. Here, each color component of the pixels are encrypted individually. A color value is taken at a time, and is added with some random value. Mod 256 has been used to accomplish this task.

red = (red + random value) mod 256;
green = (green + random value) mod 256;
blue = (blue + random value) mod 256;

Step 6: Reformation of Pixels

In the final step, these individual encrypted colors are combined together which forms the encrypted pixels. Using these pixels, encrypted image is created. Decryption process will follow the same method as encryption. Here the mod value is taken as 256, since the maximum level of the pixel is 255.

red = (red - additiveArray[i]) mod 256;
green = (green - additiveArray[i]) mod 256;
blue = (blue - additiveArray[i]) mod 256;

Encrypted column array will be decrypted then encrypted row array will be decrypted, finally we obtain the original medical image.

Compression and decompression process

The encrypted image is used for compression process where the data size will be reduced which is based on each byte. Here, Deflate is used for compression purpose, Using this Deflate function, we can compress the data in bytes and store in the array After compression, data is sent to destination side, where the compressed data is uncompressed using inflator method.

IV. RESULTS AND ANALYSIS

This proposed method is evaluated for different parameters of security for preventing the attacks.Some of the security parameters evaluated are Histogram, plain text image and cipher text image visualization, standard deviation, entropy, quality of encryption, avalanche effect.

Plain text image and cipher text image visualization test: Figure 4.1 indicates the original medical image taken for encryption process. The encryption process is such a way that there is no trace in the encrypted image which is shown in figure 4.2. All the pixels are encrypted row wise and column wise with the additive modular encryption and transposition method.

ISSN 2348 – 8034
Impact Factor- 4.022

Fig 4.1: Original medical image

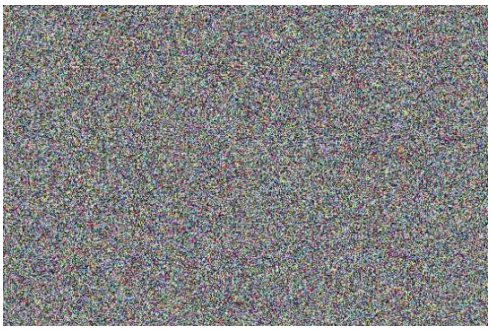


Fig 4.2: Encrypted medical image of the proposed work

The proposed system is compared with following three methods, namely single FSR (Feedback Shift Register), double FSR and triple FSR along with the graph representation**.**

Single FSR key generator model with modular additive encryption: In single FSR, only one FSR is used with the additive modular 256. Here, RGB components are extracted from the image and kept in an array. Varying key length such as 16, 32, 64 and 128 may be used. Additive modular operation is done by first adding the array[0] position element and array[2] position elements, then shifting the elements and added result is given as feedback to array[3]. Same procedure is repeated to all positions. In decryption reverse operation will be done subtracting the added values and then shift operation. As only one FSR is used, security is low.

Double FSR key generator model with modular additive encryption: In double FSR, there are two FSR used with additive modular 256 operation. RGB components are extracted and kept in an array, Different key lengths such as 16, 32, 64 and 128 may be used. Value of array[0] position element is added with array[2] followed by shifting and placing the result in array[3]. Procedure is repeated to all the position. Here two shifts are used. In decryption, reverse operation is done by subtracting the added values and shift operation.

Triple FSR key generator model with modular additive encryption: In Triple FSR key generator model there are three FSR with the additive modulo 256. RGB components are extracted and kept in an array. Different key length such as 16, 32, 64 and 128 bits may be used. Feedback operation is done by using three feed backs taking three different arrays to store the values in first, second and fourth position element are added and stored in an array and shifted. Then feedback is given to next position. Same procedure repeated to all the position. In decryption, reverse operation will be done subtracting the added values and shift operation.

In proposed encryption method the medical image is considered as input, the row array and column array will be created to store the values of row elements and elements of the column, using random key generator the row

elements are encrypted first and stored, and from the stored encrypted row arrays column elements will be encrypted and additive modulo 256 operation is done. This gives a high quality of encryption.

Histogram evaluation: The original pixel & encrypted pixel values of the medical image are considered to plot the histogram. The histogram is plotted by representing the pixel value of the image on the x-axis and its frequency on the y-axis. Image is considered to be of size 200x200.

Fig. 4.3 shows the histogram of red pixel and Fig 4.4, the histogram of encrypted red pixel. From the graph, observable aspect is that red pixels values have shown large difference. The red values in the range of 30000, 28000 and 8000 in original image are decreased to 900, 700 and 1000 in the encrypted image.

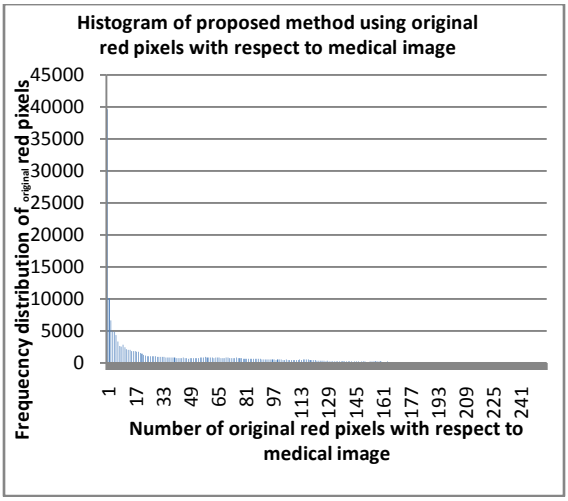


Fig 4.3: Histogram of original red pixels frequency of occupancy with respect to medical image show in fig 4.1

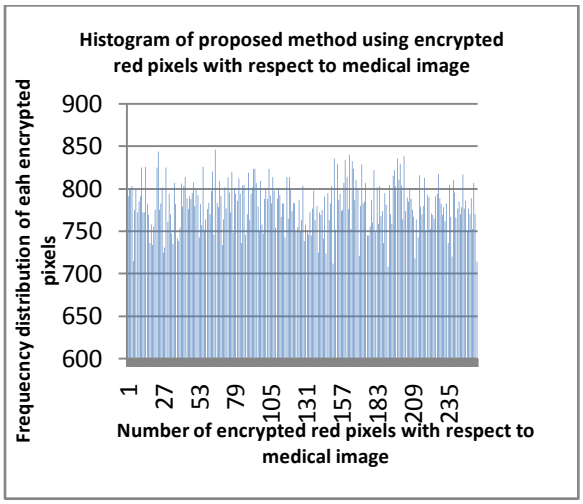


Fig 4.4: Histogram of encrypted medical images of the part of red pixels frequency of occupancy

.

Fig 4.5 shows the histogram of the green pixels. The pixels values moves up to a peak value of 35500 as it is the original green value. Fig 4.6 shows the histogram of encrypted green pixels. When encrypted green pixels are used for calculating the histogram, large difference is shown in the graph, which is very low as relate to original values occurrence.

ISSN 2348 – 8034
Impact Factor- 4.022

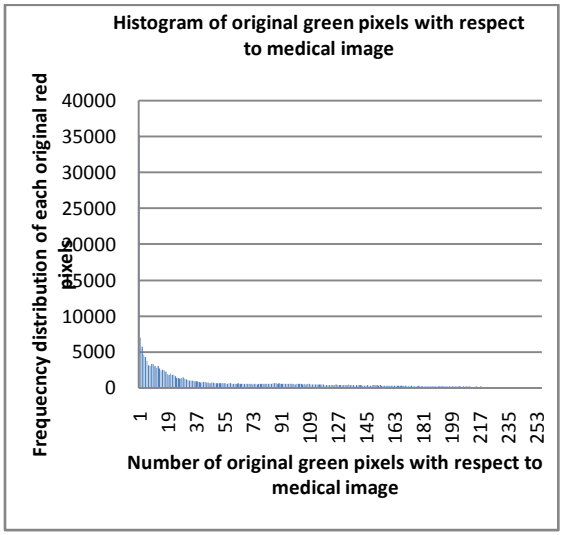


Fig 4.5: Histogram of original green pixels frequency of occupancy with respect to medical image show in fig 4.1

The histogram of original blue pixels is plotted in Fig 4.7 and the histogram of encrypted blue pixels is plotted in Fig 4.8. The graph indicates the pixels values vary from 39000 to 1000 in the original to 800 to 1000 after encryption. The blue pixel frequency values are found to be decreased in the encrypted image.

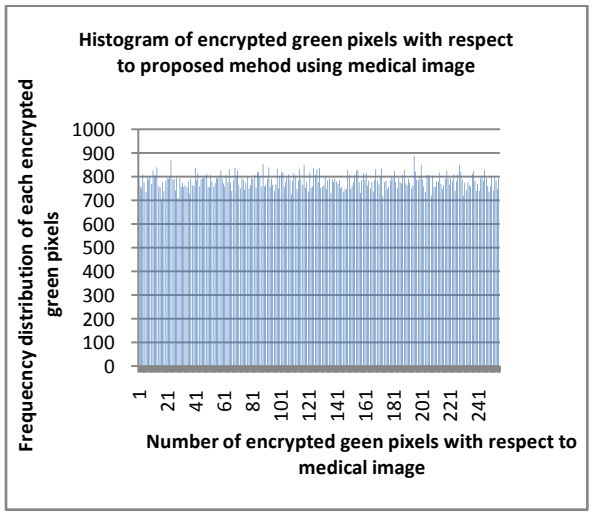


Fig 4.6: Histogram of encrypted green pixels frequency of occupancy with respect to medical image

ISSN 2348 – 8034
Impact Factor- 4.022

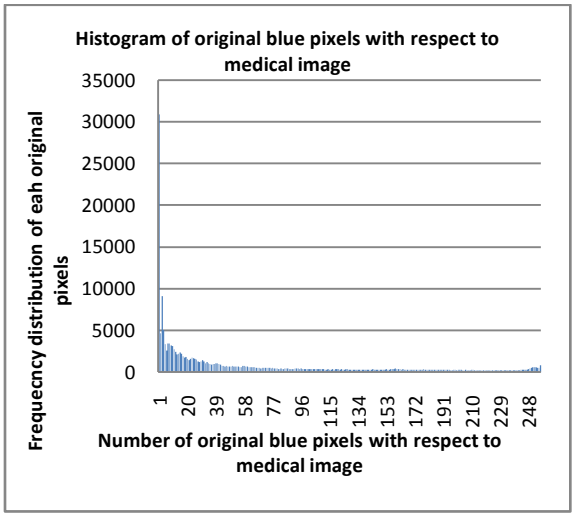


Fig 4.7: Histogram of original blue pixels frequency of occupancy with respect to medical image show in fig 4.1

Standard deviation: Graph of Fig 4.9 indicates the standard deviation of original and encrypted pixels. Standard deviation is higher in pixels which are original but lower deviation in encrypted pixels. Standard deviation of occurrence of blue pixel is low because blue components of the pixels is in large amount in the original image and after encryption the standard deviation happens to be very low when compared to red and green as it gets spread uniformly.

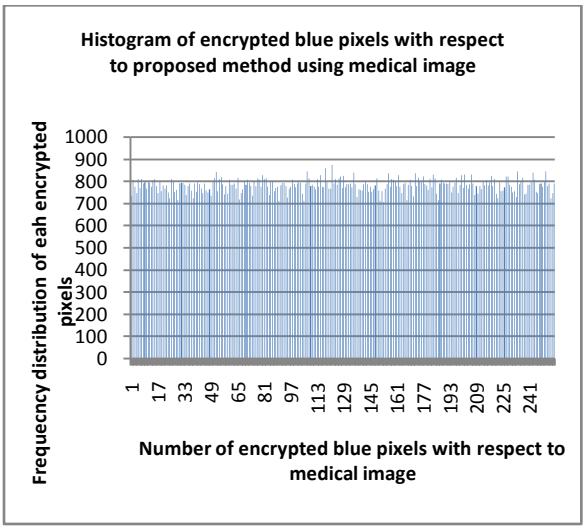


Fig 4.8: Histogram of encrypted blue pixels frequency of occupancy with respect to medical image

ISSN 2348 – 8034
Impact Factor- 4.022

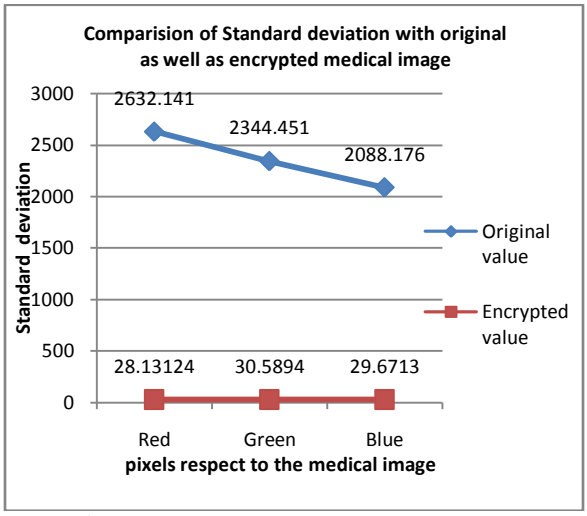
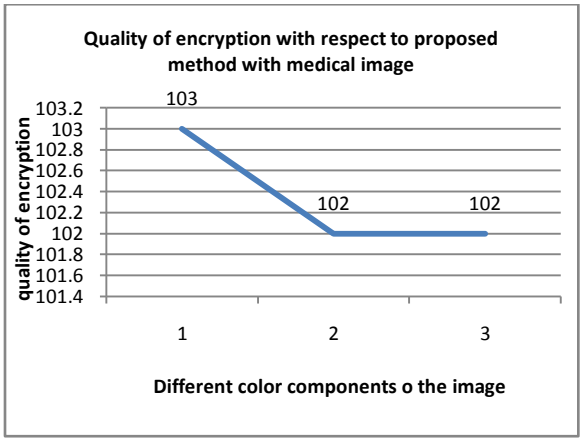


Fig 4.9: Standard deviation comparisonfor the proposed method with original and pixels which is encrypted with respect to medical image

Before encryption, the standard deviation was 2500 for every color components, but after encryption the standard deviation is around 30, so encryption makes maximum amount of decrease in standard deviation. The standard deviation is 2632.141 and 28.13124 for original and encrypted red respectively, 2344.451 and 30.5894 for original and encrypted green respectively and 29.6713 and 2088.176 for original and encrypted blue respectively, which indicates that after encryption the occurrence has decreased. This provides more security from the different attackers.

Quality of encryption evaluation: Encryption quality of proposed with medical image is about 103 for red component, for green component it is 102 and for blue it is 102 as shown in Fig 4.10.



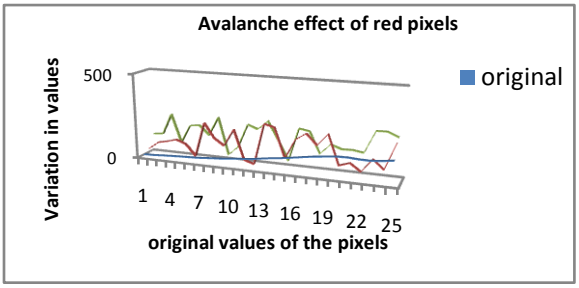


Fig 4.10: Quality of encryption for the proposed method for all three components of pixel using medical image.

Entropy evaluation: Entropy is calculated for encrypted as well as real image as plotted in Fig 4.11.

ISSN 2348 – 8034
Impact Factor- 4.022

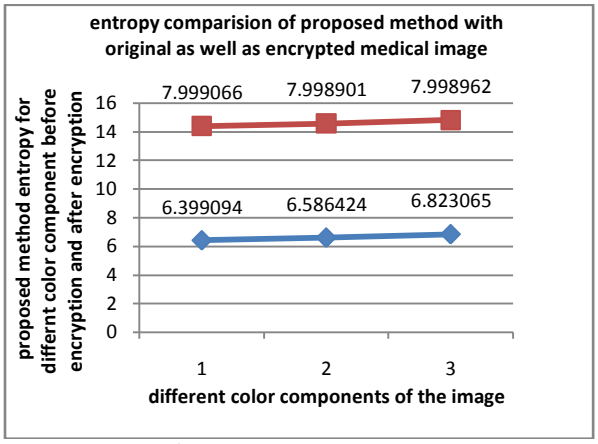


Fig 4.11: Entropy comparison of proposed method with original as well as encrypted pixel

It is found to be more encrypted which indicate that it has a good security. The original values are in the range of 6 which increases after encryption. For original red, it is 6.399094 but in encrypted 7.999066 that is better than original entropy. In green, entropy is 6.586424 which is less compared with 7.998901 for encrypted and is 7.998962 for encrypted blue.

Comparison with existing methods: Comparison analysis of standard deviation is shown in fig 4.12 and table 4.1. Here the proposed method is compared with other existing methods. The blue line directs the red pixels standard deviation values, red link specifies the green pixels standard deviation values and green line indicates blue pixels standard deviation values. In the graph x axis signifies the color components and y axis denotes the standard deviation. The result of the graph indicates that the standard deviation of proposed method is better than other methods.

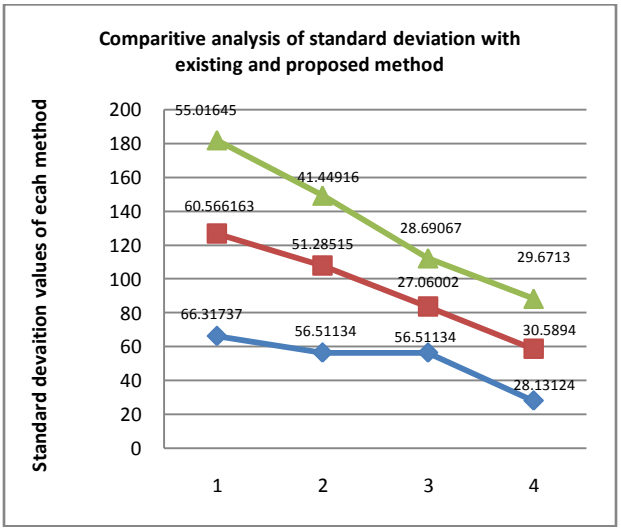


Fig 4.12: Comparative analysis of standard deviation of existing and proposed method

ISSN 2348 – 8034
Impact Factor- 4.022

Table 4.1: Standard deviation of existing and proposed method

Method	SD of Red pixels	SD of Green pixels	SD of Blue pixels
Proposed	28.13124	30.5894	29.6713
Single FSR	66.31737	60.56163	55.01645
Double FSR	56.51134	51.28515	41.44916
Triple FSR	34.20689	27.06002	28.69067

Entropy comparison: Comparison analysis of entropy is shown in figure 4.13 and Table 4.2. Here proposed technique is compared with other existing methods. The vertical line directs the entropy values of different methods and horizontal line specifies the methods. For proposed method entropy of red components is 7.999066 which is better than other methods which are little low. Entropy of proposed method for green is 7.998901 which is more than single and double FSR but comparatively less than triple FSR. The entropy for blue components is 7.998962 which is similar with other procedures.

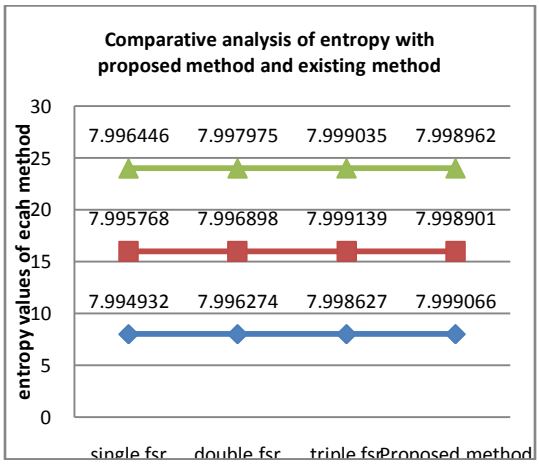


Fig 4.14: Comparison of entropy between proposed method and existing method

Table 4.2: Entropy values of existing and proposed method

Method	Entropy of Red pixels	Entropy of Green pixels	Entropy of Blue pixels
Proposed	7.999066	7.998901	7.998962
Single FSR	7.994932	7.995768	7.996446
Double FSR	7.996274	7.996898	7.997975
Triple FSR	7.998627	7.999139	7.999035

Quality of Encryption: Quality of encryption comparison is done for single, double, triple and method which is proposed in the Table 4.3. The encryption quality of transposition method is calculated for medical image. For red it is 92, for green 87 and for blue 89. The quality of encryption of proposed method with Lena image is calculated, for red 85, for green 78 and for blue 69. For Lena in single FSR it is 103, for green 101 and 102 for

blue. In double FSR encryption, quality for red is 102, for green 101 and 102 for blue components, but in the triple FSR 102 for all the components.

Table 4.3: Comparison of the Quality of encryption of existing and proposed method

Image type	Medical			Lena		
Method	**red**	**green**	**blue**	**red**	**green**	**Blue**
Proposed	103	102	102	85	78	70
Single FSR	103	101	102	84	79	70
Double FSR	102	101	102	84	79	70
Triple FSR	102	102	102	84	77	70

V. CONCLUSION

We have proposed a secured image transfer method which exhibit better performance when compared to earlier methods. The similarly comparisons of entropy clearly shows that security aspect is high because of entropy value is 7.999066. This also predicts the stubbornness of the encryption scheme. In the case of avalanche effect a small variation in the seed value of the key there will be high change seen in the pixel value with respect to the original one. As the compression ratio is good, it shows that reduction in data which allows the reduced transmission time. Also in case of visual testing, the traces of the image are not available in the encrypted image. Flat histogram shows all pixel levels are occurring equally in case of cipher text compared to that of the plain text. This also indicates that the cryptosystem is effective..

REFERENCES

1. *Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra and Ganapathi Panda "Image encryption using advanced hill cipher algorithm" An International Journal of Recent Trends in Engineering and technology, Vol.1, No. 1, Nov 2009.*
2. *K. Ganesh kumar D. Ariazhagan and S.Sundaram "Advanced cryptography algorithm for symmetric image encryption and decryption scheme for Improving data security" Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 10 March2014 563.*
3. *Al-Fahoum A and Harb B "A combined fractal and wavelet angiography image compression approach" an open medical imaging journal, 2013, 7,9-18 9.*
4. *Chandan Singh Rawat and Sukadev Maher "A hybrid image compression scheme using DCT and Fractal image Compression" The international Arab journal of information technology Vol.10, No. 6, November 2013553.*
5. *Sandhya Sharma and Sarabjeet Kaur "Image compression using hybrid of DWT, DCT and Huffman coding" International journal for science and emerging technologies with latest trends 5(1): 19-23(2013).*
6. *Kenta KURIHARA, SAYAKA SHIOTA and Hitoshi KIYA "An encryption then compression System for JPEG standard "Tokyo Metropolitan University, Hino, Tokyo, 191–0065, Japan 978-1-4799-7783-3/15/$31.00 ©2015 IEEE.*
7. *V.Radha "Secured Compound Image Compression Using Encryption Techniques" Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA*
8. *Navita Agarwal "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography" International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue.5, May 2013, pg.376 – 385*