Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Cryptography of Images Using Diffie Hellman Algorithm

Simrat Kaur[1], Rupinder Kaur[2]

[1]Computer Science Department, BBSBEC, Fatehgarh Sahib, Maharaja Ranjit Singh Punjab Technical University
[2]Computer Science Department, BBSBEC, Fatehgarh Sahib, Maharaja Ranjit Singh Punjab Technical University

Abstract — *The Digital data is widely transferred over the internet due to which it may get effected by the intervention of intruders, data tampering, unauthorized access etc. Thus to fulfill the need of data security the cryptography comes to the existence and accepted worldwide. Cryptography is a mechanism to encrypt the data in non-readable format by using a key which is only known to the sender and receiver of the information. This study develops a new encryption based cryptography approach for securing the information of the images. The proposed approach is a combination of two prominent security methods i.e. Diffie Hellman key generation mechanism, Huffman Encoding technique and XOR operation is also used to compressed data and diffie permuted key to achieve the encrypted file. This mechanism provides two-level security to the images by firstly compressing the image and then encrypting it by using XOR operation. In order to approve the proficiency of the work the present technique is compared with the chaotic-ANN encryption technique in terms of NCPR, UACI, correlation, PSNR, MSE and Entropy. The evaluated NCPR of present method is 100, UACI is52.526 and Entropy is 7.9948.*

Keywords- *Digital Data Security, Cryptography, Diffie-Hellman Algorithm, Huffman Encoding*

I. INTRODUCTION

Generally, the cryptography is a tool that used the encryption of digital documents in order to ensure the security of the information. It protects the information from unauthorized users by converting it to the unreadable format. The basic idea of cryptography is to achieve the secure data sharing over the public network. Only those users who have the private key can only encrypt or decrypt the information.

Cryptography can be applied to the medical images in order to retain the integrity and privacy of the embedded information on the images. The potential of the cryptographic mechanism relies upon the length of the encryption key. If any of the encryption mechanism satisfies the following defined criteria only then it is said to be computationally secure.

a. It charges more for breaking the cipher text in comparison to the conversion of actual text to cipher text.
b. The time required to convert the cipher text to plain text should be exceeds the useful lifetime of the information

The basic idea of cryptography is to change the original message in such a format that it could not be recognized by unauthorized user. It is beneficial to retain the confidentiality of the secret information.

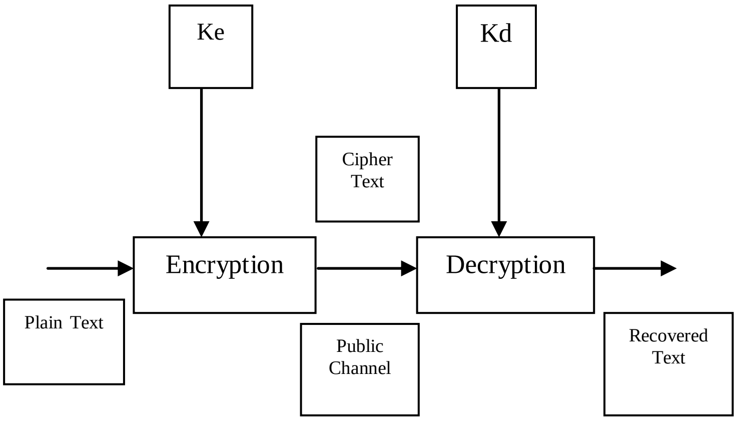

Figure 1. Cryptosystem [16]

The figure 1 depicts the process that is followed by cryptosystem to crypt the data. The essentials of discrete cryptosystem are defined below:

- A set of original message which is known as plain text (P).
- A set of Cipher Text which is defined by C.
- A set of keys that are used for encryption and decryption process and symbolized by K.
- A possible encryption and decryption framework which is depicted by E and D.

Techniques Used:

Diffie –Hellman Algorithm: It is specifically used for sharing the keys which are used for cryptography. It is oldest method which is applied for securing the key sharing. In deffie Hellman algorithm it is not necessary for the sender to have any knowledge regarding receiver of the message.

Huffman Coding: In Huffman encryption method all the pixels are considered as symbol. This technique is implemented on the basis of the frequency for which data repeating it. The symbols associated with high frequency are allocated with least number of bits and on the other hand the symbols that are associated with low frequency are allocated with large number of bits. This encoding method is comprised of code book. The code book contains all the codes used for generation of image. The encryption method operates in following way.

- Disintegrates the image into 8x8 blocks.
- All the pixels and block are considered as a symbol i.e. to be coded.
- Calculate the Huffman codes for set of pixels.
- Finally, encrypt the symbols.

II. PROBLEM FORMULATION

Cryptography is a technique that consists in encrypting the digital document to ensure security in the intended service. Several techniques and imaging models have been proposed by many researchers. These models have proven to be successful in diagnosing many of the problems as copywriting integrity etc. However, these techniques are often insufficient or inconclusive due to the complexity of the models or the limitation of the imaging techniques themselves. The main problem of these endeavors arises when managing the integrity and confidentiality of data on the internet against pirates. Several solutions based on the use of access control techniques exist, but they remain elusive. Hence, the appearance of cryptographic techniques in order to ameliorate the security control of the network in which those images are shared. In the literature review it was seen that a new approach with the logistic mapping with chaotic and ANN was proposed, it was simple to implement as complexity reduction was the major objective of work but still it was concluded that the use of Logistic Map (LM) has some flaws such as periodic windows in bifurcation diagram and a limited range of key space, there is to overcome these drawbacks so a new approach for the process is to be introduced in the model and enhance the system for the security purpose.

III. PROPOSED WORK

It was concluded that the use of Logistic Map (LM) has some flaws such as periodic windows in bifurcation diagram and a limited range of key space, there is to overcome these drawbacks so a new approach for the process is to be introduced. In the proposed work for overcome the limitation of the LM approach an Deffie Hellman with permutation for the key generation is used along with that an data compression approach using Huffman techniques for reducing the data size will be done which will provide reduced data for space utilization and the security as data will get encoding too by using Huffman.

For enhancing the security along with this XOR operation is applied to the compressed data and secret key to observe the encrypted data. This will provide 2 levels of security of the data, as first level with compression and encoding using Huffman and second level with the XOR operation the key and encoded data is combined to get the encrypted file.

Proposed Methodology:

1. Select Image

First step of the proposed work is to input the digital image so that further encoding can be applied to it. If the input image is of RGB format then firstly it has to be converted in grayscale format.

2. Apply Huffman Encoding

After selecting the image the next step is to apply the Huffman encoding to the selected image. The Huffman encoding is security technique that is specifically used in proposed work to compress the image size without losing its original information.

3. Generate Key

After encoding the image next step is to generate the key by using the diffie key generation technique. The generated key is further used for encryption process.

4. Encrypt the data

In this step the permutation is applied to the diffie key generation algorithm. The encryption of the data is done by performing the XOR operation on encoded image and key which is generated by using diffie key generation in previous step.

5. **Encrypted Image:** After performing the XOR, at last the encrypted image is obtained.

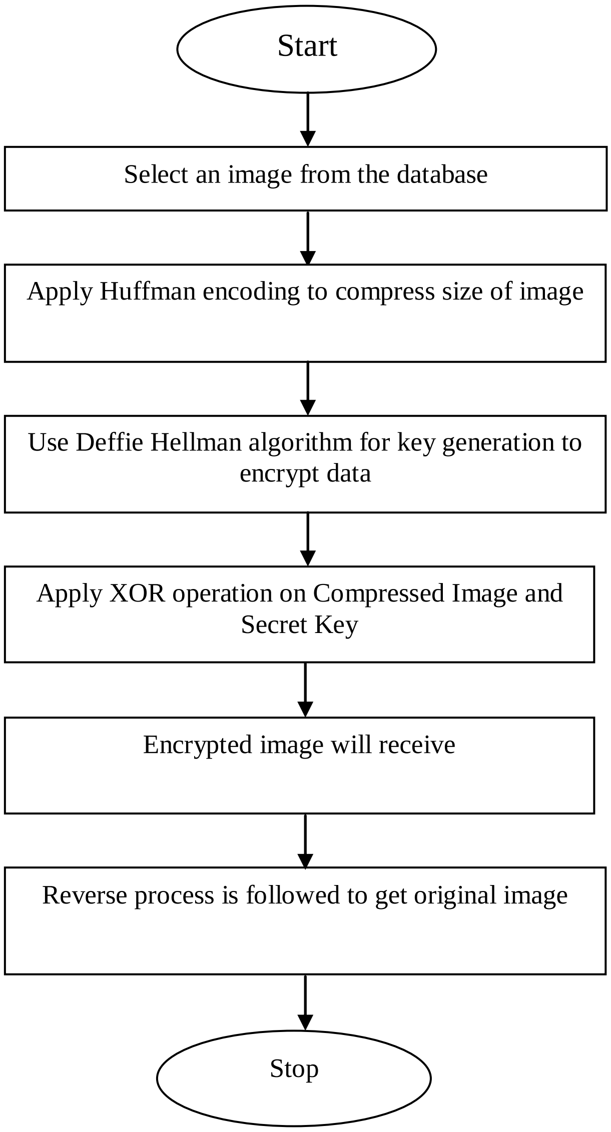
Start
Select an image from the database
Apply Huffman encoding to compress size of image
Use Deffie Hellman algorithm for key generation to encrypt data
Apply XOR operation on Compressed Image and Secret Key
Encrypted image will receive
Reverse process is followed to get original image
Stop

Figure 2. Framework of Proposed Mechanism

Performance Parameters:

1. Histogram:

A histogram is a graphical formation of the distribution of numerical data. It is an approximation of the probability distribution of a constant variable. To build a histogram, the first step is to split the intact series of values into series of intervals and then count no. the values fall into interval. The intervals must be adjacent, and are often of equal size. Image histograms show frequency of pixels intensity values. In image histograms, it has two axes one is x-axis and other is y-axis. The x-axis shows RGB level intensity and y-axis shows frequency of these intensities. The x-axis shows that range of pixel values. The histogram shown in this work has two axis graphs on which the x axis stands for number of pixels in the histogram of the image and the y axis stands for the number of count. Histogram shows the numerical values of red, green and blue layers with respect to 2000 counts.

2. **NCPR:** It depicts the variations in pixel rate value in contrast to the encrypted image. It can be evaluated as follows:

$$NCPR = \sum_{i,j} \frac{D(i,j)}{W \times L} \times 100\% \ldots\ldots(1)$$

3. **UACI:** It is evaluated to depict the intensity ratio with respect to the C1 and C2 (represents the two cipher images) whereas the related original image is different with respect to single pixel only.

$$UACI = \frac{1}{W \times L} \sum_{i,j} \frac{|C_1(i,j) - C_1(i,j)|}{T} \times 100\% \ldots..(2)$$

Here in equation (5) , T depicts the total number of pixels corresponding to cipher image W and L.

4. **CORRELATION:** Following formulation is used for evaluating the correlation among two images:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \dots \dots (3)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))^2 \dots \dots (4)$$

$$cov\ (x, y)$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)(y_i - E(y)) \dots \dots (5)$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y}} \dots \dots (6)$$

5. **ENTROPY:** To evaluate the entropy value of the images the following equation is used:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log_2 \frac{1}{p(m_i)} \dots \dots (7)$$

6. **Mean Square Error (MSE):** This is a parameter which is used to evaluate the degradation level of the system. The value of the MSE represents the acceptable value of minimum error in the system.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i, j) - K(i, j)]^2 \dots \dots \dots \dots \dots \dots \dots \dots \dots (8)$$

7. **Peak Signal to Noise Ratio:** This parameter replicates the existence of error corresponding to the information in the current signal. In medical images the approximately 50 dB PSNR is acceptable, whereas in simple images this value is 30 dB.

$$PSNR = 10Log_{10}\left(\frac{(L-1)^2}{MSE}\right) dB$$

IV. RESULTS

This section provides an overview to the results that are obtained after implementing the proposed cryptographic mechanism in MATLAB simulation platform. The experiments are done by using the Lena image. The figure 3 illustrates the considered plain image of Lena.

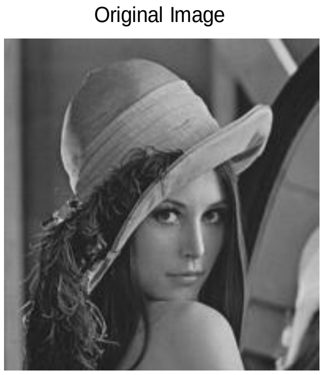

Figure 3. Original Image

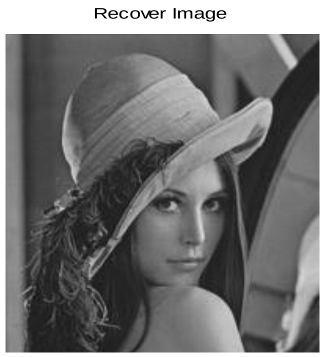

Figure 4. Recovered Image

The graph in figure 5 represents the histogram of original image. In this graph the x axis ranges from 0 to 300 and y axis starts from 0 and ends at 1000. The histogram defines the pixel count in original image.

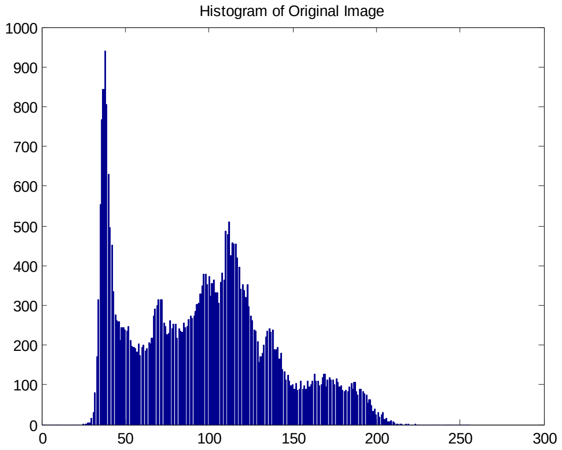

Figure 5. Histogram of Original Image

After generating the histogram of original image, the compression is applied to the image by using Huffman compression technique. The graph in figure 6 portrays the histogram of compressed image.

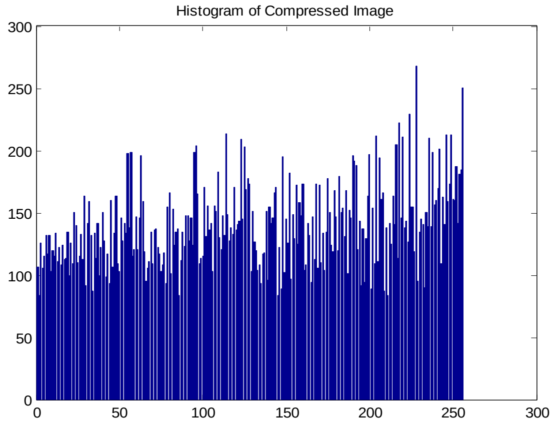

Figure 6. Histogram of Compressed Image

The Huffman compression technique compressed the original information in such a way that the originality of the information remains constant or in other words it is a lossless compression mechanism.

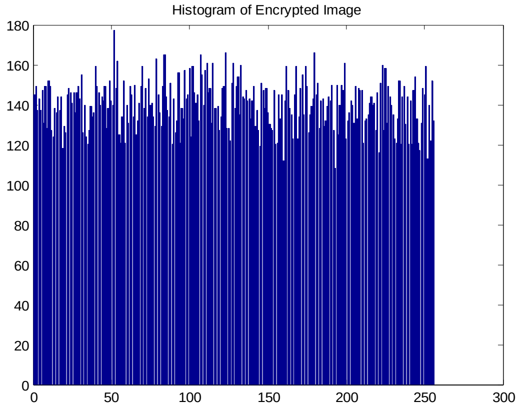

Figure 7. Histogram of Encrypted Image

The XOR operation is applied to the compressed image in order to make it highly secure from unauthorized access or alterations. The histogram represented in figure 7 shows the values of the pixels in the encrypted image. As it can be evaluated from the graph of figure 6 that the spikes of the histogram are quite high in comparison to the histogram of original image which replicates that it is not possible to recognize the originality of the image from the encrypted image.

The comparison graph in figure 8 represents the contrast of proposed and traditional work in terms of NCPR. From the graph it can be observed that the NCPR of traditional (Chaotic-ANN) is 99.43 whereas the NCPR of proposed work is 100. It proves that the proposed work has highest value of NCPR thus it leads to the best and reliable results.

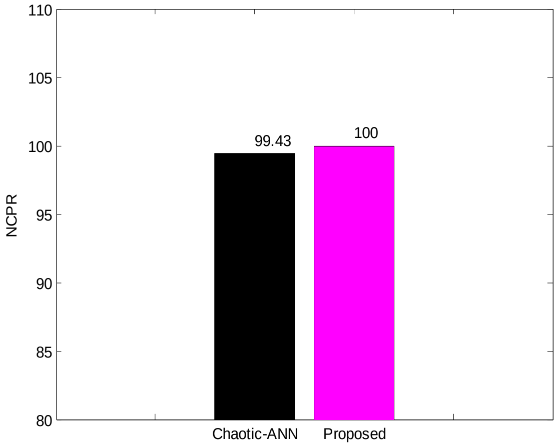

Figure 8. NCPR of Chaotic ANN and Proposed Work

The graph in figure 9 defines the comparison of Chaotic-ANN and present work on the basis of the UACI parameter. The UACI of Chaotic-ANN is 33.7 and for proposed work it is 52.526. The UACI of the proposed work is higher is comparison to the chaotic-ANN.

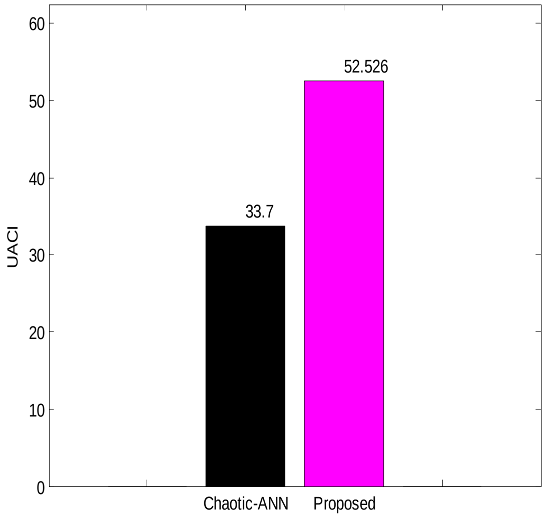

Figure 9. UACI of Chaotic-ANN and Proposed work

The graph in figure 10 illustrates the value correlation among the plain and cipher image in case of proposed and Chaotic-ANN. The correlation of chaotic-ANN is 0.00537 and -0.106.02 is for proposed work

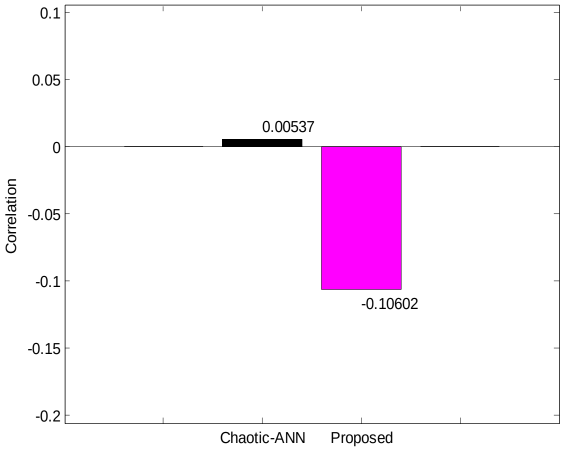

Figure 10. Correlation of Chaotic-ANN and of proposed work

The comparison graph in figure 11 shows the comparison of entropy value for proposed work and traditional work. The entropy of proposed work is greater than the entropy value of chaotic-ANN mechanism.

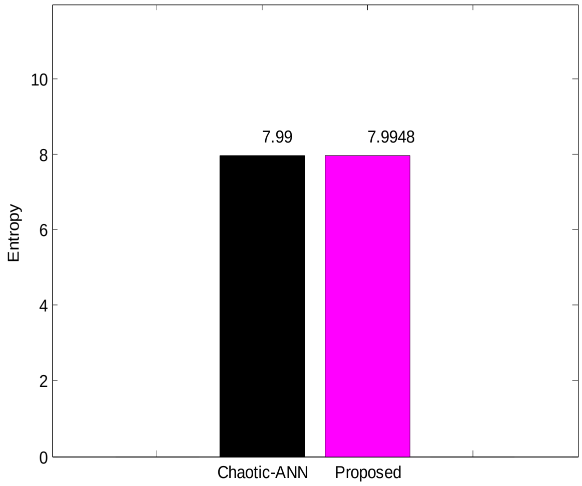

Figure 11. Comparison of Entropy

The graph in figure 12 is draw on the basis of the mean square error of the work. The obtain value of MSE in proposed work lies at 3.1*10^4 which is quite better. Mean Square Error is evaluated to analyze the overall average of the error.

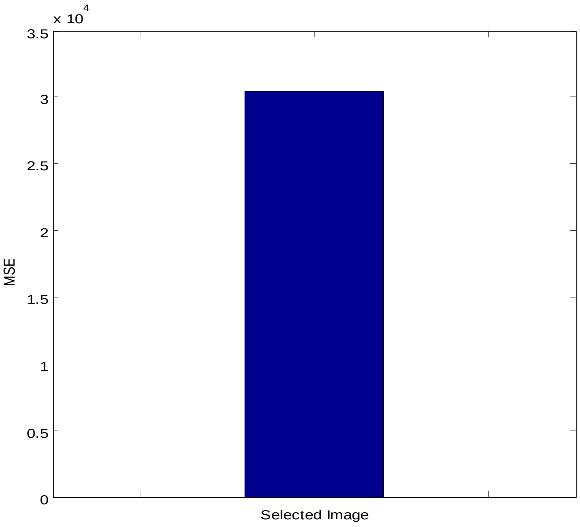

Figure 12. MSE of Proposed Work

The graph in figure 13 depicts the peak Signal to Noise ratio of the proposed work. Peak Signal to Noise Ratio is used to evaluate the existence of signal with respect to noisy content. The x axis in the graph shows selected image and y axis shows the value of PSNR which ranges from 0 to 35. The graph represents that the PSNR of the proposed work is near by 33.

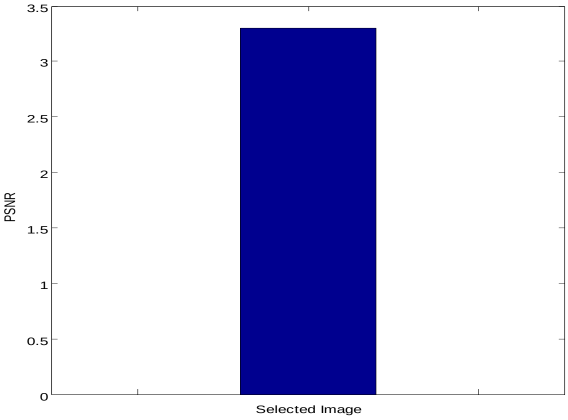

Figure 13. PSNR of proposed work

Table 1 Comparison of Proposed work with Chaotic ANN

Parameters		Choatic ANN[1]	Proposed Work
NCPR		99.43	100
UACI		33.7	52.526
Correlation		0.00537	-0.10602
Entropy	Original Image	_	7.1691
	Encrypted Image	7.99	7.9948
Compression Ratio		_	0.90038

V. CONCLUSION

Cryptography or image cryptography is a approach used for providing the security to the images in order to make them secure from various attacks such as unauthorized modification or data tampering etc. This study has been specifically conducted to develop a novel encryption based image cryptographic mechanism based on two different security enhancement mechanism i.e. compression and encryption. For the purpose key generation, the Diffie-Hellman mechanism is applied and Huffman encoding method is applied for reducing the image size without losing any content. Then the compressed image is encrypted by using the XOR operation on compressed data and generated key. This work provides two level securities to the images firstly by applying compression and then encrypting the compressed image. To measure the proficiency of proposed work over traditional the simulation is done by using the Lena image. The result section depicts the outcome that is observed after implementing the proposed work and after seeing the results it is concluded that the proposed work achieves the highest NCPR, UACI and Entropy value in comparison to the chaos-ANN[1] based encryption mechanism. The result section proves that the proposed work outnumbers the traditional work in means of various performance parameters.

It is observed that due to using three various methods the complexity of the proposed work has been increased therefore in future more enhancements can be done to reduce the complexity of the system.

REFERENCES

[1]. Vinay Pandey, Manish Shrivastava “Medical Image Protection using steganography by crypto image as cover Image”, International Journal of Advanced computer Research, VOL 2, Issue 5, 2012.

[2]. Ali Al-Haj, Gheith Abandah, Noor Hussein, “Crypto-based algorithms for secured medical image transmission”, IET, Vol 9, Issue 6, Pp 365-373, 2015.

[3]. Madhu B., Ganga Holi, Srikant Murthy K. “An Overview of Image Security Techniques”, International Journal of Computer Applications, Vol 154, 2016.

[4]. Fahad bin Muhaya, Muhammad Usama and Fahim Akhter “Chaos based Secure Storage and Transmission of Digital Medical Images” Applied Mathematics & Information Sciences An international Journal, Vol 8, Pp27-33, 2014.

[5]. Naina Gaharwar Reena Gunjan “Reversible watermarking for digital Images using Visual cryptography and Pixel histogram shifting” IJCSMC, Vol. 4, Issue. 7, Pp 185-193, 2015.

[6]. ManelDridi et al, “Cryptography of medical images based on a combination between chaotic and neural network”, IET Image Processing, pp. 1-10, 2016

[7]. A. Umamageswari, “A Survey on Security in Medical Image Communication”, IJCA, Vol 30(3), Pp 1-5, 2011

[8]. Hongjun Liu, “Image encryption using DNA complementary rule and chaotic maps”, ELSEVIER, Vol 12 (5), pp 1457-1466, 2012

[9]. Prema T. Akkasaligar “Secure Medical Image Encryption based on Intensity level using Chao’s theory and DNA Cryptography”, IEEE, 2016

[10]. S.Manimurugan, “A New Fast and Efficient Visual Cryptography Scheme for Medical Images with Forgery Detection”, IEEE, 2011

[11]. Mamta Jain, “Secure Medical Image Steganography with RSA Cryptography using Decision Tree”, IEEE 2017

[12]. Ali AI-Haj, “Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images”, IEEE, 2016

[13]. Meghdad Ashtiyani, “Chaos-Based Medical Image Encryption Using Symmetric Cryptography”, IEEE, 2008

[14]. Swati malik, Ajit “Securing Data by Using Cryptography with Steganography”, 2013

[15]. Mohit Kumar , “A Review on Various Digital Image Encryption Techniques and Security Criteria”, IJCA, Vol 96 (13), Pp 1-8, 2014

[16]. Reena Dhiman et al., “Image Encryption Techniques: A Literature Review”, IJARCS, Vol 8 (7), PP 1-5 , 2017

[17]. Mamta Juneja et al., "A Review of Cryptography Techniques and Implementation of AES for Images", IJCSEE, Vol 1 (4), Pp 1-5, 2013,

[18]. Mohamed M.Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine", ELSEVIER, Vol 14 (1), Pp 1-13, 2013

[19]. Nidhal Khdhair, "New Image Encryption Algorithm Based on Diffie –Hellman and Singular Value Decomposition", IJARCCE, Vol 5(1), Pp 1-5, 2016,

[20]. Dr. Parmanand Astya, "Image encryption and decryption using Elliptic curve cryptography", IJARSE, Vol 3 (10), Pp 1-8, 2014

[21]. A. Joseph Aamalraj et al., "A Survey Paper on Cryptograph y Techniques", IJCSCMC, Vol 5 (8), Pp 55-59, 2016

[22]. Xiaolong Li et al., "A New Reversible Data Hiding Scheme Exploiting High-Dimensional Prediction-Error Histogram", 2016 IEEE International Conference on Image Processing (ICIP), pp.2732 – 2736, 2016.

[23]. Siren Cai et al., "A New Reversible Data Hiding Scheme Based On High-Dimensional Pixel-Intensity-Histogram Modification", 2016 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), pp.1 – 6, 2016

[24]. Shuang Yi et al., "Improved Reversible Data Hiding in Encrypted Images using Histogram Modification", 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp.004819 – 004823, 2016.

[25]. Tanwi Biswas et al., "A New Method of Reversible Data Hiding Based on Compressed Gray Level Histogram Shifting", 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp.1 – 6, 2016.