Research Result

Enhancement of Image Encryption Technique Using Pixel Shifting Algorithms and Chaotic Map

Hitesh Kumar Chandak[1], Dr. Anshuj Jain[2]

[1]*M.Tech. Scholar, Department of Electronics & Communication Engineering, Scope College of Engineering, Bhopal (M.P.), INDIA*
[2]*Guide, Department of Electronics & Communication Engineering, Scope College of Engineering, Bhopal (M.P.), INDIA*

ABSTRACT

The encryption field is turning out to be vital in the current period in which data security is of at most concern. Security is a significant issue in correspondence and capacity of images, and encryption is one of the ways of guaranteeing security. The image encryption has turned into the main center point in this period of break of safety and classified data held inside a piece of information or data. Image Encryption or ciphering of images is the methods to secure image being hacked or damaged while transmitting. Such security method applied on transmits information from one node to another node which is sensitive to disclose and need to be kept as secure as possible. Previous researches were having different security algorithms to encode image, and here this work promises to enhance the safety better than previous methods need to maintain that security levels must be increased to make the encryption more robust and reliable. Above idea is making strong system and ciphered image is not able to guess. In the proposed encryption system security levels are here divided in parallel security also, which multiplies the security means all the layers RGB are encrypted divergently. The simulation steps will clearly show the strength of proposed methodology and average of entropy for scope, lena, baboon is 7.9995 for all three R, G and B. the NPCRs of Encrypted Images is 99.67243,99.61978 and 98.69395 for R, G and B respectively. The UACIs of Encrypted Images is 27.6398, 27.2161 and 29.0811 for R, G and B respectively.

KEYWORDS

Chaotic Map, Matrix Operations, Cipher Image, Fast Encryption, elliptic curve encryption, encryption de-encryption, image encryption

1. INTRODUCTION

There are enormous advancements in the various multimedia-based applications like clinical imaging, and multimedia image/audio/video database services etc. This increasing advancement of digital and multimedia-based applications has increased the demands of transmitting them over various types of networks. For scientific and research community, the prime concern of such types of applications has been the efficient and secure transmission over the channel. Because of the increasing evolution of Internet in today's digital world, the safety of transmitted has become very important concern. It is very well known that a huge part of such information is either private or confidential. So different security strategies have been utilized to give the important assurance. For such reason a wide range of image encryption techniques have been proposed to upgrade the security of these images.

A digital image is either a simple gray image which can be represented as two-dimensional matrix with pixel intensities in it or a colored image which can be represented as three dimensional or RGB matrix where matrix three planes are corresponds to red, green and blue respectively. The images in data are bulky; therefore, encryption algorithms should be designed very carefully. These algorithms may involve few complex computations, fast in implementation and secure to various possible threats.

Encryption is the study of concealing information which may be uncovered just by honest to goodness clients. It is utilized to guarantee the mystery of the transmitted information over an unsecure channel and avert listening stealthily and information altering. Another field called "cryptanalysis" worries with assaulting and decoding these ciphers. Many encryption plans were proposed and utilized for securing information, some utilization the common key encryption, while some others utilize the general population key encryption (PKC).

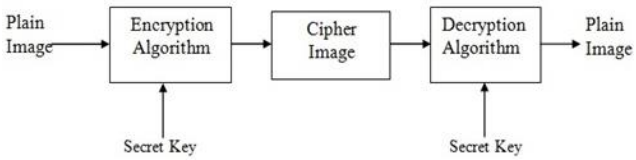

Fig.1.1Basic block diagram of Image Encryption/Decryption

The mutual key encryption is a framework which utilizes just a single key by both sender and beneficiary with the end goal of scrambling and unscrambling messages. Then again, open key encryption utilizes two keys, in particular private-

key and open key. To encrypt a message for people in general key plan, the general population key is utilized, while the private-key is utilized to unscramble it.

The basic block diagram of image Encryption/Decryption process is shown in the Figure 1.1. The cipher image is produced by encryption of plain image with the help of chaotic maps. The cipher image is given as an input to decrypting the original plain image. The encryption and decryption of image is done with the help of symmetric key. The plain picture is scrambled utilizing chaotic maps and there by figure picture is delivered. The code image is given as a contribution to decode the original plain image.

Encryption depends on hard numerical issues like prime number factorization, Elliptic curve discrete logarithm issue and discrete logarithm issue. The thought behind these issues is the calculation can be effortlessly done in one course; however, it is extremely troublesome the other way.

This is not hard to discover the consequence of increasing two numbers, yet it is to a great degree testing to discover prime elements of a number. Along these lines, encryption is worried with the outline and the investigation of numerical systems which can offer secure communications within the sight of malignant foes. This is a region which is stressed with the difference in data for the sake of security

2. IMAGE ENCRYPTION TECHNIQUES

Elliptic Curve Encryption (ECC) is the most resource traditionalist opens key cryptosystem as of now known. The serious conditions involved by encryption domain make ECC the main feasible answer for sound encryption for image ciphering. The security of every ECC primitive, including verification, relies on the point augmentation operation. This means to build up a point increase segment that could be conveyed on an image ciphering system. For this an approach novel to low power, little zone ECC plan for RFID applications was picked. Besides unprecedented consideration was taken to make the circuit solid against side channel assaults. The Elliptic bend cryptosystem (ECC) gives a littler and quicker public key cryptosystem. Likewise, the ECC is additionally a practical and secured innovation to be actualized in compelled applications.

Elliptic Curve Encryption (ECC) was found in 1985 by Victor Miller (IBM) and Neil Koblitz as an option component for actualizing public-key encryption in view of elliptic curve over limited field. ECC depends upon discrete logarithm which is significantly harder to challenge at equal key lengths as contrast with another public key encryption. It utilizes littler key as contrast with another public key encryption with same security level. Along these lines, it is used generally in lower asset framework like mobile communication.

Chaos Based Image Encryption Techniques-These days, image security has drawn in significant consideration as a rising number of images are communicated over the networks, partook in cell phones and re-appropriated by the cloud storage. As encryption is the most well-known procedure for safeguarding security, many image encryption calculations utilizing various types of strategies have been created in the previous many years.

At the point when a image is communicated over the channel, certain data misfortune is unavoidably brought about by noise or organization climate. Here, we don't consider the error correcting, error checking or re transmission systems of data. Communicated over the network, yet just break down the strength of encryption algorithm. Once the encrypted ciphertext of the customary encryption calculation experiences the deficiency of pixel block, the lost piece of data or information won't be perceived, and in the event that the piece contains the significant data of the image, the image clearly becomes invalid.

In this way, conventional encryption calculations are not truly reasonable for image encryption, and another image encryption technique based on the diffusion and permutation have been proposed. Among them, the image encryption in light of the chaotic system is a significant branch. Chaotic systems which have many excellent intrinsic properties such as unpredictability, random-like dynamical behaviors, sensitivity to initial conditions, and complex topological structures are appropriate for designing image cryptosystems.

Chaos is a dynamic system which produces succession of numbers that are irregular in nature. These irregular successions are applied to encrypt and decrypt the image. The sequences are purely based on initial condition. Small changes in initial condition might prompt to a different sequence of generation. This chaotic behavior facilitates to develop image encryption methods. The image encryption is done by chaotic mapping for scrambling the image pixel to different areas with changes in pixel values. The image encryption techniques are uncovered through built-in internal key generator for image encryption, hash keying based image encryption and parity bit based image encryption.

Most of chaos-based image encryption schemes are generally composed of two main stages: permutation and diffusion. These two stages repeat for multiple times for the sake of obtaining a good security level.

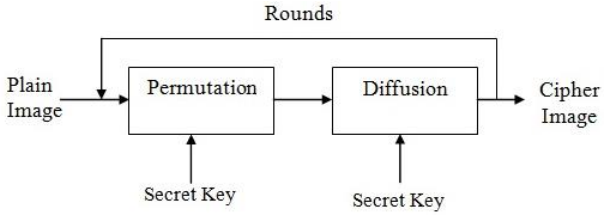

Figure 2.1 Image Encryption based on permutation & diffusion

The permutation and diffusion are broadly utilized as an encryption method as shown in Figure. In permutation stage, the pixel positions are altered by utilizing chaotic maps. In the diffusion, the pixel values are altered by utilizing chaotic maps. The initial value of chaotic map is taken as a secret key and it is iterated in accordance to the size of the image. The encrypted image is taken as input and it is rehashed for number of rounds. Various Different keys are chosen for each round in permutation and diffusion process. The performance analyses tests are carried out to examine the encrypted image. The same process is repeated to decrypt the original plain image.

The permutation stage is liable for diminishing areas of strength for the between pixels adjoining one another. The techniques of permutation can be separated into two classifications: pixel-level and bit-level, according to the smallest processing element. In the first category, a pixel is treated as the smallest scrambling element. Most pixel-level permutations shuffle the image by changing the pixel positions without modifying pixel values, so the histograms of the permuted image and the original image are identical. Such pixel-level permutations are vulnerable to histogram attacks and chosen/known-plaintext attacks if they have no diffusions or bad diffusions.

In the second category, bit is considered as the fundamental operating element and the pixel matrix of a plain-image is typically changed into a binary matrix unlike pixel-level permutation, the bit-level permutation can change the position and value of a pixel simultaneously, so the histogram of permuted image is different with that of the original image. However, since every pixel corresponds to eight bits, the time consuming of bit-level permutation is eight times as much as the pixel-level permutation if same permutation method is applied to two levels.

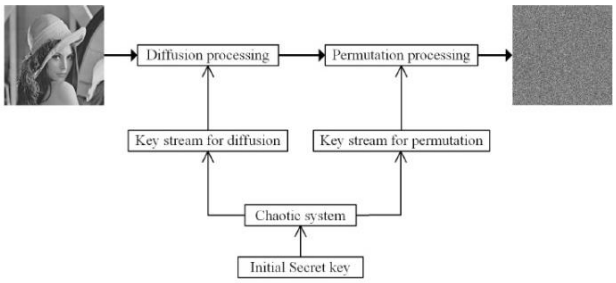

Figure 2.2 Chaotic system of Image encryption based on Permutation and diffusion

Arnold Cat Map -Arnold Cat maps which was named after Vladimir Arnold. He used an image of a cat to display the effect of this chaotic map. In this mapping technique, images go through a transformation that randomizes the original image pixels. It is a good example of hyperbolic total automorphism where a torus is given by a square matrix.

Some key features of this mapping technique are it is area preserving that is the transformed image requires the similar region as the actual image, it can be even deduced as the determinant of the matrix is 1. Also, if the image is iterated several times the original image reappears.

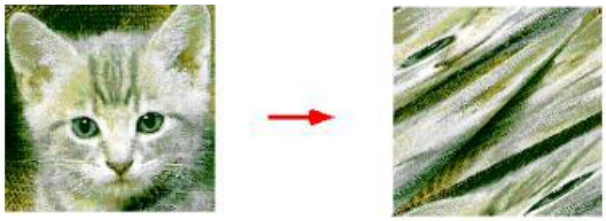

Figure 2.3 Arnold Cat Map transformation

Figure 2.3 shows how the linear map changes the unit square and how the pieces are rearranged after modulo operation. Even though the usefulness of Arnold Cat Map is limited, but it illustrates the power of the science behind the chaos-based system.

3. PROPOSED METHODOLOGY

The cryptographic technique is being discussed in our work is explained here and the different parts of proposed encryption framework is explained below. The working of the system is also explained by means of flow charts after block diagrams.

Encryption Module- In below figure 3.1 the proposed framework is explained with main blocks where the framework is divided among multiple security layers. The first block is RGB separation in which we separate our image in to its separate RGB components. After that we normalize them to changes the range of pixel intensity values. After that blending of layers i.e. RGB layers are mixed each other to create it more difficult to recover. The next level is chaotic Distribution which is performed over RGB layer with different frequencies which will further complicate the encryption algorithm to increasing the security. Toward the finish of this, one will get encrypted image which is most secured image ever.

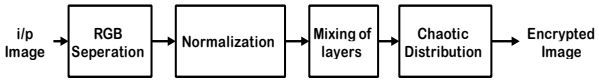

Figure 3.1 Basic block diagram of proposed encryption system

Decryption Module- The decryption procedure is the reverse operation of encryption process and the steps are separation of RGB layers then apply reverse chaotic distribution to RGB layers with the specified frequencies followed by de-mixing of RGB layers.

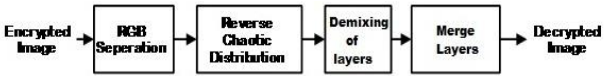

Figure 3.2 Basic block diagram of proposed decryption System

A. Proposed Encryption

Choose the image you want to use for the image ciphering purpose extract file for saving results read the selected image resize image to square shape and normalize layers of the image and apply layer mixing the layers and apply chaotic image Distribution with different frequencies. Save encrypted image and time required. Flow/Stream of the process is shown in figure 3.3.

Algorithm 1: Encryption Process

Input: I input RGB image with size 256×256

K_p Three Digit Private Key ($111 \leq K_p \leq 999$)

Output: I_E Encrypted Image of size 256×256

1. Load RGB Image I
2. Split Channels into I_R, I_G, *and* I_B
3. Normalize the I_R, I_G, *and* I_B Matrices – Convert datatype to double
4. Mix the matrix elements (inter channel mixing)
    a. Square Matrix → Row Matrix conversion (I_R, I_G,

and I_B) Separately

b. Transpose Row Matrices (I_R, I_G, *and* I_B)

c. Form Mix Matrix with $[I_M] \leftarrow [I_{R1}, I_{G1}, I_{B1}, I_{R2}, I_{G2}, I_{B2}, \ldots I_{R256}, I_{G256}, I_{B256}]$

d. Split I_M into 3 equal parts I_{M1}, I_{M2}, & I_{M3}

e. Row Matrices → Square Matrices Conversion of each I_{M1}, I_{M2}, & I_{M3}

5. Apply Chaotic Operation using Private Key K_p

a. $I_{E1} \leftarrow I_{M1}$ with K_{ph}

b. $I_{E2} \leftarrow I_{M2}$ with K_{pt}

c. $I_{E3} \leftarrow I_{M3}$ with K_{po}

6. $I_E \leftarrow$Concate(I_{E1}, I_{E2}, I_{E3})

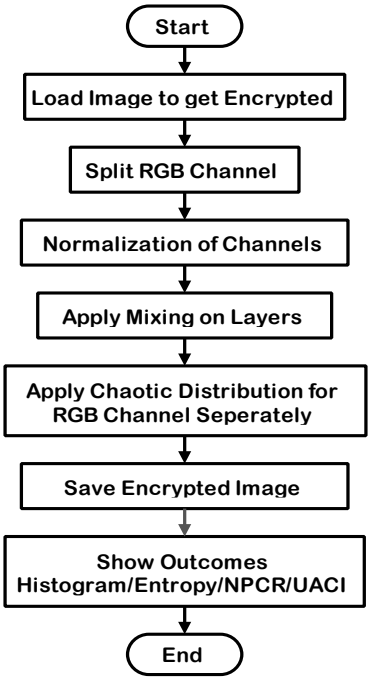

Figure 3.3 Flow Chart of Encryption Process

B. Proposed Decryption

Algorithm 2: Decryption Process

Input: I_E Encrypted Image of size 256×256

K_p Three Digit Private Key ($111 \leq K_p \leq 999$)

Output: I input RGB image with size 256×256

1. Load RGB Image I_E

2. Split Channels into I_{E1}, I_{E2}, *and* I_{E3}

3. Apply Reverse Chaotic Operation using Private Key K_p

a. $I_{M1} \leftarrow I_{E1}$ with K_{ph}

b. $I_{M2} \leftarrow I_{E2}$ with K_{pt}

c. $I_{M3} \leftarrow I_{E3}$ with K_{po}

4. Demixing the matrix elements

a. Square Matrix → Row Matrix conversion $[I_M]$

c. Form Mix Matrix with $[I_{R1}, I_{G1}, I_{B1}, I_{R2}, I_{G2}, I_{B2}, \ldots I_{R256}, I_{G256}, I_{B256}] \leftarrow [I_M]$

d. Split $[I_{R1}, I_{G1}, I_{B1}, I_{R2}, I_{G2}, I_{B2}, \ldots I_{R256}, I_{G256}, I_{B256}]$ into I_{M1}, I_{M2}, & I_{M3}

e. Square Matrices Conversion ←Row Matrices of Each I_{M1}, I_{M2}, & I_{M3}

b. Transpose Square Matrices I_{M1}, I_{M2}, & I_{M3}

5. Normalize the I_R, I_G, *and* I_B Matrices – Convert datatype to double

6. $I \leftarrow$Concate(I_{M1}, I_{M2}, & I_{M3})

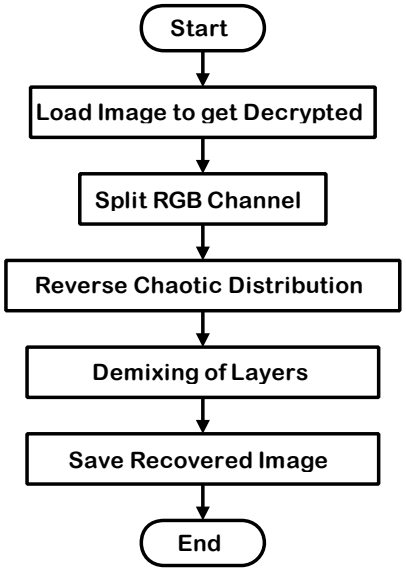

Figure 3.4 Flow Chart of Decryption Process

Figure 3.4 demonstrated the Flow/stream of the proposed decryption system. To decrypt select our encrypted image which has to be decrypt. Decryption process is just a reverse of encryption process. After selecting image apply reverse chaotic Distribution and apply reverse mixing of layers implemented to image after that it showing decrypted images.

4. SIMULATION OUTCOMES

The execution of our system explained previously is performed on simulation tool using MATLAB 3.7 with on a DELL laptop with system configuration as Intel(R) Core (TM) i3-8250U CPU@2.40GHz with 4GB RAM and the various images are tested over proposed system and few simulation results are explained here. We can see effect on input image of that during different steps of simulation.

We have selected four images (256X256) with different distribution of pixel values for encryption. Among them, figure 4.1(a) is the original color images. Figure 4.2(b) shows the blending of layers of images shown in figure 4.1(a). Figure 4.3(c) shows the Chaotic Distribution Operations on respective previous stage outputs. Fig.4.4-4.7 depicts various stages of decryption process.Fig.4.7-4.10 depicts respective histograms. It can be seen that the image is completely unrecognizable and becomes a cluster of

disorganized pixels encrypted images. The security parts of the proposed method analyzed based on MATLAB simulation.

Experimental Results & Security Analysis

Various security and statistical tests are carried out to explore the strength of the proposed algorithm. The analyses carried out include histogram analysis, key space analysis, and entropy of cipher images, measuring resistance to differential attacks with NPCR (Number of Pixel Change Rate) and UACI (United Average Changed Intensity) parameters.

Histogram Analysis

The histogram of an image is represented as a graph. This graph shows the number of pixels in an image at different intensity values as found in the image. Histogram analysis is done to analyze the occurrence of relative frequency of different pixel values. The histograms for the plain and cipher images are illustrated in Fig. 4.7 to 4.10. When the two histograms are compared, it is observed that the histogram of the encrypted images is totally different as compared to the original plain Lena image and other images, and moreover the cipher images does not provide any useful information to the attacker, which makes the image resistant against statistical attacks.

Key Space

Security of an encryption and decryption depend a lot on the size of the key used. The bigger the key size, the more it is difficult to perform an attack. In our implementation we have used a 3-bit key which has got a sample key size to provide the necessary security. In general, to better defend against exhaustive search attacks, the encryption System must have a key space of at least 2100 to achieve a sufficiently secure. System must have a key space of at least 2100 to achieve a sufficiently secure.

Key Sensitivity

A slight change in original key should give a drastic change in the recovered image obtained from the cipher image. Our proposed algorithm has good key sensitivity. It shows the recovered image same as original image from cipher image using the correct private key of the receiver. A wrong key is one which is just one digit different from the original key.

Entropy

Entropy is the measure of degree of randomness. Entropy is directly proportional to the degree of uncertainty present in the data. For image encryption, we want the cipher image pixel values to be highly random. The information entropy is calculated using Shannon's method. A good cipher image will have an entropy value close to 8 and it confirms that the cipher image is random and secured against entropy attack. Table 4.1 shows the various entropy values of the cipher images which are very close to 8 and confirms that the cipher image is random and secured against entropy attack.

Resistance to Differential Attacks

Differential attacks are a form of cryptanalysis to find the secret key by tracing the differences in the cipher data due to minimal changes in the plain data. In image encryption, algorithms strength to resist different attacks is usually evaluated using two most common quantities number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI). NPCR and UACI values are dependent upon two factors image or pixel size and chaotic map used. In differential attacks, if a minor change in the input image can bring significant change in the cipher image, then the differential attack is difficult and NPCR and UACI are the used to measure them.

Table 4.2 shows the performance of algorithm proposed in this work in terms of NPCR for the red, green and blue channels for input images. The optimum NPCR achieved is 99.67243.

Table 4.3 shows the performance of algorithm proposed in this work in terms of UACI for the red, green and blue channels for input images. The optimum UACI achieved is 29.0811.

The proposed algorithm achieves larger values NPCR >99.5 and UACI value 29.0811 thereby resisting differential attack and became more protected encryption system.

Figure 4.1- Input Images (Scope, Lena, banboon and tower)

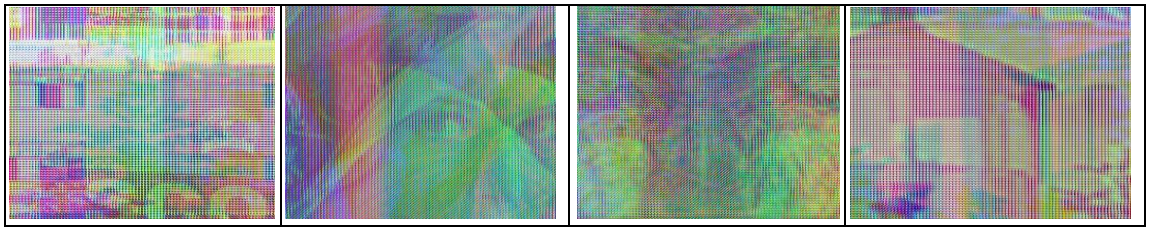

Figure 4.2- Blending of layers of respective previous stage outputs.

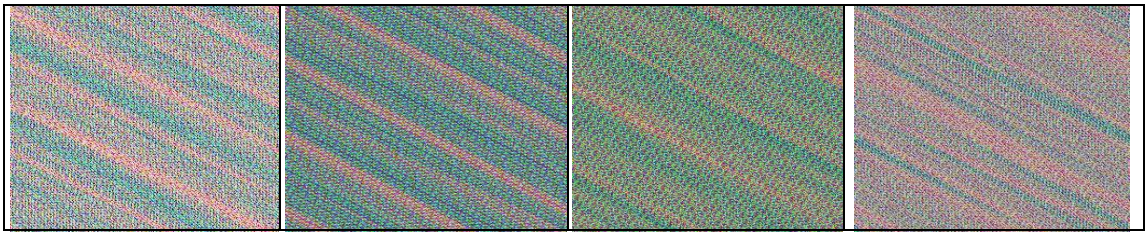

Fig 4.3- Chaotic distribution operations on respective previous stage outputs

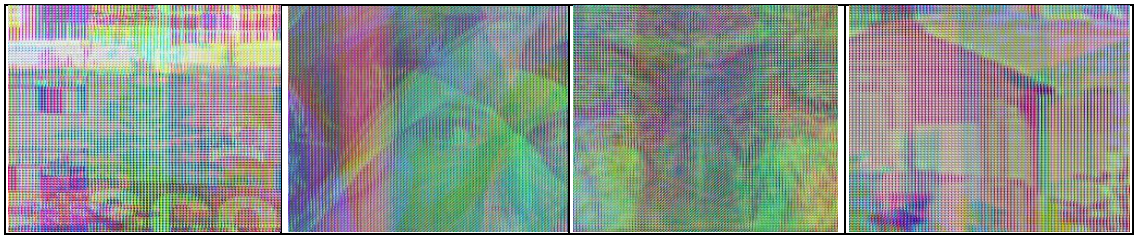

Figure4.4: Reverse chaotic distribution (Scope, lena, banboon and tower)

Figure 4.5: Demixing of layers of respective previous stage outputs.

Figure 4.6: Recovered original image from chipper image.

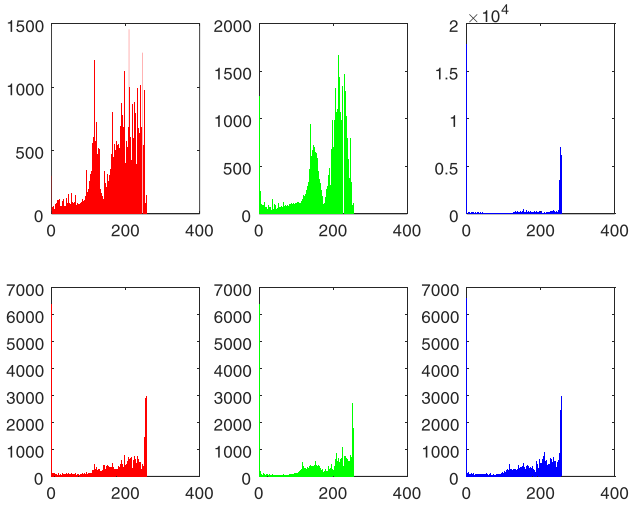

Fig. 4.7 Histogram of SCOPE image

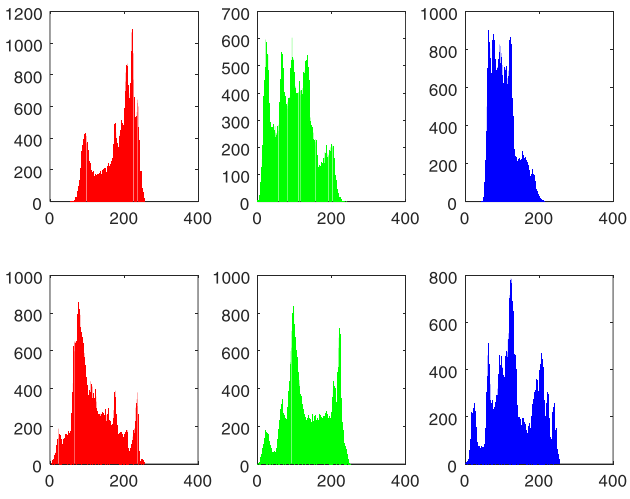

Fig. 4.8 Histogram of LENA image

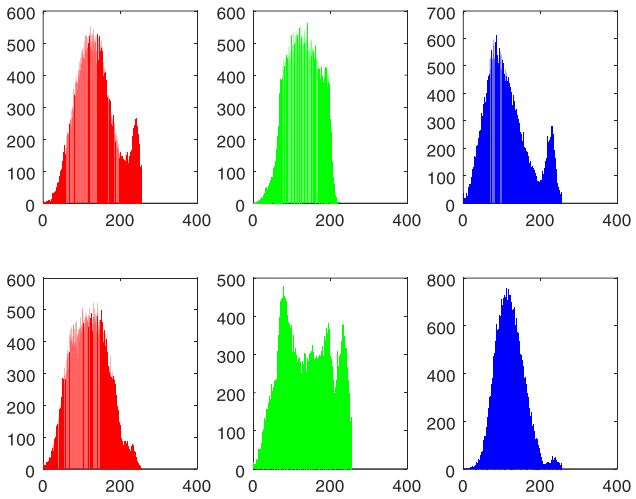

Fig. 4.9 Histogram of BABOON image

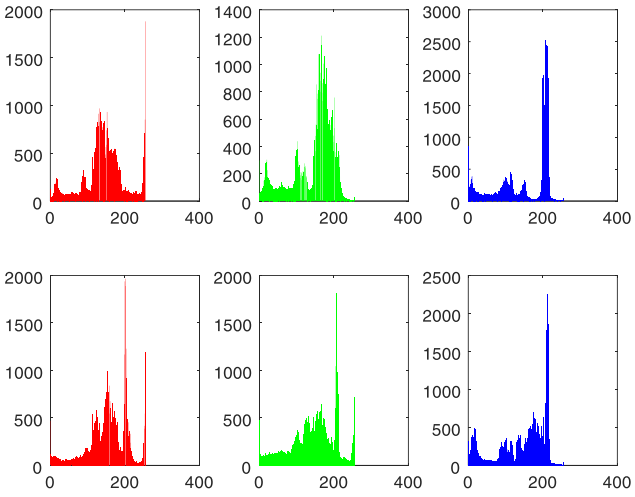

Fig. 4.10 Histogram of TOWER image

Table 4.1: Entropy of Encrypted Images

Image	*R*	*G*	*B*
Scope	7.9995	7.9995	7.9995
Lena	7.9996	7.9996	7.9996
Baboon	7.9996	7.9995	7.9996
Tower	7.9995	7.9995	7.9995
Average (Our)	***7.9995***	***7.9995***	***7.9995***
Previous	7.9998	7.9993	7.9993

Table 4.2: NPCRs of Encrypted Images

Image	*R*	*G*	*B*
Scope	99.6400	99.3745	96.2251
Lena	99.8643	99.7392	99.6232
Baboon	99.6339	99.7407	99.6354
Tower	99.5515	99.6247	99.2921
Average (Our)	***99.67243***	***99.61978***	***98.69395***
Previous	99.6110	99.6138	99.6080

Table 4.3: UACIs of Encrypted Images.

Image	**R**	**G**	**B**
Scope	31.3755	31.2004	42.1472
Lena	32.1116	27.6777	23.1152
Baboon	22.7396	24.7521	21.3443
Tower	24.3328	25.2343	29.7180
Average (Our)	**27.6398**	**27.2161**	**29.0811**
Previous	33.4824	33.4263	33.4119

Results Discussion It can be seen from the various results that when the two histograms are compared, it is observed that the histogram of the encrypted images is totally different as compared to the original plain Lena Image and other images, and moreover the cipher images does not provide any useful information to the attacker, which makes the image resistant against statistical attacks. The optimum entropy achieved is 7.9995 which are closed to 8 and it confirms that the cipher image is random and secure against entropy attacks.

It is also found that the average value of NPCR and UACI of the ciphertext image obtained by image encryption using the encryption algorithm proposed in this dissertation is 99.6% and 27.6% respectively which shows the anti-attack capability is ideal, and is sufficient to resist differential attack and statistical attacks. The analysis result shows that the proposed encryption scheme has better encryption efficiency. It has good security performance, and strong resistance to attack.

5. CONCLUSION AND FUTURE SCOPE

The image security is a major concern in these days communication. Therefore, any high confidential image exchange in normal network is a concern of network and data security. In various applications such as security agencies and their communications are needed to be prevented from any kind of attack and mislead. Therefore, by motivation of this a new technique is presented in this work. Here our main aim is to secure image transfer in un-trusted environment of communication.

We have implemented our image encryption algorithm which is based on pixel shifting algorithm and chaotic map. At first, we separate our image in to RGB layers and then these RGB layers are mixed each other to create it more difficult to recover. The second level is chaotic Distribution are also performed over RGB layer with different frequencies which will further complicate the encryption algorithm to increasing the security. Toward the finish of this, one will get encrypted image which is most secured image ever.

The proposed algorithm is expected to show good performance, low correlation and high entropy. Based on

the results, the proposed scheme is more secure and has higher average NPCR & UACI and can resist statistical, differential and noise attacks. The proposed model is proven to be robust, lightweight and competent against the statistical and cryptanalytic attacks.

This idea makes future encryption algorithms more secure even a portion of the old robust encryption algorithms can modify with this concept to enhance the shield of old systems and can facilitates the high-end modern encryption systems. The proposed algorithm can be improved by combining the traditional encryption techniques together, thereby getting a new encryption scheme to achieve highly secured image encryption scheme.

REFERENCES

[1] Cengfei Chen, Kehui Sun*, Qiaoyun Xu, "A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map" in Electrical, Electronics, China Communications, May 2020 pp.12-20.

[2] Zahir Muhammed, Ziad Muhammad And FatpihÖzkaynak, "Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique" IEEE Access, vol. 7,pp.99945_99951,2019.doi10.1109/ACCESS.2019.2930606.

[3] Nazir A. Loan, Shabir A. Parah, Javaid A. Sheikh, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption" IEEE Access, vol. 6,pp. 19876_19897,2018.doi0.1109/ACCESS.2018.2808172.

[4] Sudeshna Bora, Pritam Sen and Chittaranjan Pradhan, "Novel Color Image Encryption Technique using Blowfish and Cross Chaos Map" IEEE ICCSP 2015 conference.pp.0880-0883.

[5] Congxu Zhu and Kehui Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps" IEEE Access, vol. 6, pp. 18759_18770, 2018. doi 10.1109/ACCESS.2018.2817600.

[6] Chengqing Li, Dongdong Lin, Bingbing Feng, JinhuLü And Feng Ha, "Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy" IEEE Access, vol. 6, pp. 75834_75842,2018.doi0.1109/ACCESS.2018.2883690.

[7] Wei Feng and Yi-Gang He "Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling" IEEE Photon. J., vol. 10, no. 6, Dec. 2018, Art. no. 7909215.

[8] Yu Liu, Zheng Qin and Jiahui Wu "Cryptanalysis and Enhancement of an Image Encryption Scheme Based on Bit-Plane Extraction and Multiple Chaotic Maps" IEEE Access, vol.7, pp. 74070_74080, 2019. doi 0.1109/ACCESS.2019.2916600.

[9] Wang Xingyuan and Zhao Hongyu "Cracking and Improvement of an Image Encryption Algorithm Based on Bit-Level Permutation and Chaotic System" IEEE Access, vol.7, pp. 112836_112847,2019.doi0.1109/ACCESS.2019.2935017.

[10] Hossam Diab "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations" IEEE Access, vol.6, pp. 42227_42244, 2018. doi 109/ACCESS.2018.2858839.

[11] Ping Ping, Jinyang Fan, Yingchi Mao, Feng Xu, and Jerry Gao "A Chaos Based Image Encryption Scheme Using Digit-Level Permutation and Block Diffusion" IEEE Access, vol.6, pp. 67581_67593, 2018. doi 0.1109/ACCESS.2018.2879565.

[12] Sinha, A., & Singh, K. (2003). "A technique for image encryption using digital signature" Optics communications, 218(4), 229-234.

[13] Panchal, D., Jani, C., & Panchal H., "An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing." International Journal of Engineering Development and Research. Vol. 3. No. 4 IJEDR, 2015.

[14] Kumar, S., Sinha, B., & Pradhan, C. (2015). "Comparative Analysis of Color Image Encryption Using 2D Chaotic Maps. In Information Systems Design and Intelligent Applications" (pp. 379-387). Springer India.

[15] X.-J. Tong, M. Zhang, Z.Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," Nonlinear Dyn., vol. 84, no. 4, pp. 2333_2356, 2016.

[16] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," Opt. Lasers Eng., vol. 77, pp. 118_125, Feb. 2016.

[17] Y. Liu, X.-J. Tong, and J. Ma, "Image encryption algorithm based on hyper chaotic system and dynamic S-box," Multimedia Tools Appl., vol. 75, no. 13, pp. 7739_7759, 2015.

[18] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Opt. Lasers Eng., vol. 78, pp. 17_25, Mar. 2016.

[19] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," Opt. Lasers Eng., vol. 90, pp. 225_237, Mar. 2017.

[20] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," IEEE Multimedia, vol. 24, no. 3, pp. 64_71, 2017.

[21] C. Zhu, "A novel image encryption scheme based on improved hyper chaotic sequences," Opt. Commun., vol. 285, no. 1, pp. 29_37, 2012.

[22] Q. Shen and W. Liu, "A novel digital image encryption algorithm based on orbit variation of phase diagram," Int. J. Bifurcation Chaos, vol. 27, no. 13, Dec. 2017, Art. no. 1750204.

[23] C. Li, T. Xie, Q. Liu, and G. Chen, "Cryptanalyzing image encryption using chaotic logistic map," Nonlinear Dyn., vol. 78, no. 2,pp. 1545_1551, 2014.

[24] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," Nonlinear Dyn., vol. 92, no. 2, pp. 305_313, 2018.

[25] S. L. Sun, "A novel hyper chaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," IEEE Photon. J., vol. 10, no. 2, Apr. 2018, Art. no. 7201714.

[26] X. Y. Li et al., "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," IEEE Photon. J., vol. 8, no. 4, pp. 1–11, Aug. 2016.

[27] A. A. A. El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," Signal Process., vol. 93, no. 11, pp. 2986–3000, 2013.

[28] X. Y. Wang and C. M. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," Multimedia Tools Appl., vol. 76, no. 5, pp. 1–17, 2016.

[29] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vis. Comput., vol. 24,no. 9, pp. 926–934, 2016.

[30] P. Liu, T. Zhang, and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," Multimedia Tools and Applications, vol. 12, 2018, pp. 1-13.

[31] X. Wang, H. Zhang,X. Bao, "Color image encryption scheme using CML and DNA sequence operations," Biosystems, vol. 144, 2016, pp. 18-26.

[32] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Opt. Lasers Eng., vol. 90, pp. 238_246, Mar. 2017.

[33] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," Optik, vol. 126, no. 24, pp. 5703_5709, 2015.

[34] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Opt. Commun., vol. 284, nos. 16_17, pp. 3895_3903, 2011.