Optimization Based DNA for Image Encryption

[1]Ritu Devi, [2]Navneet Kaur

[1]P.G. Student, [2]Assistant Professor
Department of Computer Science & Engineering,
Global Research Institute of Management & Technology,
Kurukshetra, Haryana, India

***Abstract*: Users of Internet daily send and receive many images through social media. These images are vulnerable to hack and tamper by attackers. Therefore, it is necessary to develop methods for the security of these images. In this thesis work, a non-traditional encryption method for encrypting images is presented that makes images more and more protected and secured. These operations are implemented depending on extracted chains from the secret key used in the algorithm. Here we proposed an algorithm which takes the improvement of the ILM algorithm that aims to develop the unpredictability of the image pixels. Due to an enlarged randomness, the information entropy is considerably enhanced, powerfully resisting a vibrant range of arithmetic and differential attacks. Also DNA operation applies over the chaotic map algorithm substantially increased the effectiveness of the crypto system; Apart from this, the image encryption approach is rapid due to synchronous permutation and diffusion process that performed both these operation in a single iteration. To establish the efficiency of the proposed algorithm, we also performed a differential investigation to calculate NPCR and UACR and statistical for discriminating the histogram, entropy analysis, contrast analysis and CC analysis. Furthermore, Other DNA operations like DNA XOR, Addition, and Subtraction are used with (GA) genetic algorithm for better performance. Results are evaluated on MATLAB.**

***Index Terms*: Image retrieval, machine learning, image extraction, Histogram intersection, CBIRS technique.**

I. INTRODUCTION

Image Encryption is one of the extensively used techniques for data security. In this Data Encryption technique, data is transformed from its innovative to other form so that information cannot be access from the data without decrypting the data i.e. the invalidate process of encryption. The imaginative data is usually referred as basic data and the transformed form is called cipher data. Encryption of image can be definite as the art of convert data into coded form which can be decoded by intended recipient only who poses knowledge about the decryption of the cipher data. Encryption can be functional to text, image, and video for data protection. Responsiveness in digital image processing techniques and methods division from the following most important application areas: enhancement of pictographic information for human understanding; and dispensation of image data for storage space and communication for machine surveillance. At whatever time an image has to be transmitted, two noteworthy issues require to be addressed. One is to accommodate the image contained by the selected bandwidth and the other is to ensure protected transmission of images. Image density and image encryption are two elementary image processing techniques expansively used towards meeting the prerequisite of efficient consumption of bandwidth and security [1][2].

1.2 Image Encryption Procedure

The main purpose of keeping images secured is to preserve confidentiality, reliability and authenticity [4]. Different techniques and methods are available for creation images secured and one technique is by encryption method. Normally, Encryption is a process that transformed an image into a cryptic image by utilizing a key. In addition, a user can recover the original image by applying a decryption method on the cipher image [4], which is frequently a reversed implementation of the encryption process. For further description, Figure 1 represent a primary image; a user operate an encryption technique and generated a secrete image; Figure 2 showed an encrypted image that is the output of an encoded process. Alternatively, when a receiver gets this unknown image, he applied the decryption process and recovered the original information [3]. Figure 3 illustrates the recovered image


Fig 1: Panda

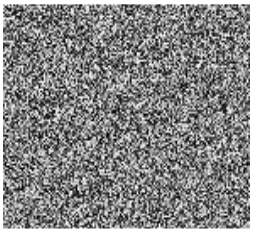
Fig 2: Cipher


Fig 3: Recovered image (Panda)

Cryptography has two main categories given as follows; (1) symmetric key cryptography and (2) asymmetric key cryptography [4]. In symmetric or secret key cryptography, senders and recipients use a same key in encryption and decryption [4].

1.3 Block Diagram of Encryption and Decryption

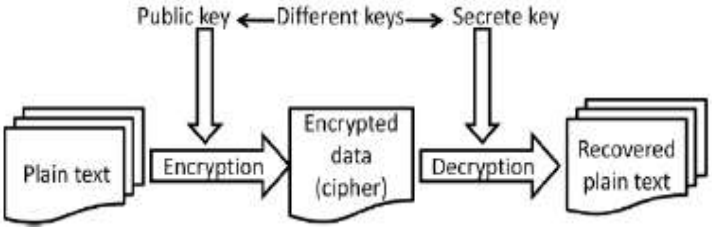

Fig. 4 Symmetric key encryption

Asymmetric or public key cryptography used different keys in encrypting image and decrypting messages received [4]. This procedure applied a public key and a private key to encode and decode an image correspondingly. on the other hand, both keys are exceptional, but scientifically have a connection.

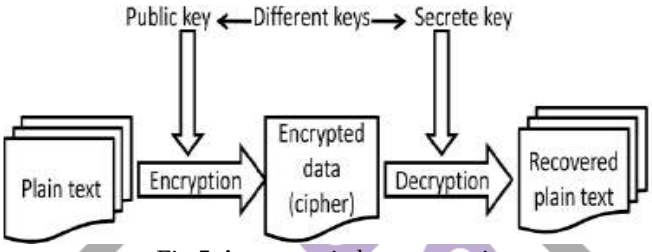

Fig.5 Asymmetric key encryption

The miscellaneous algorithms are available to encrypt information, particularly RSA, DES, AES, etc. nonetheless these algorithms are dominant to encipher a text data, however, inept for the image encryption [4]. Since, images have essential characteristics such as abundant dismissal and a strong connection between adjoining pixels [4]. So, one can effortlessly infer the values of neighbours of a pixel. Hence, images necessitate an efficient method to accomplish an invulnerable safety.

1.4 Image security

For image Encryption chaotic mapping techniques are used for scrambling the image pixels. And it can encrypt images by dealing out image widen and fold procedure. First of all a square image is divided into two isosceles triangles according the diagonal. Operating the difference of the pixel statistics of two adjacent columns of the triangles, each pixel in a column is interleaved to the adjacent column. The simple image can then be rigid to a line. [3]This line of image value can then be converted to 2D array for i.e. inform of encrypted image. Some of available scheme for image compression are JPEG-LS, SPIHT, JPEG2000, CALIC etc. Renovate like DWT or DCT are generally functional currently. The avail- able techniques use the transformation of pixels but the proposed method here doesn't transform rather it uses basic mathematical operations. Subsequent the numeral theoretic approach afford an additional advantage of image encryption, concurrently, using keys, making the transmit data both short and secure. And in casing of image hiding, the information will be in the form of image. This image is said to be the furtive image. Hence we are providing protection in the form of image. Fig.1 showed that how the process implicated in in sequence hiding. The secret image is first split into 9 parts. Suitable target image have to be particular. The selection procedure depends upon the database. The objective image should be picked from the database and that objective image should be a appropriate match for the source image. The objective image we have preferred should be double in size then the resource image. Mosaic image is then created. The tile images can be used constantly. By resources of a secret key, the mosaic image has been placed beneath the process and thus we are achievement the secret image after embedded process.[5]

II. RELATED WORK

M. Zeghid, M et al. 2007 [6] Here investigated the (AES) associated Encryption Standard and in their image encryption procedure they add a key stream generator (W7,A5/1) to AES for make sure the encryption arrangement.

Mohammad Ali Bani Younes et al. 2008 [7] this paper proposed a block-based uprising algorithm which is based on the agreement of image renovation and a well-known encryption and decryption algorithm called Blowfish. The original image was separated into blocks, and using the revolution algorithm it was rearrange, and then the Blowfish algorithm is used for encrypting the distorted image their results show that the correlation between image fundamentals was significantly decrease. Their results also show that increasing the figure of blocks by using smaller block sizes resulted in a lower relationship and higher entropy.

Bibhudendra Acharya et al. 2009 [8] This Image Encryption technique Using Self-Invertible Key Matrix of Hill Cipher Algorithm have proposed an advanced Hill (Advil) cipher algorithm which uses an Involuntary key matrix for encryption. They proposed

Advil cipher algorithm using the old one. And it is undoubtedly seen that original Hill Cipher is incapable to do its working appropriately as it did not encrypt the images accurately if the image consists of large area enclosed with same color or gray level. But their planned algorithm works for any images with different gray scale as well as color images.

Seyed Mohammad Seyedzade et al. 2010 [9] Novel Image Encryption Algorithm base on Hash Function and presented an algorithm depend on SHA-512 hash function, which was novel algorithm. It had 2 sections. First of all does pre-processing method to shuffle one half of image then hash function to generate a random number mask? The mask is then XORed with the other part of the image which is disappearing to be encrypted.

Amitava Nag et al. 2011 [10] This method of Image Encryption used Affine convert and XOR procedure, investigated a new algorithm using affine convert and was based on shuffled the image pixels. It was two phase encryption decryption algorithm. By utilized XOR gate operation they encrypted the resultant image and then used the affine renovated pixel value that is redistributed to diverse position with 4 bit keys. In the case of imprecise image then separated into 2 x 2 pixels blocks and all block is encrypted using XOR gate operation by four 8-bit keys. The result proves that the connection between pixel values was significantly reduced after the affine renovate.

Leo Yu Zhang et al. 2012 [11] in today's era colour image encryption algorithm based on chaos was presented by cascade two locality permutation operation and one switch over operation, which are all unwavering by some pseudo-random number sequences generate by iterating the logistic map. This paper evaluated the protection level of this encryption algorithm which find out the locality permutation-only part and the replacement part can be autonomously broken with only $\lceil(\log_2(3MN))/8\rceil$ and 2 chosen plain-images, correspondingly, where *MN* is the size of the plain-image. The efficiency of the planned chosen-plaintext attack is maintain by concise theoretical analysis and is established by experimental results.

Yogita Verma et al. 2013 [12] Here proposed encryption technique is used to defend multimedia data. There are diverse techniques used to protect private image data from unauthorized access. In this paper presented a susceptibility to investigated on reachable work that is employed totally dissimilar practice for image encryption and that furthermore, provide general introduction regarding cryptography. It has been survey about the presented works on the encryption techniques are AES, 3DES, Blowfish and DES.DES key size is too small as contrast to other techniques. 3DES is slower than other block cipher methods and has poor presentation AES is supposed to be better algorithm which was compared to original Blowfish Algorithm.

Dr. Parma Nand Astya et al. 2014 [13] a variety of encryption and decryption algorithms are available to defend the image from unauthorized user. RSA and Diffie-hellman key substitute provide a good level of safety but the size of encryption key in these two is a big problem. ECC is a better substitute for public key encryption. In this paper the image which is measured to be in the form of a grid, is first distorted on an elliptic curve. These points or coordinates are then encrypted and send to the receiver. At the recipient end decryption algorithm is utilized to exchange the encrypted image into the unique image. Brute force attack is infeasible for ECC since of the discrete logarithmic nature of elliptic curves and used technique to encrypt and decrypt the digital image (BMP) from Elliptic Curve Cryptography.

Ali Abdulgader et al. 2015 [14] This paper proposed a technique that overcome the fixed S-box weak points and improved the presentation of AES when used for encrypting images, predominantly when the image data are large. In adding together, the Mix Column stage is replace by chaotic mapping and XOR procedure to reduce the high computation in Mix Column transform. The proposed technique is tested on numerous images, and the results show that the proposed method efficiently engendered cipher images with very low connection coefficients of adjacent pixels and afford better encryption speed and high security as a result of the dependence of the S-box on the key description of the chaotic system

J. Gayathri et al. 2016 [15] A research work supported on chaotic cryptosystem has been presented to convince the specific desires defined for image communication. In spite of all the remarkable development neighbouring the chaotic cryptosystem, many of the proposed methods discuss with the mandatory number of characteristic that influenced the design of the cryptosystems. Associated with this issue, careful cutinisation of the performance of the existing chaos-based encryption technique is needed for its further development towards practical applications. Encryption technique used according to their association with the chaotic system engaged in three dissimilar categories has been propound to assess the protection and efficiency functions and summarised the existing image encryption techniques in all the three categories followed by a discussion on the security and efficiency constriction.

Cheng Qing Li Set al. 2017 [16] complex dynamics of chaotic map and technologies are used in encryption was studied systematically in the past two decades. Chaotic image encryption scheme was intended by iterating chaotic position permutation and value replacement some rounds, which arriving intensive concentration in the field of chaos-based cryptography. By choosing Chosen-cipher text assault on the Fridrich's scheme utilized influenced network between cipher-pixels and the analogous plain-pixels. This paper scrutinizes some properties of Fridrich's scheme with concise arithmetical language. Then, some minor defect of the real performance of Solak's attack method was given. The proposed work provided some basics for further optimizing attack on the Fridrich's scheme and its variants.

Xingyuan Wang et al. 2018 [17] proposed a new chaotic image encryption technique, which employs Josephus traverse and mixed chaotic map. The technique consists of three processes: key stream generation process; three-round scrambling process; and one-

round diffusion process. The proposed numerical model is applied for the key stream producer in the first process. The initial values and parameters are sensitive to both the secret keys in the new method and plain images. The second development employs the Josephus traversing in scrambling; then the rows and columns of pixels are exchange the third process can modify the pixel gray level values and crack the strong correlation between adjacent pixels simultaneously. The preliminary conditions for chaotic methods are derived using external secret keys by applying some algebraic transformations to the key. Security analysis indicates that the new scheme is effective which can oppose common attacks.

Rashad J. Rasras et al. 2019 [18] This paper will introduced three methods of image encryption-decryption, these method will be implement and tested, and the obtained investigational results will be compared with experimental results of the projected method in order to do some judgment concerning the efficiency and the security of the p Four methods of color image encryption-decryption were studied and all these methods gave efficient parameters. The fourth proposed method gave the best parameter by decreasing encryption-decryption time and acceptable values for MSE and PSNR, and it is highly secure because of the private key has several values and the number of values is variable and changeable the window size is variable and unpredictable reposed method.

III.PROPOSED APPROACH

To establish the efficiency of the proposed algorithm, we also performed a differential investigation to calculate NPCR and UACR and statistical for discriminating the histogram, entropy analysis, contrast analysis and CC analysis. Furthermore, Other DNA operations like DNA XOR, XNOR and bit shift have also been engaged with two other operations including addition and subtraction in accumulation to chaos maps. By recovering the DNA encoding approach using two additional operations that makes it easier to decode the encryption process. A single transform in the input bit can direct to enormous change in the output seed. Here we explained different terms used in proposed algorithm.

4.2 Random sequence generation using ILM

Due to its innate properties including periodicity and sensitivity to initial circumstances and control parameters, the chaos map technique has been utilized expansively for encryption process. Logistic Map (LM) is quite simple algorithm to realize and has very problematical vibrant behaviour. Hence, LM is the most commonly established chaos out of the many chaotic function projected. Equation 1 shows the arithmetical expression for the basic LM function.

$$Kr+1 = \delta * Kr\ 1 - Kr \quad (1)$$

Where *Kr* stands for the region (0,1] and represented the value in progression at *r*th location and δ is a control parameter which provide a absolutely chaotic sequence when it is in the range 3.57 and 4. Though LM has good periodicity, it is sensitive to one control parameter only and has a smaller key-space. The one-dimensional LM is extensive to two-dimensional as shown Esq. (2) and (3).

$$X_{r+1} = \delta_1 * X_r(1 - X_r) + \mu_1 * Y_r^2 \quad (2)$$

$$Y_{r+1} = \delta_2 * Y_r(1 - Y_r) + \mu_2(X_r^2 + X_r Y_r) \quad (3)$$

The given equations generate two chaotic sequence in the region (0,1] represent by X and Y. The chaos map is to be in chaotic state when δ and μ are taken as $2.75 < \delta 1 \leq 3.4$, $2.75 < \delta 2 \leq 3.45$, $0.15 < \mu 1 \leq 0.21$, $0.13 < \mu 2 \leq 0.15$. Likewise, this two-dimensional LM is promoting extensive to three-dimensional as depict in equation (4), (5), (6).

$$X_{r+1} = \delta * X_r(1 - X_r) + \mu Y_r^2 X_r + \lambda Z_r^3 \quad (4)$$

$$Y_{r+1} = \delta * Y_r(1 - Y_r) + \mu Z_r^2 Y_r + \lambda X_r^3 \quad (5)$$

$$Z_{r+1} = \delta * Z_r(1 - Z_r) + \mu X_r^2 Z_r + \lambda Y_r^3 \quad (6)$$

The above presented equations represented a non-linear system which exhibit chaotic state when δ and μ are taken as $0.53 < \delta < 3.81$, $0 < \mu < 0.022$, $0 < \beta < 0.015$ where $X0$, $Y0$ and $Z0$ are [0,1]. Based on the three-dimensional LM algorithm an inter-twining relative between three dissimilar LM sequence was considered which shows how for every iterations, the value of each sequence depends upon the other two sequence given in equation (7), (8), (9).

$$X_{r+1} = [\delta * \alpha * Y_r * (1 - X_r) + Z_r] Mod 1 \quad (7)$$

$$Y_{r+1} = [\delta * \beta * Y_r + Z_r * (1 + X_{r+1}^2)] Mod 1 \quad (8)$$

$$Z_{r+1} = [\delta * (Y_{r+1} + X_{r+1} + \gamma) * \sin(Z_r)] Mod 1 \quad (9)$$

δ have value between 0 and 3.9999, > 33.5, β > 37.9, μ > 35.7. Being a 3-dimensional LM, ILM conquer the drawback of one-dimensional LM such as stable windows, blank windows and irregular distribution of iterated sequence. Thus provide enhanced information entropy, thereby decreasing the achievement of encryption attacks. Further, ILM utilize along with DNA will again improve the efficiency of encryption process.

4.3 Permutation (Shuffling)

In third step, permutation is done where ILM performs iterations using the three seed value produced in the previous step. The three sequence fashioned by the ILM are then used to shuffled the one-dimensional R, G and B matrix. The fourth step, comprise converted the R, G and B pixels value into the DNA sequence. The seed values that produced in the first step are utilized to generate the mask DNA. DNA XOR, subtraction and addition operations are applied on mask DNA and one-dimensional R, G and B matrices. The diffusion carried by DNA's XOR, addition and subtraction operation that eliminated unnecessary data and unify all the pixels value. This step is performed out synchronously on pixels of each of the R, G and B matrices by shuffling the diffused pixels obtained.

4.4 DNA Encoding

These days, DNA computation is prominent as a tool for just beginning higher protection cryptosystems. DNA-based image cryptosystems used DNA as a starting place to carry out information and use DNA computation method for accomplish image encryption. DNA has four nucleic acid bases that are adenine (A), cytosine (C), guanine (G) and thymine (T) where A is reciprocal of T and G is the reciprocal of C and vice versa Given in the table-2. These associations are named as Watson–Crick complement rule presented by the two scientists. Comparable to the conservative binary operations of the DNA sequences also have addition, subtraction and XOR operations. Table 1 gives the DNA encoding rules, and Table 2 showed DNA XOR operation that is use widely for performing image encryption.

	A	C	G	T
Rule 1	00	10	01	11
Rule 2	00	01	10	11
Rule 3	11	10	01	00
Rule 4	11	01	10	00
Rule 5	10	00	11	01
Rule 6	01	00	11	10
Rule 7	10	11	00	01
Rule 8	01	11	00	10

Fig.11 encoding and decoding of DNA rule

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Fig.12 DNA XOR Operation

4.5 Performance Matrix

Here we used some terms in performance matrix defined as below:-

4.5.1 Entropy

Entropy is a significant aspect of randomness that is used for defining rank of improbability in images. The entropy parameter can be used in measuring the identical distribution of pixels value during the images. Higher is the value of entropy, higher will be the improbability or randomness caused by uniform distributions of pixels throughout. The preferable image entropy value is eight. Hence, for a good image encryption algorithm the entropy value should be closer to eight. The arithmetical formula for the information entropy calculations is given as below:

$$H(m) = \sum_{i=0}^{2^N - 1} P(m_i)\log_2 \frac{1}{P(m_i)},$$

Where N is the number of grey level and has a value 8 in case of grey level image and M (= 2N) denoted as the total number of symbol. m_i M and $P(m_i)$ is the probability of having m_i levels in the image. The information entropy details use color components R, G, B for the encrypted color image.

4.5.2 UACI, NACR

By doing a judgment of the two images, an association is realized between the original image and the encrypted image, i.e. called as encryption process. To test the effect of differential evolution, two indices are used: Number of pixel change rate (NPCR) and Unified average changing intensity (UACI). These two terms are defined as:

$$NPCR = \frac{1}{P \times Q} \sum_{j=1}^{P} \sum_{k=1}^{Q} D(j,k) \times 100\% \quad (10)$$

$$UACI = \frac{1}{P \times Q} \sum_{j=1}^{P} \sum_{k=1}^{Q} \frac{|c_1(j,k) - c_2(j,k)|}{255} \times 100\% \quad (11)$$

where D(j,k) in NPCR is defined as

$$D(j,k) = \begin{cases} 1, & c_1(j,k) \neq c_2(j,k) \\ 0, & otherwise \end{cases} \quad (12)$$

NPCR signify the percentage of pixels in the encrypted image that changed, and UACI is the proportion of the average transform in intensity of corresponding pixels. c_1 and c_2 are the two encrypted images and c (i, j) is the pixel value at index [i, j] in the image. To examine NPCR and UACI, two images opposed only in one pixel are encrypted with same secret key, and the results are tabulate.

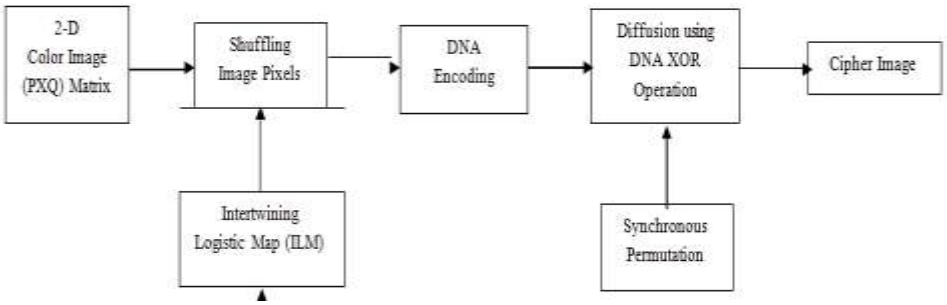

Fig.13 Block diagram of proposed approach

4.5.3 Histogram

Histogram is an essential statistical characteristic of an image and it demonstrated the frequency of pixels allotment throughout the image. Histograms are the plan of number of pixels for each pixel values in the image. Plain image have steep histogram, thus shows that information can be fetch from them. In addition to this, ciphered image should have histogram as smooth as potential thus ensure higher level of randomness.

4.5.3 Correlation

It established the relationship between two adjacent pixels of image. In a significant image, the correlation function is very high between adjacent pixels of image, while the correlation coefficients of an encrypted image ought to be irrelevant enough. The correlation between two pixels can either be horizontal, vertical or diagonal and thus it provide three version of the coefficient. The correlation coefficient *rxy* accurately expressed by using Eqs. (13) to (16).

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (13)$$

$$cov(x,y) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)) \quad (14)$$

$$D(x) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \quad (15)$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S}x_i \quad (16)$$

Where x and y are the two adjoining pixel and S is the count up of such pixel duplet (x,y) in use from the image. E(x) and D(x) correspondingly denoted anticipation and variance of x. To scrutinize the correlation coefficient in an image, two neighboring pixels are compulsory. Hence, the method used is: first, 1000 pairs of pixels are preferred randomly from the image, and secondly the correlation coefficient is considered using the chosen set. The pixels preferred at random are first all horizontal, then vertical and at last diagonal so as to compute the three variants of the correlation coefficient.

IV EXPERIMENTS AND RESULTS

Simulation Results

.

Entropy- The preferable image entropy value is eight. Hence, for a good image encryption algorithm the entropy value should be closer to eight. Higher is the value of entropy, higher will be the improbability or randomness caused by uniform distributions of pixels throughout.

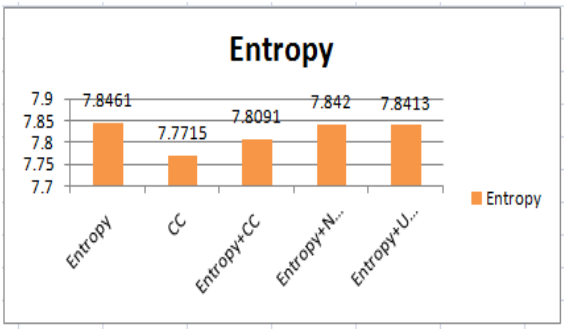

Fig23. entropy for uniform distribution of pixels

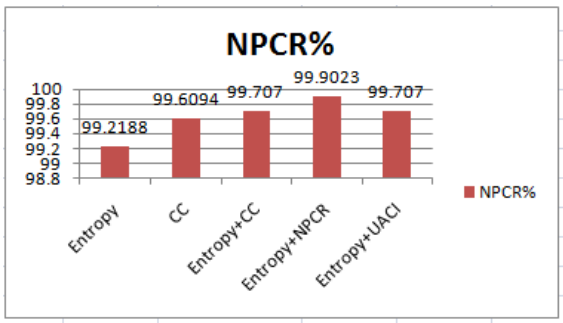

Fig.24. Number of pixel change rate (NPCR)

Calculate NPCR and UACI- NPCR signifies the percentage of pixels in the encrypted image that changed, and UACI is the proportion of the average transform in intensity of corresponding pixels. These are used to test the effect of differential evolution, And here from results it is clear that it is approximately 100.

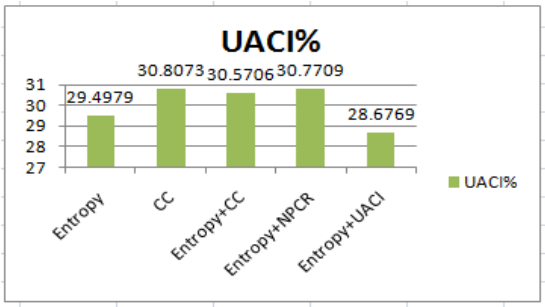

Fig.25.Unified average changing intensity (UACI)

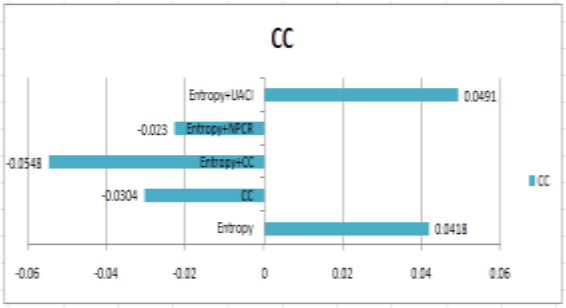

Fig.26. Correlation Coefficient (CC)

Correlation Coefficient (CC)- it established the relationship between two adjacent pixels of image. In a significant image, the correlation function is very high between adjacent pixels of image. The correlation between two pixels can either be horizontal, vertical or diagonal and thus it provide three version of the coefficient.

Objective	Entropy	NPCR	UACI	CC
Entropy	7.8461	99.2188	29.4979	0.0418
CC	7.7715	99.6094	30.8073	-0.0304
Entropy + CC	7.8091	99.707	30.5706	-0.0548
Entropy + NPCR	7.842	99.9023	30.7709	-0.023
Entropy + UACI	7.8413	99.707	28.6769	0.0491

Fig.27 Table of different parameter calculation

V CONCLUSION

The algorithm has been proposed to formulate a well-organized and secured approach towards Image encryption. (ILM) image logistic map helps to improve the encoding efficiency of image, and along with it DNA diffusion ensures secured transmissions due to its additional operations including XOR, subtraction and addition of information. The proposed approach is fast and accurate due to a synchronous permutation-diffusion technique. In addition to it, Genetic algorithm (GA) is advantageous to resist encryption attacks. Theoretical analysis and experimental results confirmed that the algorithm produced better information entropy when ILM is used for encryption along with DNA and GA. Optimization techniques like Genetic Algorithms (GA) can be implemented on the proposed method in order to achieve efficacious encryption and even better results in the future

REFRENECES

[1] Xiliang Liu, "Selective encryption of multimedia content in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.

[2] Marwa Abd El-Wahed, Saleh Mesbah and Amin shoukry "Efficiency and Security of some Image Encryption Algorithm". Vikram Jagannathan, Aparna Mahadevan, "Number Theory Based Image Compression Encryption and Application to Image Multiplexing", pp. 59-64. 2007.

[3] Feng Huang, Chao Wang, "A New Image Encryption Arithmetic Based on a Three- dimensional Map" , vol. 58, no. 7, pp. 83-91, 2001.

[4] Akshat Agrawal, Ankit Garg," A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications · July 2014

[5] Ali Al- Haj, Hiba Abdel Nabi, "Digital image security based on data hiding and Cryptograpgy", IEEE 3rd international conference on communication technology, 2017.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, A Modified AES Based Algorithm for Image Encryption World Academy of Science, Engineering and Technology 27 2007.

[7] Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35, 2008.

[8] Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[9] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, A Novel Image Encryption Algorithm Based on Hash Function 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[10] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation ,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[11] Leo Yu Zhang, Rong Ou, Kwok Wo Wong and Shi Shu," Breaking a novel colour image encryption algorithm based on chaos", Springer, 11 octuber 2012.

[12] Yogita Verma, Neerja Dharmale, "A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,2013.

[13] Dr. ParmaNand Astya , Ms. Bhairvee Singh , Mr. Divyanshu Chauhan," Image Encryption And Decryption Using Elliptic Curve Cryptography", International Journal of Advance Research In Science And Engineering http://www.ijarse.com IJARSE, Vol. No.3, Issue No.10, October 2014.

[14] Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal, Tarik Idbeaa, "Enhancement Of Aes Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption", Journal of Theoretical and Applied Information Technology ,Vol. 71 No.1, 2015.

[15] J. Gayathri , S. Subashini ," A survey on security and efficiency issues in chaotic image encryption", International Journal of Information and Computer Security , Volume 8, Issue 4,2016.

[16] ChengqingLi SiminYu JinhuLü ," On the cryptanalysis of Fridrich's chaotic image encryption scheme", Science direct, Signal Processing ,Volume 132, , Pages 150-154, March 2017.

[17] Xingyuan Wang, Xiaoqiang Zhu, And Yingqian Zhang," An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," IEEE, volume-6, 2018.

[18] Rashad J. Rasras ; Mohammed Abuzalata ; Ziad Alqadi ; Jamil Al-Azzeh ; Qazem Jaber," Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation", IJCSMC, Vol. 8, Issue. 3, March 2019, pg.14 – 26, 2019