Efficient Image Encryption with Pixel Scrambling and Genetic Algorithm

Surya R[1], Premkumar R[2]

[1]PG scholar, Department of ECE Mount zion College of Engineering and Technology, Tamilnadu, India
[2]Assistant professor, Department of ECE, Mount zion College of Engineering and Technology, Tamilnadu, India

Abstract - Advanced image managing, as a PC based innovation, visual data plays an undeniably essential job in numerous parts of our day by day life, to them from unapproved parties are increasingly vital. In this article an effective picture encryption with GA is proposed. The proposed strategy utilizes a picture encryption/decoding calculation dependent on random shuffling of pixels and permutation, substitution process. Earlier stage picture is partitioned and pixels are revised to make partially encoded picture. At last Permutation and substitution task are performed. Prior stage picture is divided and pixels are rearranged to make in part encoded picture. At last Permutation and substitution task are performed. Examinations are performed to watch the security of the framework.

Key Words: Block crossover, bitplane, mutation, genetic algorithm, scrambling

1. INTRODUCTION

Nowadays, picture encryption is among rapidly creating headways. It shapes focus inquire about zone inside structuring and programming designing controls also. Encryption is the way of transforming the information to make sure its security. With the rapid development of web and computer network, a huge amount of computerized information is being exchanged over different kinds of systems. The protection of digital information including pictures has involved more attention and various picture encryption techniques have been planned to improve the security of these pictures. Any picture encryption dependent on pixels framework is partitioned into two strategies: pixel replacement techniques and pixel scrambling strategy. In the pixel replacement technique, every pixel in the picture needs to change its values and this method also called us substitution. But, in the pixel modification scheme, the pixel needs to change its position and this technique is called confusion.

The encryption process and the decryption process explained in [1] exactly same. They similarly comprise of the comparable activities of plaintext-related scrambling once, dispersion twice and grid pivoting of 180 degrees multiple times [1]. Adaptive wavelet transform in frequency domain used for data hiding and genetic algorithm also used to encrypt the image in paper [2]. Using the travelling salesman algorithm the s box process is changed, and this s box is supported on ga. S box is an essential constituent in encryption method is filed in [3]. Cipher images are made up of using the chaotic function. After that GA initialize the population and in each stage the respond is gained from earlier stage iteration to produce a most excellent encrypted image is explained in [4].

Clients have the adaptability to pick an) any current or recently created picture as source picture b) any deterioration strategy for producing the bitplane c) any disintegrated bitplanes as the precautions key bitplane d) any scrambling technique for the bit dimension change are designed in [5]. A plausibility reproduction for separate the circulations of picture contrasts dependent on bitplane imaginable potential and carvings among bit planes. Analyze through the present picture disparity portrayals which envision the disseminations incorporate itemized setups. This model offered a group parametric showing that can be utilized to shape arbitrary conveyances with no usage a few careful restrictions on the appropriations [6].

The regular fractal measurement process is diminished in sectioning lopsided substance beginning multifaceted surroundings since it can't separate the nearby grayscale among the substance and the composite surroundings additionally divergent sizes of the substance, which are easy to starting point under-division. To get better division impact, an improved picture division technique dependent on bit-plane and morphological remaking is proposed in [7]. Three vital contributions are presented in [8] a) reason for critical bitplanes, b) encryption of just the real biplanes most imperative to diminish in computational intricacy and c) rejection of the required for part channel for pass on the succession by means of reverence to the major bitplanes. Another strategy to use a security framework for correspondence of advanced stuffing over network systems [9]. Stretch out change process based ensured many shading picture encryption framework which is totally unique than the nearly utilized a few picture encryption framework [10].

Two-dimensional unadulterated picture is changed to one measurement. From that point onward, with the motivation behind trim down the exchanging procedure time, stage and dispersion ventures for a few pixels are completing in the comparative time [11]. There are six dissimilar permutation methods based on confused and non messy producers are explained [12]. The stage is accomplished by dough puncher map and the substitution by a key identified with plain picture calculation dependent on the altered Logistic guide. Adjustment of the Logistic guide is advanced to support the opportunity of the encryption key, and along these lines support the security [13]. In paper [14] contains four stages: dissemination, substitution, dispersion and change. Dissemination is finished by bitwise XOR activity and new clamorous guide, substitution is finished by solid S boxes, third technique is finished by calculated guide are advertised. In conclusion a square stage is capable by a change work [14]. The arranged strategy makes utilization of coupled cross section guide to deliver the measure of ensured figure pictures as essential position of changed hereditary calculation. What's more, after that it relates the changed hereditary calculation to both lift the entropy of the encryption and drop off the computational time [15]. The calculated guide is use to make number of veil and GA is utilized to locate the most magnificent cover for encoding [16].

Change is finished by round move by lines and sections and substitution is finished by legitimate administrators. This framework is awfully sympathetic to each key and it reproduces the picture well great quality [17]. A irregular arrangement is utilized to locate the beginning spot position in the wave and produces a dissemination vehicle for measured procedure [18]. This technique is isolated into three sections: mystery key age, picture change and dissemination. Mystery keys contains of two phases. One is arbitrary keys and another one is hash cluster keys [19]. The plain image is transformed into two binary sequences of the same size. Subsequently, a fresh diffusion stratagem is initiated to circulate the two sequences reciprocally [20].

2. PROPOSED SYSTEM

To begin with two color image as input of the system. The plain images are segmented using split and merge segmentation. Then the segmented blocks are shuffled randomly. Again the shuffled blocks pixels are randomly scrambled after that block permutation is performed. The permuted image decomposed into eight planes and then combined finally hybrid substitution is performed. Three types of substitution are performed here; they are transpose, swap, and circular shift. Using 3d logistic map key generation is performed.

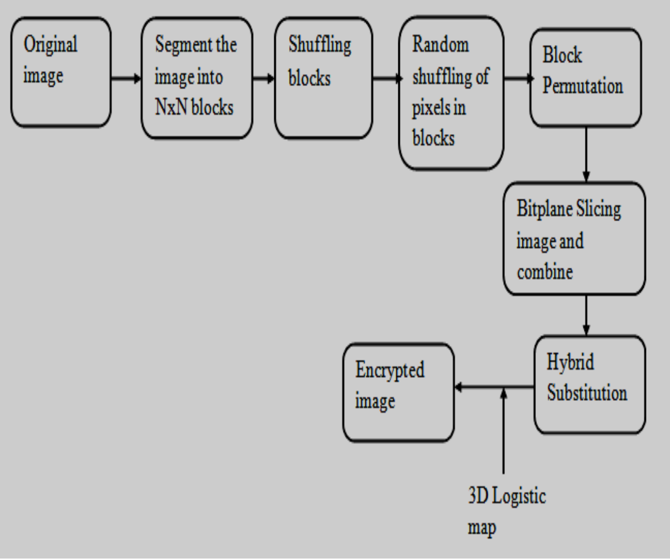

Original image
Segment the image into NxN blocks
Shuffling blocks
Random shuffling of pixels in blocks
Block Permutation
Bitplane Slicing image and combine
Hybrid Substitution
Encrypted image
3D Logistic map

Fig. 1 Encryption system

2.1 Segmentation

Segmentation is the progression of separating an image into having an important effect part, here we using a split and merge segmentation. We perform different block size to split the image. In this analysis we came to know that splitting small size of blocks are gave more efficient results.

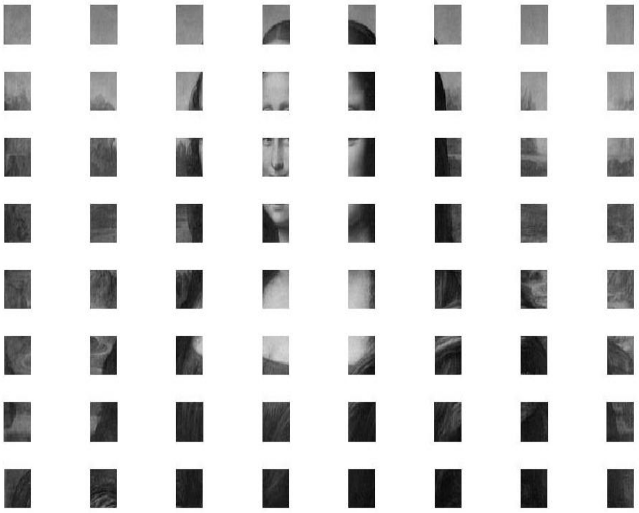
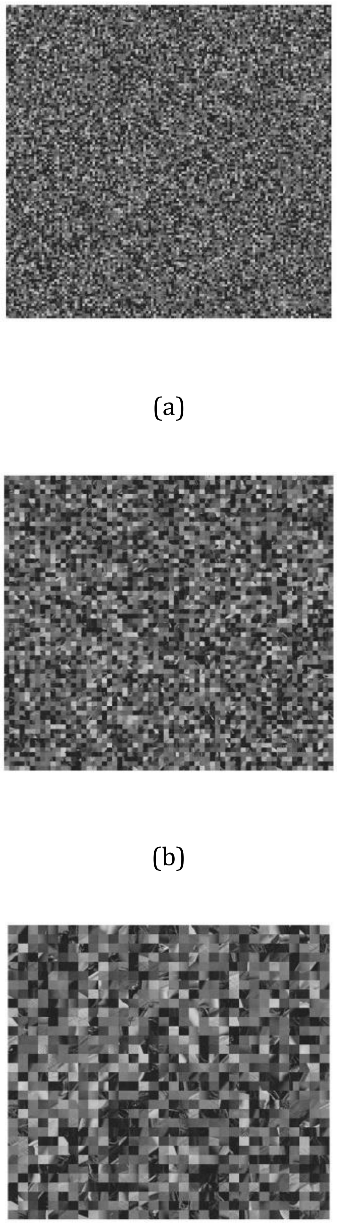


Fig. 2 Divided image

2.2 Random shuffling of pixels

Scrambling affords excellent security to the system. Scrambling is nothing but change the pixels of an image randomly. We have done with 4x4, 8x8 and 16x16. Outcomes shown in fig.2



(a)

(b)

(c)

Fig. 3(a) Scrambling with size of 4x4 (b) Scrambling with size of 8x8 (c) Scrambling with size of 16x16

2.3 Bitplane slicing algorithm

With the help of this algorithm we separate the LSB and MSB of the image. And the n combine the LSB and MSB to get partial image with random noise.

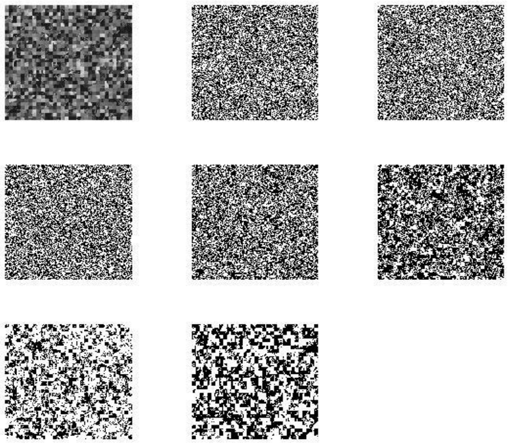


Fig. 4 Bit plane slicing of Scrambled image

2.4 Genetic algorithm realization

Two main operators are in GA. They are crossover and mutation. In first stage block swapping permutation is done and in mutation three types are hybrid.

The hybrid administrator is practically equivalent to generation and natural hybrid. In this more than one parent is chosen and at least one off-spring is delivered utilizing the hereditary material of the guardians. Hybrid is generally connected in a GA with a high likelihood.

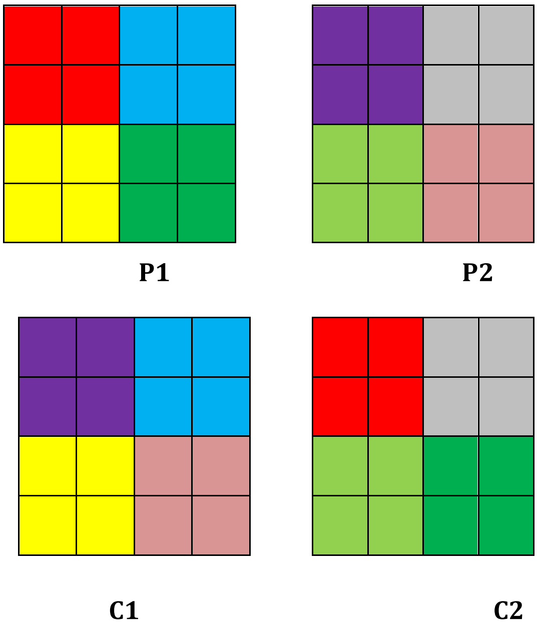


Fig. 5 Block crossover using GA

2.5 Mutation

In basic terms, change might be characterized as a little irregular change in the chromosome, to get another arrangement. It is utilized to remain awake and present assorted variety in the hereditary populace and is normally connected with a low likelihood – pm. On the off chance that the likelihood is high, the GA gets decreased to an irregular hunt.

Change is the piece of the GA which is identified with the "investigation" of the pursuit space. It has been seen that transformation is fundamental to the intermingling of the GA while hybrid isn't. three types of mutation.

- Random Swap
- Transpose
- Circular shift

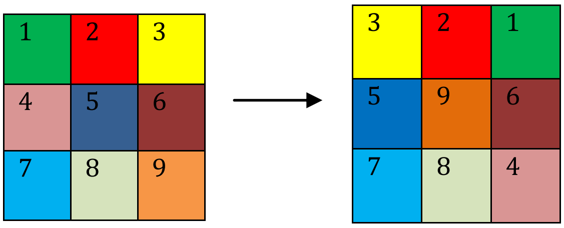


Fig. 6 Random swap

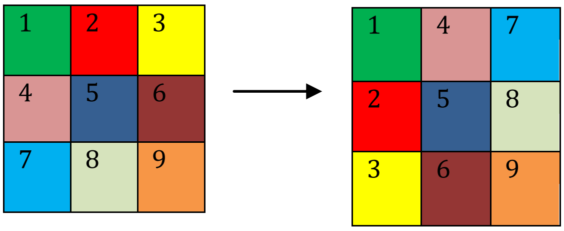


Fig. 7 Transpose

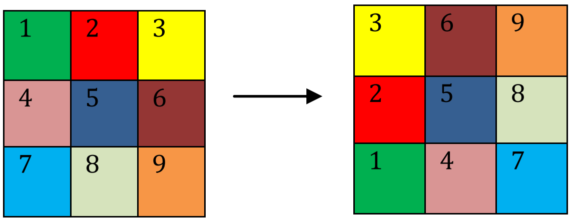
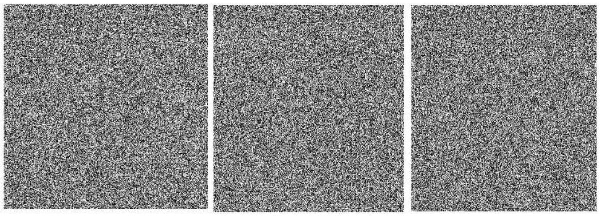


Fig. 8 Circular shift



(a) (b) (c)

Fig. 9 Mutation results. (a) Circular shift mutation (b) Transpose mutation (c) Flip mutation.

3. EXPERIMENTAL ANALYSIS

The planned encryption algorithm is capable of encrypt dissimilar sizes of images. This part affords testing consequences to demonstrate its encryption presentation. Every single one testing's executed with MATLAB 2010a in a mainframe with the configurations of Intel(R) Pentium(R) CPU 2.10 GHz; with 2 GB RAM, and Microsoft Windows 7 operation system. Our arrangement has two CPUs and one GPU.

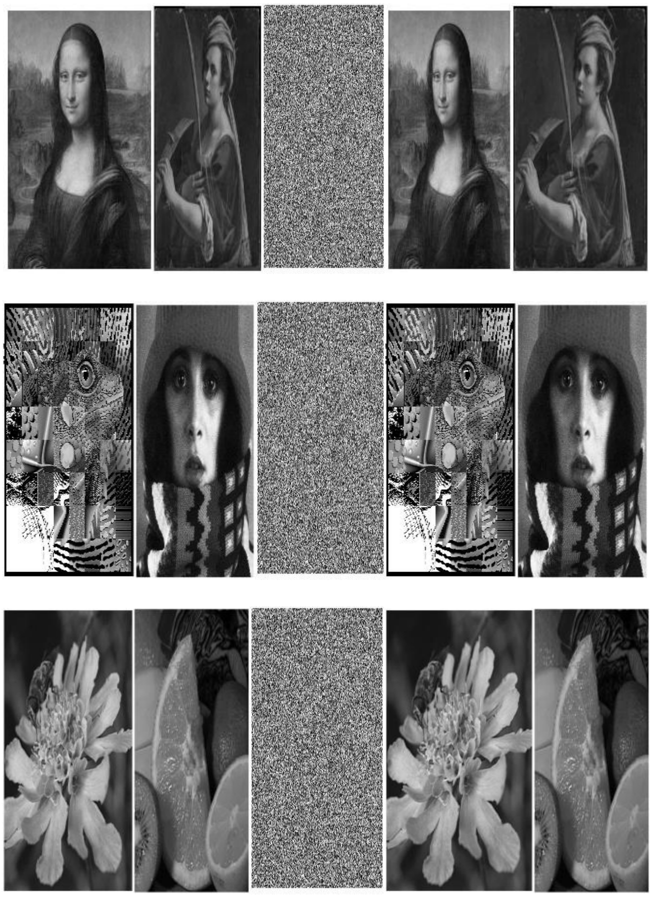


Fig. 10 Plain image and Encrypted, decrypted image

3.1 Histogram

We can obtain the allocation of pixel values of a figure from its histogram. If it is not smooth enough, a little quantity of sequence able to be leaked by the numerical attack. Therefore, a uniform and even allocation is attractive for a high-quality encryption method. The histograms of plain image and its encrypted image by the planned algorithm are shown in Fig. 6. It is understandable that histogram of the encrypted image is unvarying and considerably unlike from that of the plain image. So our algorithm able to build the statistical attack unacceptable.

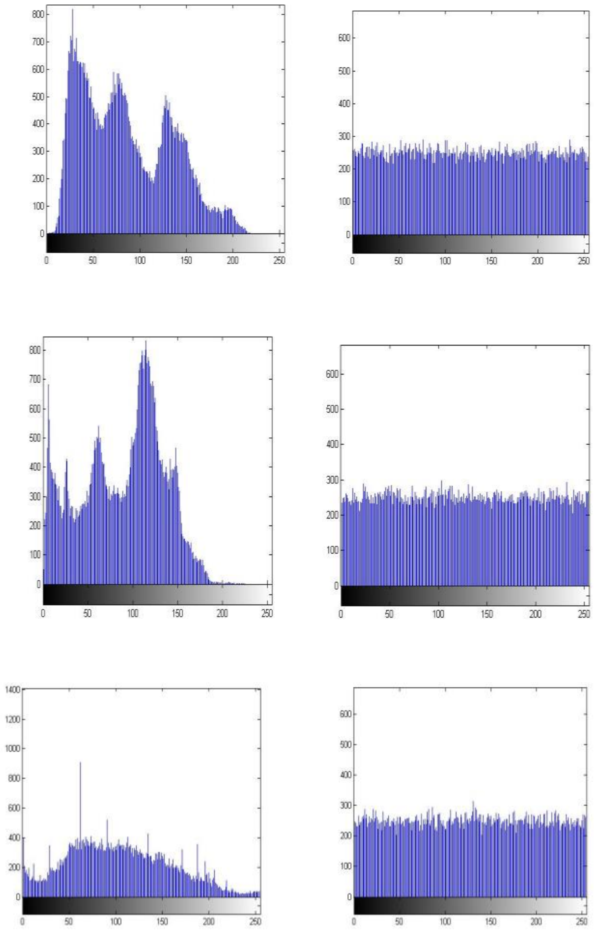


Fig. 11Histogram of original image and encrypted

3.2 Correlation analysis

Correlation analysis is worn to experiment the connections of adjoining pixels in the original image and encrypted image. 3000 pairs of adjacent pixels from the primary picture and scrambled picture are chosen arbitrarily in the event, vertical and corner to corner headings to execute this examination. Figure 7 plots the correlations of two adjacent pixels in three directions for Lena.

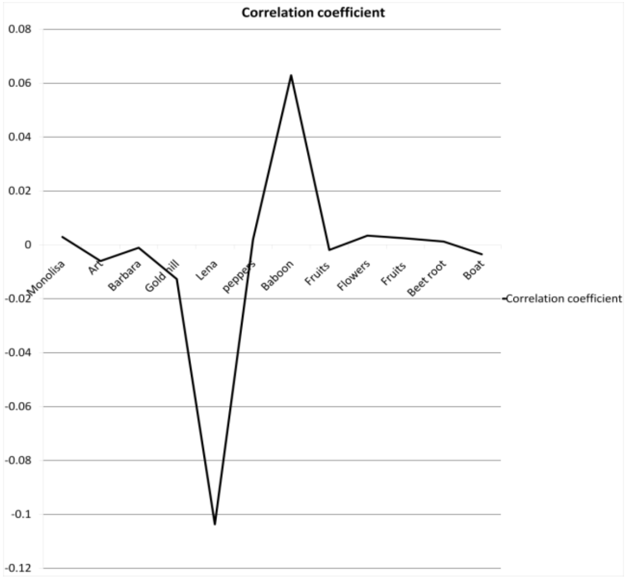


Fig .12 Comparisons of correlation coefficients

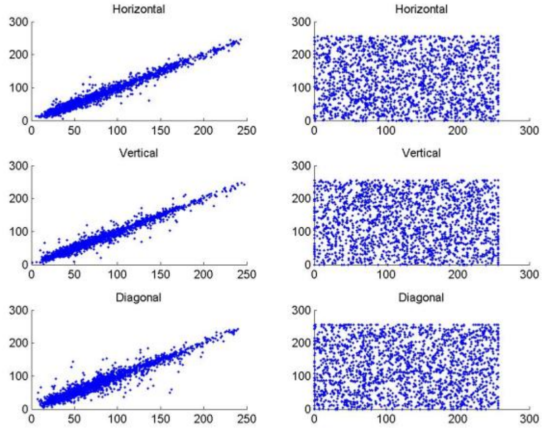


Fig. 13 Correlation of two adjacent pixels for standard image

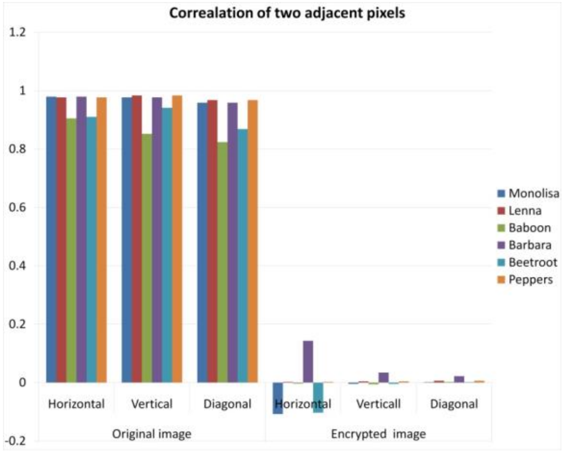


Fig .14 Correlation coefficients of two adjacent pixels in plain image and cipher image

3.3 Information entropy

The information entropy able to be designed by,

$$H(m) = \sum_{i=0}^{2^n-1} x(m_i) log \frac{1}{x(m_i)}$$

In which H(m) represents the information entropy of an sequence source m, x(mi) denotes the probability of symbol mi.

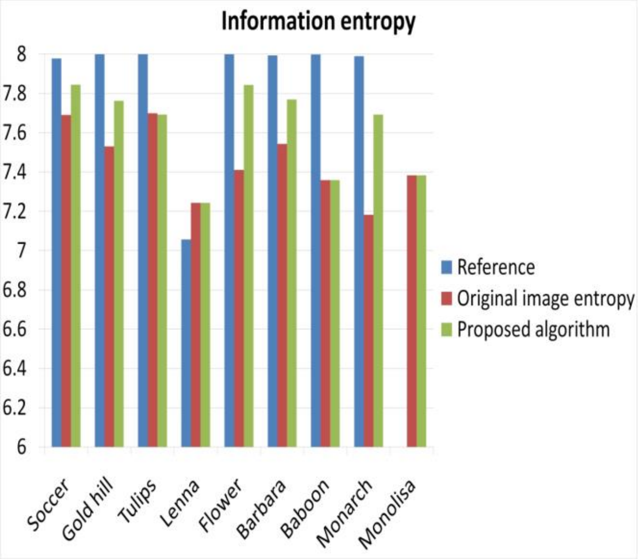


Fig .15 Information entropy of original and encrypted image

3.4 NPCR and UACI

In the discrepancy harass, a minor variation is prepared to the original image, and the proposed algorithm is engaged to encrypt the plain image earlier than and behind this transform. These two ciphered images have been evaluated to discover every achievable connection between the plain image and the ciphered image. Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) are two criterion generally used by researchers to inspect the differential attack resistance of any encryption algorithm. The NPCR and UACI are shown as Eqs.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{MxN} \times 100\%$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |c_1(i,j) - c_2(i,j)|}{255 \times M \times N} \times 100\%$$

Subjected to:

$$D(i,j) = \begin{cases} 0 & if\ c_1(i,j) = c_2(i,j) \\ 1 & if\ c_1(i,j) \neq c_2(i,j) \end{cases}$$

where M and N denote height and width of the image, respectively. $C1$ and $C2$ are two encrypted-images with one pixel difference. Fig .12 lists the best and average NPCR and UACI values.

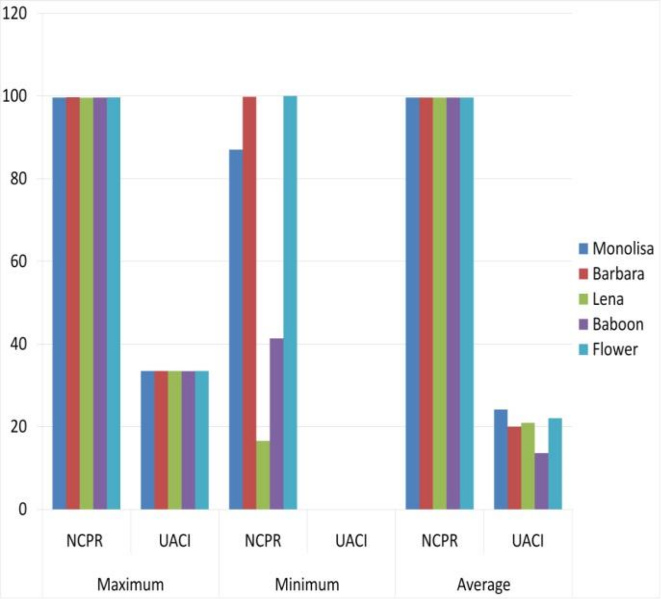


Fig .16 Security comparisons between different encryption method by number of pixel change rate (NPCR) and unified average changing intensity (UACI)

3.5 Speed analysis and performance comparison

Running speed is an important characteristic parameter for encryption algorithms, when the security level may meet the requirements. Genetic-based image encryption scheme is mostly composed of crossover process and mutation process. In the proposed algorithm, block swapping and hybrid mutation process is used. This leads to a speed advantage when compared with other algorithms.

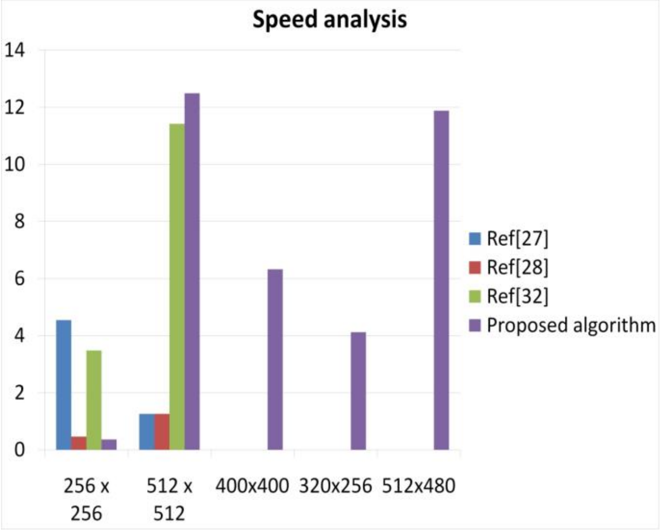


Fig .17 Encryption speed comparison

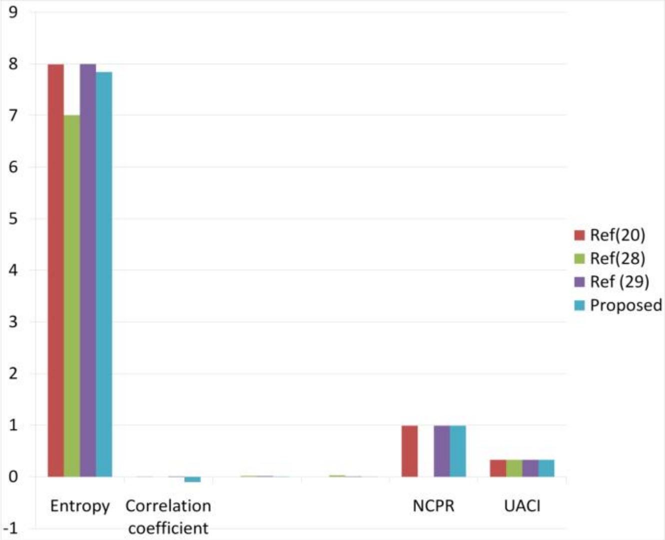


Fig .18 Performances of the proposed scheme and five comparable methods for (256 x 256)

4. Conclusion

This paper suggested an encryption based on bitplane decay with block permutation of pixels. In our system original image is split using segmentation algorithm. And then scrambling pixels are in first stage. Then the scrambled image is sliced into eight bitplanes using bitplane slicing algorithm, and swapping its blocks randomly then and mutation operation is completed. To increase the security of the system block swapping crossover and hybrid mutation is performed. Some analysis are completed to validate the system rate and safety.

REFERENCE

1. Yong Zhang, Yingjun Tang(2018), 'A Plaintext-Related Image Encryption Algorithm Based on Chaos' , Multimedia Tools and Applications, Vol. 77, No. 6, pp. 6647-6669.

2. Aref Miri, Karim faez(2017), 'Adaptive Image Stenography Based on Transform Domain via Genetic Algorithm', Optik – International Journal For Light and Electron Optics, Vol. 145, pp. 158-168.

3. Yong Wang, Kwok-Wo Wong, Changbing Li, Yang Li(2012), ' A Novel Method to Design S-box Based on Chaotic Map and Genetic Algorithm', Physics Letters A, Vol. 376, No. 6-7, pp. 827-833.

4. Abdul Hanan Abdullah, Rasul Enayatifar, Malrey Lee(2012), ' A Hybrid Genetic Algorithm and Chaotic Function Model For Image Encryption', International Journal of Electronics and Communication,Vol. 66, No. 10, pp. 806-816.

5. Yicong Zhou, WeijiCao, Philip Chen C.L (2014), 'Image Encryption Using Binary Bitpane' Signal Processing, Vol. 100, pp. 197-207.

6. Choy S.K, Kevin Yuen, Carisa Yu (2018), ' Fuzzy Bit plane dependence Image Segmentation', Elsevier – Signal Processing, Vol. 154, pp. 30-44.

7. Yanfen Lin, Liuxi wu (2018), 'Improved Abrasive Image Segmentation Method Based on Bit-plane And Morphological reconstruction', Springer – Multimedia Tools and Applications, pp. 1-14.

8. Sukalyan som, Abhijt Mitra, Sarbani Palit, B.B.Chaudhuri (2018), 'A Selective Bitplane Image Encryption Scheme Using Chaotic Maps', Springer – Multimedia Tools and Applications, pp. 1-28.

9. Ranjeet Kumar singh, Binod Kumar, Dilip Kumar, Danish Ali Khan(2018), ' Level by Level Image Compression-Encryption Algorithm Based On Quantum Chaos map', Journal of King Saud University – Computer and Information Sciences, Vol. 75, No. 22, pp. 14685-14706.

10. Abimanyu Kumar Patro K, Bibhudedra Acharya (2018), 'Secure Multi-level Permuation Operation Based Multiple Colour Imge Encryption', Elsevier – Journal of Information Security and Applications, Vol. 40, pp. 111-133.

11. Rasul Enayatifar, Adul Hanan Abdullah, Ismail Fauzi Isnin, Ayman Altmeen (2017), ' Image Encryption Using A Synchronous Permutation-diffusion technique', Elsevier – Optics and Laser Engineering, Vol. 90, pp. 146-154.

12. Salwa K. Abd –El-Hafiz, Sherif H.AbdElHaleem, Ahmed G.Radwan (2016), 'Novel Permutation Measures For Image Encryption Algorithm', Elsevier – Optics and Laser Engineering, Vol. 85, pp. 72-83.

13. Ramadan Noha, Ahmed HossamEldin H, El-khamy said, Abdul El-samie fathi E (2017), ' Permutation-substitution Image encryption based on a modified chaotic map in transform domain', Springer – Journal of Central South University, Vol. 24, No. 9, pp. 2049-2057.

14. Akram Belazi, Ahmed A. Abd El-Latif, Safya Belghith (2016), 'A Novel Image Encryption Scheme Based On Subsitution-Permutation Network and Chaos', Signal Processing, Vol. 128, pp. 155-170.

15. Hossein Nematzadeh, Rasul Enayatifar, Homayun Motameni, Frederico Gadelha Guimmaraes, Vitor Nazario Coelho (2018), 'Medical Image Encryption Using a Hybrid Model Of Modified Genetic

Algorithm and Coupled Map Lattices', Optics and Laser Engineering, Vol. 110, pp. 24-32.

16. Rasul Enayatifar, Abdul Hanan Abdullah, Ismail Fauzi Isnin (2014), 'Chaos-Based Image Encryption Using A Hybrid Genetic Algorithm And A DNA Sequence', Elsevier – Optics and Laser Engineering, Vol. 56, pp. 83-93.

17. Zahra Parvin, Hadi Seredarabi, Mousa Shamsi (2014), 'A New Secure And Sensitive Image Encryption Scheme Based On New Substitution Chaotic function', Springer – Multimedia tools and Applications, Vol. 75, No. 17, pp. 10631-10648.

18. Guodong Ye (2014), 'A Block Image Encryption Algorithm Based On Wave Transmission and Chaotic Systems', Springer – Nonlinear Dynamics, Vol. 75, No.3, pp, 417- 427.

19. Mingxu Wang, Xingyuan Wang, Yingqian Zhang, Zhenguo Gao(2018), ' A Novel Chaotic Encryption Scheme Based On Image Segmentation and Multiple Diffusion Models', Optics and Laser Technology, Vol. 108, pp. 558-573

20. Lu Xu, Zhi Li, Jian Li, Wei Hua (2015), 'A Bit-Level Image Encryption Algorithm Based on Chaotic Maps' Optics and Lasers in Engineering, Vol. 78, pp. 17-25

BIOGRAPHIES

Surya R, BE(Electronics and communication engineering) – Anna university, Trichy, ME(communication systems) – Mount zion college of engineering and technology, Pudukottai.

R. Premkumar was born in india 1984. He received a B.E degree in Electronis and Communication Engineering from anna university Chennai in 2005. He received the M.E degree in VLSI Design from Anna university, Chennai in 2017. He is currently submitted the Ph.d thesis at anna university, Chennai. His area of interest are media, security, image Processing, vlsi design, cryptography. He is the Life time member ISTE,IETE and CSI