A Survey on Protecting Image Using Blowfish and Chaos Base Image Encryption with Butterflies Permutation

[1]Rajkumar B. Gondaliya, [2] Dr. Daxa V. Vekariya, [3] Pratixa Badeliya, [4] Dr. Vipul M Vekariya

[1] PG Scholar of Computer Engineering Department, Noble Group of Institute, Junagadh, Gujarat, India
[2] Associate Professor, Computer Engineering Department, Noble Group of Institute, Junagadh, Gujarat, India
[3] Assistant Professor, Computer Engineering Department, Noble Group of Institute, Junagadh, Gujarat, India
[4] Principal & Professor, Computer Engineering Department, Noble Group of Institute, Junagadh, Gujarat, India

Abstract : Images have become one of the most efficient methods of information transfer, now a day's images are preferred. But while transferring the images, means while communicating with each other care must be taken to check that the information reaches only to the desired receiver and not to any other sources. So there is a need of secrecy between source and destination. In order to achieve this some techniques and methods are needed. While transferring information means image has to be sent in such a way that only source and destination can have access to it and also care must be taken to see that even though images are accessed by some unauthorized sources the information is not understood to them. Digital image scrambling is one of the most prominent techniques used for secure transmission of digital images. Various image encryption algorithms based on the permutation–diffusion architecture have been proposed where, however, permutation and diffusion are considered as two separate stages, both requiring image-scanning to obtain pixel values.

***IndexTerms* – Image Processing, Image encryption, Image security, Image protection.**

I. INTRODUCTION

Now a day's, Images have become one of the most efficient methods of information transfer. But while transferring the images, means while communicating with each other care must be taken to check that the information reaches only to the desired receiver and not to any other sources. So there is a need of secrecy between source and destination. In order to achieve this some techniques and methods are needed. While transferring information means image has to be sent in such a way that only source and destination can have access to it and also care must be taken to see that even though images are accessed by some unauthorized sources the information is not understood to them [2].

Images means collection of atomic units called pixel, which represents some color value. Images can be thought of as a matrix containing pixel values of each pixel for whole image. Primarily the basic idea behind scrambling of image is to change position of pixels of image through matrix transformation. In this way high quality of confusion is created in image within few evolutions. Scrambling is used to create a non-intelligible image which prevents human or computer vision system from recognizing the true content. First image is scrambled or we can say encrypted i.e. distortion is created then it is descrambled to get back actual image by using descrambling algorithm. Only authorized person is capable of descrambling the scrambled image as only he/she will be given all possible keys used while scrambling the image. Many scrambling techniques such as Rubik's Cubic Algorithm, Arnold Transform, Using Sudoku Puzzle, R-Prime Shuffle Technique, Logistic Map Sequence, etc.

II. LITERATURE REVIEW

According to this paper, the original image is isolated into a random number of blocks that are rearranged inside the image. The altered images then sustained to the double encryption process that is initially considered Blowfish encryption and furthermore considers OFP based Signcryption algorithm for medical image security process. This optimization is held to advance the private and public key of the sender, receiver procedure of encryption security. After the decryption procedure, ultimately the yield image is contrasted and the first image for assessing their execution by utilizing the PSNR. This strategy goes for improving the security level of the encrypted images with better PSNR. In proposed framework is more secure than the current framework with twofold encryption, the proposed work won't uncover any plain medical image details in the database. Here the plain image I and two-bit public and private keys like K1, K2 and encoded the image in light of double encryption system. Resulting to choose the certainty data the confirmation strategy will be used to encode the data, now starting stage blowfish encryption technique misused after second stage methodology the scrambled data over again work to OFP based signcryption strategy [1].

According to this paper, an equation has been considered for sequence generation and based on the sequence, scrambling is performed. This sequence can be generated based on two keys as inputs these keys are very sensitive to even minor changes and they give drastic changes to the output. There is a range for the keys and the range should not be exceeded, else correct results cannot be obtained. There are several parameters for the evaluation of the algorithm, in this paper three parameters have been considered for the estimation of the performance they are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM). Through this algorithm scrambling and descrambling of images can be obtained. This algorithm is very secure as the keys are very sensitive, so only if the keys are known exactly with the same precision descrambling can be obtained, the drawback with this algorithm is that the time consumption of this algorithm is more and further enhancement is necessary to reduce the time complexity [2].

According to this paper, Digital image scrambling is one of the most prominent techniques used for secure transmission of digital images. This can be done in many ways. Basically, there are two ways of image cipher First, by changing the location of a pixel and second, by changing the intensity value of a pixel. One of the most common methods employed is the Arnold Transform. Basically it is a chaotic mapping used to change the pixel location of the original image. It has a periodicity T and the original image can be reconstructed by T number of iterations. In this paper an equation has been considered for sequence generation and based on sequence scrambling is performed. The proposed method is involves both pixel value and location based. This sequence can be generated based on two input keys and these keys are very sensitive to even minor changes and produce drastic changes in the output. There is a three parameters have been considered for the estimation of the performance they are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index Metric (SSIM), PSNR is found to be infinite. The computation time taken for the proposed algorithm for cameraman image is 161.487sec and that for Arnold is 22.23sec. The delay is due to the number of iterations taken for the algorithm to converge and Arnold Cat method valid for square images only whereas proposed method works with any size of the image but takes long time to process. It is mainly due to large key space occupied by the proposed algorithm [3].

According to this paper, there are different approaches of image scrambling which will be discussed later in this section. The evaluation of scrambling degree states the security level of the algorithm. Greater the scrambling degree higher the security of encrypted image. Subjective evaluation of scrambling (i.e. using Human Visual System (HVS)) is uncertain. Objective evaluation of a scrambling algorithm can be done through unchanged pixel positions, entropy, correlation etc. There are 2 main approaches of image scrambling: 1. Pixel position based scrambling 2. Pixel value based Scrambling. In first approach, depending on the scrambling key, pixel positions of the original image are mapped to scrambled image. In this approach, as pixel values are not touched pixel distribution remains same as the original image. In second approach, pixel values are changed according to the scrambling key to get scrambled image. As this approach scramble the image data by transforming pixel values, pixel distribution of scrambled image is not same as original image. Therefore by objective evaluation, second approach is more secure as compared to first but at the cost of chance of losing image data. To get highly secure image scrambling algorithm one can effectively combine both approaches. In this paper new scrambling algorithm is introduced which uses Non-commutative wavelet transform and Poker shuffling algorithm. For image scrambling, low frequency (LF) coefficients of Non-commutative wavelet are scrambled using Poker shuffling algorithm and high frequency (HF) coefficients kept unchanged. To get final scrambled image, Inverse Non-commutative wavelet transform is applied on the scrambled-LF and HF coefficients. Logistic map require least time compared to other methods. But because it modifies the pixel value for getting scrambled image we can’t use this method with Non-commutative wavelet in proposed methodology, as it will make wavelet transformation irreversible. Though timing requirement for Poker Shuffle Transformation is more as compared to other scrambling methods, by using same scrambling sequence for both LF component and reducing no. of iterations we can reduce overall timing requirement of proposed method [4].

According to this paper, Cryptography means to encrypt and decrypt data; data is changed into some other unreadable form, and then the encrypted data is transferred to receiver. Two levels of security is employed in this paper, first one is 2D cellular automata and another one is Arnold Cat Map transformation. 2D Cellular automata is an interesting and capable way of solving problems associated with Arnold Cat Map as it doesn’t possess periodic nature and can work upon rectangular images too. Experimental study reveals that scrambling parameters like GDD (Gray difference and Degree) is better in case of combination of 2D cellular automata (Moore Neighborhood) with ACM; while Correlation Coefficient are better in case of combination of 2D Cellular automata (Von Neumann) with Arnold transform. 2D Cellular automata is an interesting and capable way of solving problems associated with Arnold Cat Map as it doesn’t possess periodic nature and can work upon rectangular images too. They proved by experimental study that combine 2D Cellular automata with ACM not only overcomes above problem associated with Arnold transform but performs better scrambling effect as compare to 2D CA alone. Scrambling parameters like GDD (Gray difference and Degree) is better in case of combination of 2D cellular automata (Moore Neighborhood) with ACM; while Correlation Coefficient are better in case of combination of 2D Cellular automata (Von Neumann) with Arnold transform. Proposed system perform row wise scrambling only not column wise. For make a batter chaos to scramble not only row wise but column wise too [5].

According to this paper, a novel image encryption scheme has been proposed using pixel level scrambling, bit-level scrambling, and DNA encoding. First, initial conditions of five dimensional hyper-chaotic system are computed and chaotic sequences are generated. Then, pixel-level scrambling and bit-level scrambling are implemented to permute the plain image. Permuted image and generated pseudorandom sequence are executed decomposition operations in order to enhance security. DNA encoding, DNA XOR operation, and DNA complementary rules are also adopted to improve the security of the cryptosystem. Experiments results and theoretical analysis show that the proposed scheme is secure enough and can resist known plain text attack, statistical attacks, and differential attacks. It is suitable for practical application [6].

According to this paper, The rotation processes are used to divide the original image into six sub-image, each image attached to the one faces of the Rubik’s cube then divide each sub-image into a number of blocks ex. 3 pixels by 3 pixels blocks that are then scrambled the blocks image into original image through rotate the rows and the columns within each sub-image based a rotation table. The security measurements of the original images have highly correlated elements. This means there is a good relationship between the elements of the original images, which also have a low entropy value and a large standard deviation. The correlation between the image elements is significantly decreased and the entropy value is significantly increased by using the proposed techniques (rotation technique). The proposed technique showed that an inverse relationship exists between number of blocks and correlation, while there is a direct relationship between number of blocks and entropy. The proposed algorithm is expected to show good performance, low correlation and high entropy [7].

According to this paper, various image encryption algorithms based on the permutation–diffusion architecture have been proposed where, however, permutation and diffusion are considered as two separate stages, both requiring image-scanning to obtain pixel values. If these two stages are combined, the duplicated scanning effort can be reduced and the encryption can be accelerated. In this paper, a fast image encryption algorithm with combined permutation and diffusion is proposed. First, the image is partitioned into blocks of pixels. Then, spatiotemporal chaos is employed to shuffle the blocks and, at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudorandom numbers from spatiotemporal chaos is suggested, which further increases the encryption speed [8].

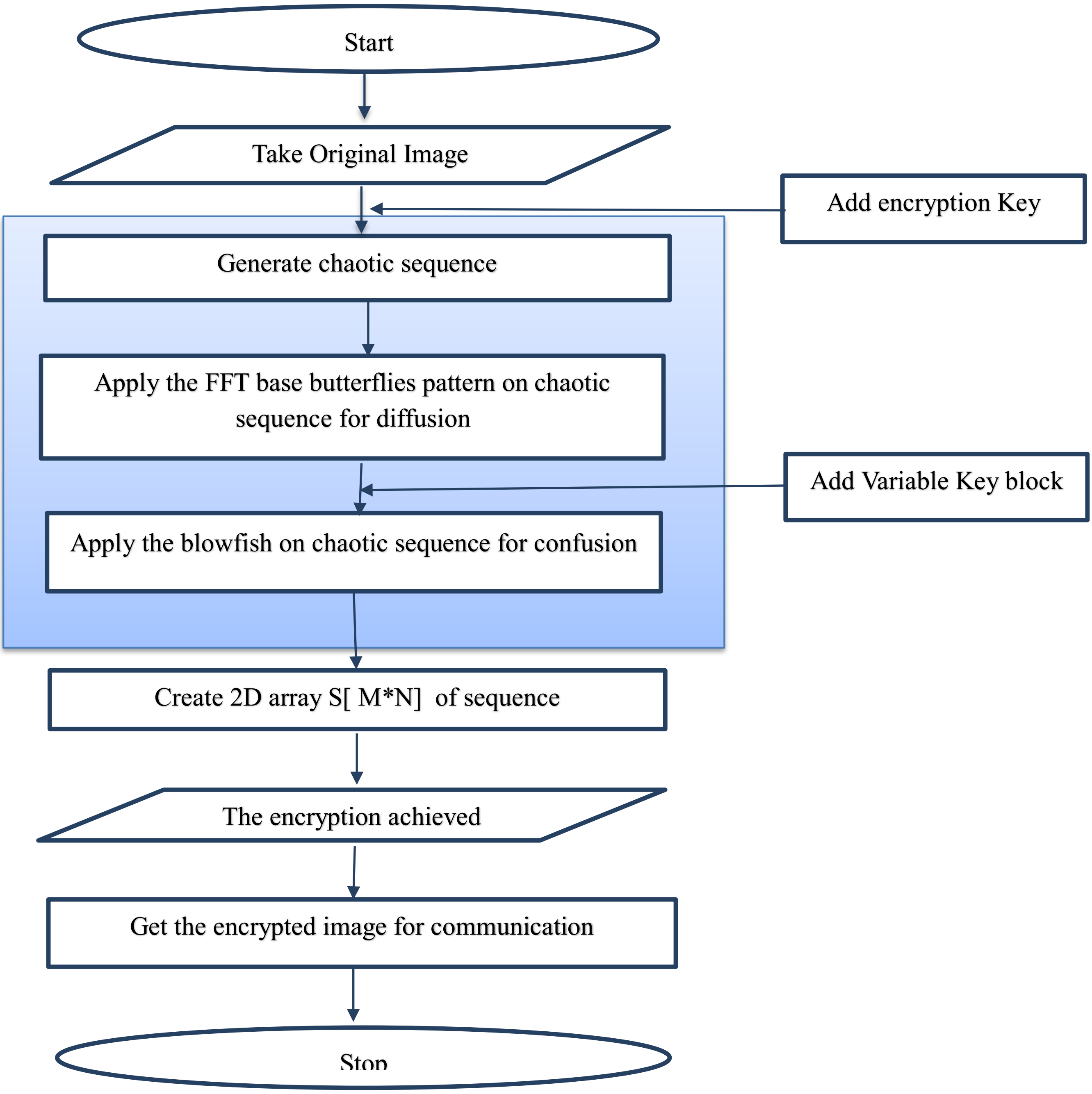
Table 1: Table of Literature Survey

No.	Paper Tittle	Methods	Publication	Summary
1	Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm [1].	Blowfish encryption algorithm. Signcryption algorithm	IEEE, 2018	*.Dual encryption procedure * The confidentiality of the image is upheld in the long run and reclaimed image is offered the unique image.
2	Digital image scrambling based on sequence generation [2].	Sequence generation	IEEE, 2017	*By using the scrambling we can protect the image at some level. * key is very sensitive * Change only pixel position.
3	Image scrambling methods for digital image encryption [3].	non-commutative wavelet transform and poker shuffle transform	IEEE, 2016	* Get highly secure image scrambling algorithm. * Not modify the pixel value for scramble image.
4	Comparative analysis of image scrambling sequence generation method with Arnold [4].	Arnold Transform Sequence generation	IEEE, 2017	* That is take long time for execution. * Periodic nature. * Only for square image.
5	Two Level Encryption of Grey Scale Image through 2D Cellular automation [5].	Gray Difference Degree (GDD)	IEEE, 2017.	* It doesn't possess periodic nature and can work upon rectangular images too. * Only row wise scrambling apply. * Fellow neighborhood approach
6	A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling [6].	Pixel level scrambling. Bit-level scrambling	IEEE, 2018.	* Resist differential attack. Brute-force attack, statistical attack and plaintext attack. * Switching row and column.
7	A New Image Scrambling Technique using Block Rotation Algorithm based on [8].	Block Rotation Algorithm	OJBAS, 2013	* Correlation between image element has been decreased and higher entropy has been achieved
8	A new chaos-based fast image encryption algorithm [9].	Pseudorandom sequence generated from spatiotemporal chaos	ELSEVIER, 2011	* Spatiotemporal chaos is employed to shuffle the blocks and, at the same time, to change the pixel values.

III. PROPOSED APPROCH

In this system, we are going to implement three layer of security for image scrambling. Proposed system follow both approach of scrambling one is changing the location of pixel and another is change the value of pixel. Here we are going to apply the FFT context butterflies operation on chaotic sequence for diffusion and changing the location of pixel and apply the symmetric key encryption algorithm blowfish on chaotic sequence for confusion. After that create a new 2D image pixel array of output chaotic sequence which is scrambled image. Anyone cannot get original without perform reverse step with key

3.1 Proposed Flowchart


Start
Take Original Image
Add encryption Key
Generate chaotic sequence
Apply the FFT base butterflies pattern on chaotic sequence for diffusion
Add Variable Key block
Apply the blowfish on chaotic sequence for confusion
Create 2D array S[M*N] of sequence
The encryption achieved
Get the encrypted image for communication
Stop

3.2 Proposed Algorithm

```
Step 1 – Start
Step 2 – Take the image, variable length of key block, Scrambling key
Step 3 – Generate a chaotic sequence Sq of length M*N using below equation
         X(n+1) = r Xn (1-Xn)
         Where, value of X0 and r can be used as scrambling key
Step 4 – Apply the butterflies operation on Sq for diffusion
Step 5 – Apply the blowfish on Sq for confusion
Step 5 – Create a 2D array of size M*N of Sq
Step 5 – The encrypted image is achieved
Step 6 – Stop
```

IV. FUTURE WORK

Here after these techniques introduction and understanding, we are encrypt the image applying confusion and diffusion on pixel for archive a high degree of encryption of image. So in future we are going to use both of these techniques for the further implementation.

V. CONCLUSION

As we can see that, new encryption technique use the Chaos based technique for generate an initial level sequence. After generating sequence perform diffusion using butterfly technique. And after diffusion of the sequence perform encryption operation for given sequence. At last generate 2D metric of encrypted sequence and achieve scrambled image. For descrambling reverse process of given step. Proposed techniques is follow pixel position and pixel value base encryption approach to archive a high degree of PSNR and correlation coefficient

REFERENCES

[1] T. Avudaiappan, R. Balasubramanian, S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, K. Shankar, "Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm",Journal of Medical Systems(2018) 42:208,Springer Science+Business Media, LLC, part of Springer Nature, 2018.

[2] Sarma, K. S. K. S., and B. Lavanya. "Digital image scrambling based on sequence generation." Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on. IEEE, 2017.

[3] Shelke, Raviraj, and Shilpa Metkar. "Image scrambling methods for digital image encryption." Signal and Information Processing (IConSIP), International Conference on. IEEE, 2016.

[4] Lavanya, B., and M. Kiran Kumar. "Comparative analysis of image scrambling sequence generation method with Arnold." Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of. Vol. 1. IEEE, 2017.

[5] Bhardwaj, Rupali, and Deepali Bhagat. "Two Level Encryption of Grey Scale Image through 2D Cellular Automata." Procedia Computer Science 125 (2018): 855-861.

[6] Sun, Shuliang. "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling." IEEE Photonics Journal 10.2 (2018): 1-14.

[7] Abugharsa, Ahmed & Samad Bin, Abd & Almangush, hamida. (2014). A New Image Scrambling Technique using Block Rotation Algorithm based on Rubik's Cube. Australian Journal of Basic and Applied Sciences, 7(14) December 2013, page: 97-108.

[8] Wang, Yong, Kwok-Wo Wong, Xiaofeng Liao, and Guanrong Chen. "A new chaos-based fast image encryption algorithm." Applied soft computing 11, no. 1 (2011): 514-522.

[9] Li, Min, Ting Liang, and Yu-jie He. "Arnold transform based image scrambling method." 3rd International Conference on Multimedia Technology. 2013.

[10] Pakshwar, Rinki, Vijay Kumar Trivedi, and Vineet Richhariya. "A survey on different image encryption and decryption techniques." International journal of computer science and information technologies 4.1 (2013): 113-116.

[11] Prarthana Madan Modak, Dr. Vijaykumar Pawar, "A Comprehensive Survey on Image Scrambling Techniques", International Journal of Science and Research (IJSR), https://www.ijsr.net/archive/v4i12/NOV152034.pdf, Volume 4 Issue 12, December 2015, 813 – 818

[12] Shang, Zhenwei, Honge Ren, and Jian Zhang. "A block location scrambling algorithm of digital image based on Arnold transformation." Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. IEEE, 2008.

[13] Hsu, Chao-Yung, Chun-Shien Lu, and Soo-Chang Pei. "Image feature extraction in encrypted domain with privacy-preserving SIFT." IEEE Transactions on Image Processing 21.11 (2012): 4593-4607.

[14] Lakshmi Dadala, V. Venkata, C. H. Satya Naresh, and R. Anil Kumar. "Butterfly Design for RADIX-4K DIF FFT." IJRCCT 3.10 (2014): 1348-1353.

[15] Agrawal, Monika, and Pradeep Mishra. "A modified approach for symmetric key cryptography based on blowfish algorithm." International Journal of Engineering and Advanced Technology (IJEAT) 1.6 (2012): 79-83.

[16] Suresh, Manju, and M. Neema. "Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things." Procedia Technology 25 (2016): 248-255.

[17] Buijs, H., et al. "Implementation of a fast Fourier transform (FFT) for image processing applications." IEEE Transactions on Acoustics, Speech, and Signal Processing 22.6 (1974): 420-424.

[18] NehaKhatri–Valmik, Ms, and V. K. Kshirsagar. "Blowfish Algorithm." IOSR Journal of Computer Engineering 16.2 (1994).

[19] Anitha, T. G., and S. Ramachandran. "Novel algorithms for 2-D FFT and its inverse for image compression." Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on. IEEE, 2013.