IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-11, Nov 2019 E-ISSN: 2347-2693

Image Encryption Using Image Division and Suffling Technique

Abhishek Kumar Saw[1*], Yogesh Kumar Rathore[2]

[1,2]Raipur Institute of Technology, Raipur (CG), India

**Corresponding Author: abhisheksaw7890@yahoo.com*

DOI: https://doi.org/10.26438/ijcse/v7i11.6467 | Available online at: www.ijcseonline.org

Accepted: 15/Nov/2019, Published: 30/Nov/2019

Abstract- Encryption is the most effective way to achieve data security and converting data to an unrecognizable or encrypted form. Its wide used to secure data sent over wireless networks and the internet. This paper aims at improving the protection and efficiency of image cryptography by employing a highly efficient shuffle based encryption rule and a comparable decryption rule supported random values obtained by using pseudo random number generator .In this paper, a image encryption is projected which has pixels shuffling image division technique. The planned algorithmic program has been examined using multiple analysis ways in and a PSNR value obtained is more than 35 in all cases which shows a good decryption.

Keywords**:** Transposition, Error free encryption, PSNR, Cryptography.

I. INTRODICUTION

Computer has become an important device now days. The most use of computer is to store information and send it from one location to another. The information that is shared should be transferred in a much secured manner. To make secure transmission of information, information is encrypted to unclear format by an unauthorized person. Cryptography is that the science of information security that has become a really essential side of model computing system towards secured data transmission and storage. The exchange of digital information in cryptography leads to completely different algorithm which will be classified into 2 cryptographic mechanism: symmetric key, during which same keys are involve for encrypting and decryption and asymmetric key ,during which different keys are involve for encryption and decryption[1].The rapid progress of mobile phones has created it challenge for the secure usage and transfer of information. It's vital to induce the efficient and quick operational algorithm for encryption. It's a wise call to require that which encryption technique should be used to do quick image encryption for low computing device. Researchers have planned various techniques which can be used for image encryption, most of those techniques works under Advanced encryption standard (AES) and Compression friendly encryption scheme (CFES).

II. LITERATURE SURVEY

Recent analysis trends within the field of image encryption suggests the utilization of chaotic maps in image encryption algorithms S.S. Maniccam and N.G. Bourbakis given an algorithm program that will lossless compression and encryption of binary and gray-scale photos supported scan technology [2]. Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen used vector quantisation for designing higher cryptosystem for images. In vector quantisation (VQ) firstly the images are decomposed into vectors and then consecutive encoded vector by vector [3]. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, HaWmn Lee, and SmJmng Kim projected an algorithmic program that was multilevel type of image encryption using binary part exclusive OR operation and image dividing technique [4]. Guosheng Gu and Guoqiang Han created a brand new extermely optimised image algorithmic program involve permutation and substitution strategies [5].Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal and Hasan Mahmood propose a criterion to analyse the prevailing S-boxes and study their strengths and weaknesses so as to work out their quality in image encryption applications [6]. Ibrahim S I Abuhaiba and Maaly A S Hassan represent a brand new effective technique for image encryption that employs magnitude and section manipulation using Differential Evolution (DE) approach [7]. Sesha Pallavi Indrakanti and P.S.Avadhani introduced an algorithmic program on the premise of random pixel permutation with the motivation to take care of the standard quality of the image [8]. Amitava Nag replacement a new algorithmic program using affine transform and were supported shuffling the image pixels [9]. In recent years, combined with the twin advantage of the DNA molecule and chaotic systems, an image encryption algorithmic program supported DNA molecules and chaotic systems is given. In 2012, Liu et al. projected an image encryption algorithmic program supported DNA encoding and chaotic map [10]. In 2014, [11] Liu et al. projecteed a RGB image encryption algorithmic program supported DNA encoding and chaos map. In 2015,Wang et al. given a image encryption technique supported 2d logistical mapping and DNA operations [12].In 2017, Chai et al. presented an image encryption algorithmic program that is supported chaos combined with DNA operations [13]. Within the same year, we tend to projected a type of digital image encryption technology supported hyper chaos mapping and DNA sequence library arithmetic to understand a scrambling position transformation of image pixels and therefore spread of the pixel values [14]. Authors in [15] conferred similar work on image the Authors in [16] have mentioned the positive consequences of employing a shuffle based mostly technique. The projected algorithmic program design additionally thought about the author in [17] mentioning the downside of using linear congruential generator because the PRNG which has applied statistical determinism due to the mechanical nature of the algorithmic program. Zhang et al. [18] introduced a novel image encryption program by combining 1D and 2D Logistic maps and DNA addition operation. A novel image encryption scheme using DNA sequence operations was conferred in official. [19] and therefore the spatio- temporal chaotic system was used to manufacture the pseudorandom sequences. Recently, Wang et al. [20] projected a brand new image encryption technique supported the mixed linear-nonlinear coupled map lattices (MLNCML). They used the strategy of DNA computing and one-time-pad policy and located out a better security level algorithmic program. Quist-Aphetsi Kester[21], projected the work sets resolute contribute to the overall body of data within the space of cryptography application and by developing a cipher algorithmic program for image encryption of m*n size by shuffling the RGB pixel values Finally, the algorithmic program created it potential for encryption and decryption of the images supported the RGB pixel. Musheer Ahmad and M. Shamsher Alam [22] planned a brand new image encryption algorithm supported 3 totally different chaotic maps. During this work, the plain-image is 1st decomposed into 8x8 size blocks and so the block based mostly shuffling of image is parameters meant for shuffling are randomly generated by using 2D coupled Logistic map.Subsequently the shuffled image is encrypted through chaotic sequence generated by one dimensional Logistic map. generated by one dimensional Logistic map. Varsha Bhatt and Gajendra Singh Chandel[23] planned a brand new algorithmic program that deals with the representative image encryption techniques, position permutation, naive, substitution transposition and value transformation. Selective techniques are represented, assessed and matched up with reference to security level and encryption speed. Hiral Rathod, Mahendra Singh Sisodia et.al[24], introduced a brand new permutation technique supported the mixture of image permutation and developed an encryption algorithmic program called “Hyper Image Encryption Algorithm (HIEA)”. The chosen image are converted into binary value blocks, which can be arrange into a permuted image employing a permutation method, so the generated image are encrypted employing the HIEA algorithmic program. Scrambling techniques in transform-domain and codestream-domain are planned in [25], [26], and [28]. Pseudo-random permutation-based RoI encryption approaches for H.264 videos planned in [27] and [28].

III. METHODOLOGY

A. Encryption Algorithm

Detailed methodology shown in below:

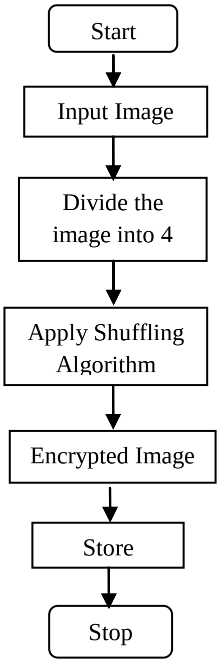

Figure 3.1 flow chart of encryption process

Pseudo Code for Encryption:

Step 1. Start
Step 2. Import data from image and create an image graphics object by interpreting each element in a matrix.
Step 3Convert input image into gray scale image i.
Step 4. Reshape in size of m × n.{ where m is number of row & n is number of column}
Step 5. Divide the image row wise into 4 parts. P1, P2, P3, P4

```
P1 =  i[(1:m/4),:];
P2=  i[(m/4+1:m/2),:];
P3=  i[(m/2+1:3m/4),:];
P4=  i[(3m/4+1:m),:];
```

Step 6.Create new Zero Matrix
X=zeros(m,n);
Step 7.Perform following operation on each part:-Z1=1; Z2=2; Z3=3; Z4=4;

```
for a=1:m/4
   X(Z1,:)=P1(a,:);
   X(Z2,:)=P2(a,:);
   X(Z3,:)=P3(a,:);
   X(Z4,:)=P4(a,:);
   Z1=Z1+4;
   Z2=Z2+4;
   Z3=Z3+4;
   Z4=Z4+4;
end

Step 8.  Store 'X' as Encrypted image.
   Z3=Z3+4;
   Z4=Z4+4;
end
Step 8.  Store 'X' as Encrypted image.
```

B. DECRYPTION ALGORITHM:

The inverse of the algorithm will decrypt the encrypted image back into the plain image.

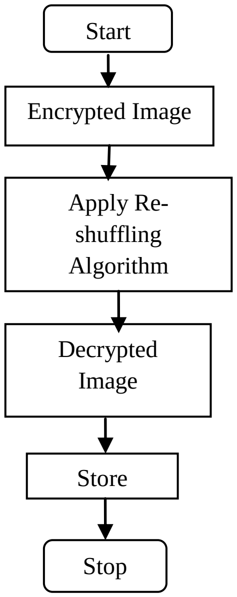

Figure 3.2 Flow chart of decyption Algorithm

Pseudo Code for Decryption:

```
Step 1. Start
Step 2. Import data from Encrypted image (X) and create an image graphics object by interpreting each element in a matrix.
Step 3. Reshape in size of m×n.{where m is number of row & n is number of column}
Step 4. Create 4 new Zero Matrix P1, P2, P3, P4
P1=zeros(m/4,n);
P2=zeros(m/4,n);
P3=zeros(m/4,n);
P4=zeros(m/4,n);
Step 5.Perform following operation on each part:-
Z1=1; Z2=2; Z3=3; Z4=4;
for a=1:m/4
   P1(a,:)=X(Z1,:);
   P2(a,:)=X(Z2,:);
   P3(a,:)=X(Z3,:);
   P4(a,:)=X(Z4,:);
   Z1=Z1+4;
   Z2=Z2+4;
   Z3=Z3+4;
   Z4=Z4+4;
end
Z=[P1;P2;P3;P4];
Step 6.Convert matrix 'Z' to image
Step 7.  Store 'Z' as Decrypted image.
```

IV. RESULT ANALYSIS

Table.1 ENCRYPTION_TRANSPOSITION

Image	Method	Psnr	Nae	Entropy	Ssim	Npcr	Uaci
Girl (I_ENTROPY=7.617)	4	28.2	0.24	7.65	0.11	99.7	33.45
Paper's (I_ENTROPY=7.578)	4	28.0	0.3	7.60	0.03	99.7	33.46

From table 1 we can observe that highest value of PSNR is 28.2 that we got encryption also highest NPCR value 99.7 for the 4 parts image division.

Table.2 DECRYPTION_ TRANSPOSITION

IMAGE	METHOD	PSNR	NAE	ENTROPY	SSIM	NPCR	UACI
Girl.jpg(I_ENTROPY=7.617)	4	35.8	0.02	7.66	0.88	43.6	13.43
Pepper.jpg(I_ENTROPY=7.517)	4	38.2	0.01	7.60	0.91	44.6	13.6

From table 2 we can observe that highest value of PSNR is 38.2 and also lowest NPCR value 43.6 for the 4 parts image division decryption.

Table 1 and table 2 show the experimental results our encryption and decryption techniques respectively. From table 1 we can observed that the PSNR value between input and encrypted image is near about 28 entropy is near about 7.65, which makes it unpredictable. From table 2 we can observed that now PSNR between input and decrypted image is more than 35 which makes it more similar.

V. CONCLUSION

The presented technique provides high security and confidentiality in transmission of image data over networks or storage of the same. The encryption method in our work has been tested on different image formats with best possible seed values and packs immense flexibility due to variable number of parameters that can be used as a deciding factor for the encryption process. The experiments shows that highest PSNR value we got encryption i.e. 28.78 , and highest NPCR value is for 4 part division encryption i.e 99.7. when we consider PSNR then it is also more than 35 for decrypted image which makes it good decryption algorithm. In future diagonal type of division may be applied to increase the accuracy.

REFERENCES

[1]. A.J.Menezes ,P.C.Van Oorschot, and S.Vanstone , "Handbook of Applied cryptography", CRC Press, Boca Ration,Florida, USA,1997.

[2] S. Maniccam and N. G. Bourbakis, "Lossless image compression and encryption using scan," Pattern Recognition, vol. 34, no. 6, pp. 1229–1245, 2001.

[3] C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," Journal of Systems and Software, vol. 58, no. 2, pp. 83–91, 2001.

[4] C.-M. Shin, D.-H. Seo, K.-B. Cho, H.-W. Lee, and S.-J. Kim, "Multilevel image encryption by binary phase xor operations," in Lasers and Electro-Optics, 2003. CLEO/Pacific Rim 2003. The 5th Pacific Rim Conferenceon, vol. 2. IEEE, 2003, pp. 426–vol.

[5] G. Gu and G. Han, "An enhanced chaos based image encryption algorithm," in First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06), vol. 1. IEEE, 2006,pp. 492–495.

[6] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of s-box in image encryption applications based on majority logic criterion," International Journal of Physical Sciences, vol. 6,no. 16, pp. 4110–4127, 2011.

[7] M. A. S. Hassan and I. S. I. Abuhaiba, "Image encryption using differential evolution approach in frequency domain," ar Xiv preprintarXiv:1103.5783, 2011.

[8] S. P. Indrakanti and P. Avadhani, "Permutation based image encryption technique," International Journal of Computer Applications (0975–8887) Volume, 2011.

[9] A. Nag, J. P. Singh, S. Khan, S. Ghosh, S. Biswas, D. Sarkar, and P.P.Sarkar, "Image encryption using affine transform and xor operation," in Signal Processing, Communication, Computing and Networking Technologies (ICSC).

[10] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[11] Y. Liu, J. Tang, and T.Xie, "Cryptanalyzing a RGB image encryption algorithmbased on DNA encoding and chaosmap," *Optics and Laser Technology*, vol. 60, pp. 111–115, 2014.

[12] X.-Y. Wang, Y.-Q. Zhang, and Y.-Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dynamics. An InternationalJournal of Nonlinear Dynamics and Chaos in Engineering Systems*,vol. 82, no. 3, pp. 1269–1280, 2015.

[13] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[14] Y. Niu, X. Zhang, and F. Han, "Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database," *Computational Intelligence and Neuroscience*, vol. 2017, Article ID 4079793, 9 pages, 2017.

[15] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number, "Proceeding of *the IEEE Inter Symposium On Circuits and Systems, Vancouver ,Canada* ,Vol .03 , PP .965-968 , 2004.

[16] Nishith Sinha and Kishore Bhamidipati "Improving Security of Vigenère Cipher by Double Columnar Transposition", International Journal of Computer Applications (0975 – 8887), Volume 100 – No.14, August 2014.

[17] Stallings W. "Pseudorandom Numbers "in Cryptography and Network Security- Principles and Practices, 5th edition.

[18]Zhang, GuoL, WeiXP .Image encryption using DNA addition combining with chaotic maps.MathComputModel2010;52:2028–35.

[19]Wang XY ,Zhang YQ ,Bao XM .A novel chaotic image encryption scheme using DNA sequence operations.OptLasersEng2015;73:53–61.

[20]ZhangYQ,WangXY,LiuJ,ChiZL. An image encryption scheme based on the MLNCML systemusingDNAsequences.OptLasersEng2016;82:95–103.

[21]. Quist-Aphetsi Kester," Image Encryption based on the RGB PIXEL Transposition and Shuffling", International Journal of Computer Network and Information Security, 2013, Vol 7, Pages:43-50.

[22]. Musheer Ahmad, M. Shamsher Alam," A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering,Vol.2(1), 2009, 46-50.

[23].Varsha Bhatt, Gajendra Singh Chandel,"Implementaion of new advance image Encryption Algorithm to enhance the security of Multimedia Component" International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536 Volume 2, Issue 4, July 2012.

[24]. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma,"Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3, ISSN 2249-6343.

[25] F. Dufaux and T. Ebrahimi, ``Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 8, pp. 1168_1174, Aug. 2008.

[26] F. Dufaux and T. Ebrahimi, ``H. 264/AVC video scrambling for privacy protection," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2008,pp. 1688_1691.

[27] P. Carrillo, H. Kalva, and S. Magliveras, ``Compression independent reversible encryption for privacy in video surveillance," *Eurasip J. Inf.Secur.*, vol. 2009, no. 1, pp. 1_13, 2010.

[28] F. Dufaux, ``Video scrambling for privacy protection in video surveillance: Recent results and validation framework," *Proc. SPIE*, vol. 8063, pp. 307_314, May 2011.