Image Encryption Method Using Permutation and Rubik's Cube Principle for Images

Mr. Nilesh Tiwari, *M. Tech., SRIST, Jabalpur*
Prof. Urooz jabeen , *SRIST, Jabalpur*

Abstract: The primary goal of this paper is security management. This will provide authentication of users, and integrity, accuracy and safety of images which is traveling over internet. Moreover, an image-based data requires more effort during encryption and decryption. The Proposed Architecture for encryption and decryption of an image using suitable user defined key is developed with the same objective. In this paper, we introduce a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image we will binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm (HIEA)" algorithm.

KeyWord: **- Encryption, Decryption, Cryptography, Image Encryption.**

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. From the study of research paper and other proposed work have conclude that in [5, 7, and 9] there are no clarifications which type of images they are using to perform image encryption and decryption procedure. Paper work have also analyzed that there is no clarification about the configuration of machine and platform where all the experiment are calculating. Another thing which paper work has measured that proposed transformation table of [2, 3, and 5] have very complex structure and not easy to understand which is the cause of poor efficiency. From further study I have observed that Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data.

The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the Characteristic of human perception, a decrypted image containing small distortion is usually acceptable. After the detailed study of image encryption, we presented some problem which find during study and how we can remove these with the help of our proposed work.

Thus, a recent work for the security of the images data were directed towards the design of new algorithms (for example the algorithms which are based on chaotic signals) which ensure a reliable security and minimize the cost of computing time and the loss of information. However, its disadvantages reside mainly in the need for carrying out calculations with a high degree of accuracy and in the risk to succeed in obtaining the initial key, after several attempts at launching, and so the attack of the cryptosystem becomes easy.

II. PROPOSED WORK

Proposed Architecture: proposed architecture is shown in figure 1.

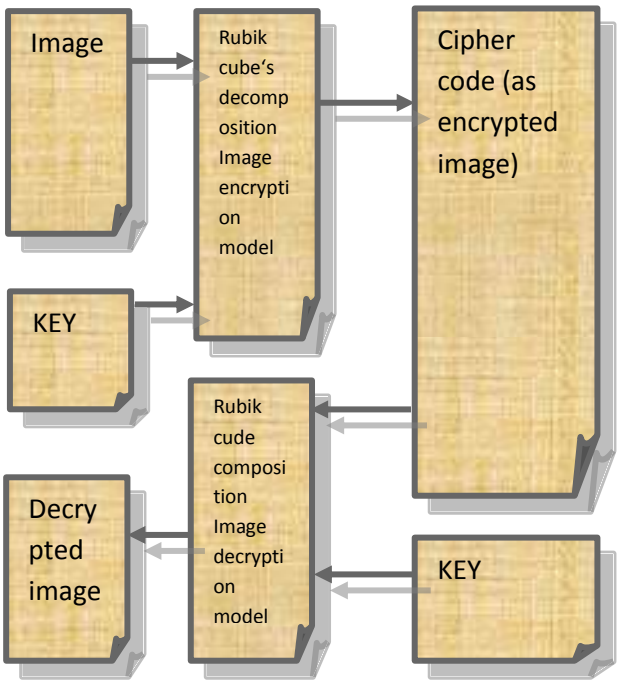


Figure 1: Encryption approach

2.1 Encryption

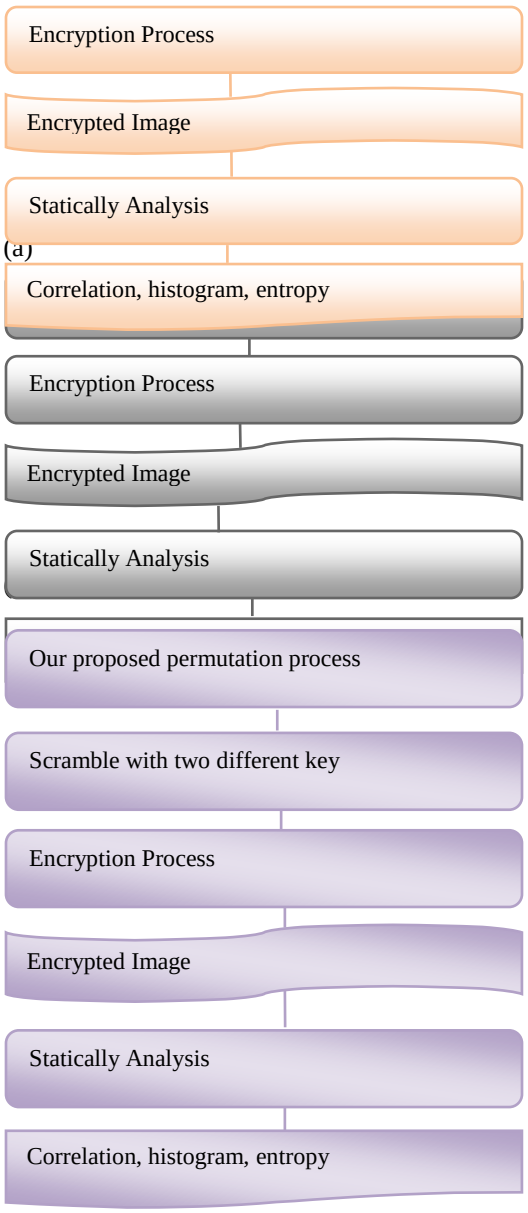
The ciphers the plain-image image while passing by the following stages:

1. To read the plain-image image of NxM pixels;
2. To transform the plain-image into binary values and to store them in X ;
3. N ← the size of X ;
4. for i =1 to N to make ;
5. To generate the key-stream Y(i)
6. for i = 1to N to make
8. C(i) = xor(X(i),Y(i)) ;
9. The binary flow of the cipher-image C is sent.

2.2 Decryption

Deciphers the binary flow of the cipher-image C while passing by the following stages:

1. N ← the size of C ;
2. for i =1 to N to make ;
3. To generate the key-stream Y(i) by using the algorithm 3.2 ;
4. for i =1 to N to make;
5. Z(i) = xor(C(i),Y(i)) ;
6. To put the binary flow of the deciphered image Z in the form of an image of n x m pixels and to store it in imgdech;
7. To post the deciphered image imgdech. Figure 2 is showing comparative study architecture between various algorithm and proposed algorithm.



(c)

Fig-2: (a)-ref[1] work, (b)-ref[2] work , (c)- proposed method flow chart

III-RESULTS

Simulation will be carried out using MATLAB V 7.5. The proposed crypto-data hiding methodology will be tested for different images. However, paper work will have some standard images; will be ciphered with the same key of size 128-bit. After applying our cryptosystem to different images, proposed work is expecting to recover encrypted Rubik cube based image as in original from up-to 98-99%.

Proposed work also plan to resistance our cryptosystem to the noise by adding to the cipher-images a noise for testing our cryptosystem to the sensibility to the keys, for example, we cipher an image with the secret key bits and, we decipher it with different key; after all this the corresponding

correlation coefficient between plain-images and cipher-images will be measured for comparing proposed work with other work.

IV. CONCLUSION

In this Work, a new algorithm based encryption scheme for image data is been introduced; simulations will be carried out for different images. In addition, this method is very simple to implement, the encryption and decryption of an image. The proposed algorithm can to resists the additive noises. In this paper, an efficient image encryption algorithm based on blocks permutation and Rubik's cube principle is proposed in order to enhance the security of chaotic systems against replay attacks, which may occur in different points as stated. The proposed algorithm starts by first partitioning the image into blocks of size *MxM* which are then randomly permuted using a secret key. Then, for each block and using a second key, rows and columns are right or left circular shifted. After that, the XOR operator is applied to the shifted rows and columns to produce the encrypted image.

REFERENCES

[1] Ratha, N.K., J.H. Connell and R.M. Bolle, 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3): 614-634.

[2] Fingerprint Verification Competition, "FVC-2000," http://bias.csr.unibo.it, Nov. 2012.

[3] Jain, A.K., R. Bolle and S. Pankanti, 2005. Biometrics: Personal Identification in Networked Society. Kluwer Academic Press.

[4] Wu, C., 2007. Advanced feature extraction algorithms for automatic fingerprint recognition systems. Ph.D. thesis, University Of New York at Buffalo.

[5] Ratha, N.K., H.H. Connell and R.M. Bolle, 2001. An Analysis of Minutiae Matching Strength. In Proceedings of The 3rd International Conference on Audio and Video Based Biometric Person, 2091: 223-228.

[6] Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, 2003. Handbook of Fingerprint Recognition. Springer, New York.

[7] Uludag, U., S. Pankanti, S. Prabhakar and A.K. Jain, 2004. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE, 92(6): 948-960.

[8] Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A Secure Image Encryption Algorithm Based on Rubik's Cube Principle. Journal of Electrical and Computer Engineering, 13.

[9] Han, F., J. Hu, X. Yu and Y. Wang, 2007. Fingerprint images encryption via multi-scroll chaotic attractors. Applied Mathematics and Computation, 185(2): 931-939.

[10] Khan, M.K. and J. Zhang, 2007. An Intelligent Fingerprint-Biometric Image Scrambling Scheme, 1141-1151.

[11] Alghamdi, A.S. and H. Ullah, 2010. A Secure Iris Image Encryption Technique Using Bio-Chaotic Algorithm. International Journal of Computer and Network Security, 2(2): 78-84.

