An Experimental Study with Two Level Image Encoding Algorithm

[1]Amit Joshi, [2]Dr S K Sharma and [3]Dr Sanjay Gour
[1, 2] Department of Computer Science & Engineering, Pacific University, Udaipur
[3]Department of Computer Science & Engineering JECRC, Jaipur
Email: [1]amitjoshiudr@gmail.com, [2]sanjay.since@gmail.com

Abstract: *Data security in the private cloud is one of the major concerns for the present time. Lots of techniques are available in the vicinity of the same. Advancements in the data security are continuous but advancements sometimes create complexity also. So always there is need of advanced but easy to understand technology. To improve the previously mention effort there is requirements to expand the work. The proposed work is used for the audio and video file also except text file and Image file. The proposed work implemented with a dual side synchronized process of data communications, here two level RBBLES algorithm has been applied to encode gray scale image..*

Key Words: *Security, Encryption, Decryption, algorithm, communication.*

1. INTRODUCTION:

To enhance the previously mentioned work in the area of the data security and image processing there is need to extend the work in the all facet. It is obvious that data security in the private cloud is one of the key issues for the user in present. Plenty of methods are exists in the surrounding area of the same. Always there is need of advanced but easy to understand technology. The proposed work is used for the audio and video file especially including text and Image file. So there is big challenge to implement the security process the extended form. Again the implementations with video file need more efforts to done it in efficient manner because video means a huge series of the image sets. .

2. Assumption for study (Hypothesis)

The assumption for the study is designed in the form in which one can use best encryption and decryption techniques to secure the data in the private cloud. The assumption can be dividing into five major sections. Each section is able to represent the steps and procedures of the encryption and decryptions process. Each and every steps or section tries to ensure the policy of secrecy safe and secure in the favor of data security. The accompanying suspicions have been mulled over:

- The algorithm would utilize 25 move keys from 1 to 25. Each move key would move the characters as indicated by its esteem.
- All the letter sets have been kept in one gathering and all numbers and uncommon characters (aside from accentuations) have been kept in another gathering. The information bunches have been appeared in Table.
- In instance of letters in order we can move them to 25 areas as indicated by 25 move keys. Essentially numbers and extraordinary characters can likewise be moved to 25 areas in same way. The courses of action of the 26 letter sets and 10 numbers and extraordinary characters are assembled together according to the necessities of the proposed algorithm.
- Encryption and decoding both processes will dependably be from starting to the last.
- A clear space between the message words partitions the message into various squares. Each square is dealt with distinctively and another move key is produced for each square.

3. Two Level Image encoding scheme using RBBLES Algorithm

The proposed work will now implemented with a dual side synchronized process of data communications. In this proposed work, two level RBBLES (Swamp Computing,2012) algorithm has been applied to encode gray scale image.

- Text Encoding / Encryption: In the cases of text encoding, single level RBBLES algorithm is enough to encode values. The algorithm can alter each single character in the text. It is noted that the text having no visual information.
- Image Encoding / Encryption: Where as in the cases of image, changes the pixel value leads to distortion of visual information which needs to be retain. In this proposed encoding scheme two levels of RBBLES algorithm is deployed with two different keys. One key is predefined and another key is shared key (required during data sending).

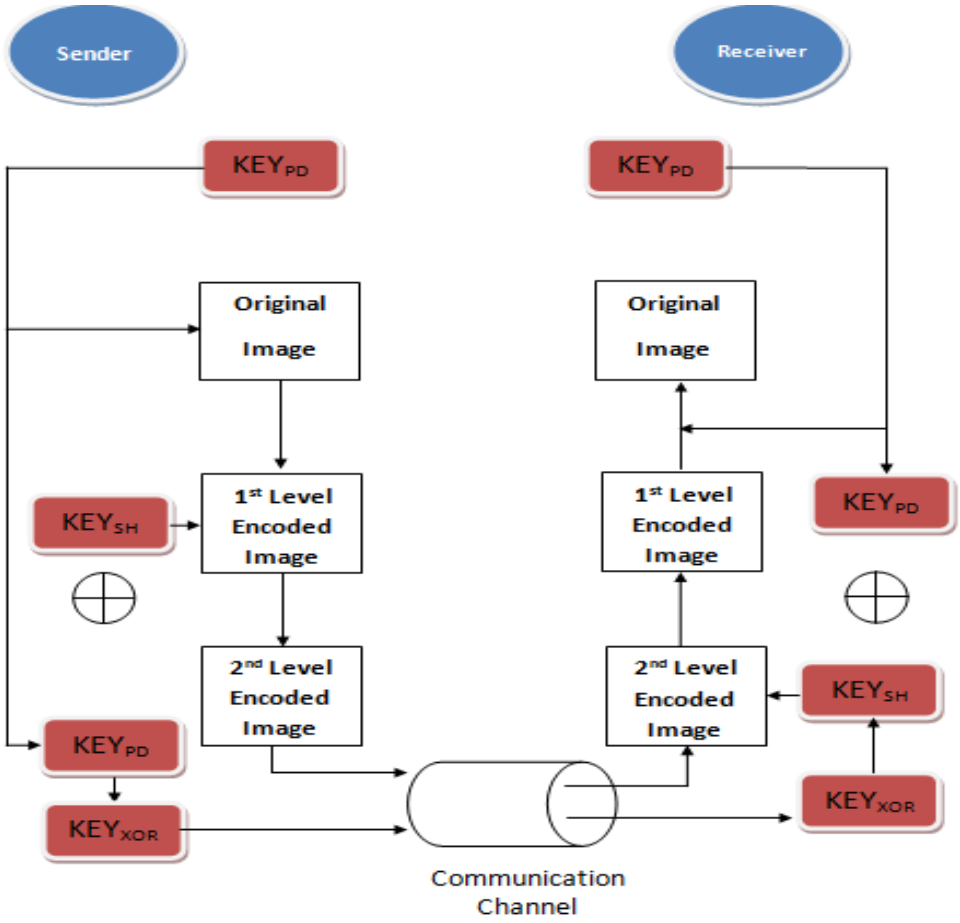


Figure-1: Two Level Image encoding scheme using RBBLES Algorithm

Pre defined (KEY_{PD}) and shared key (KEY_{SH}) both are of 4 bits. To provide extra security, KEY_{SH} is not needed to send directly to the receiver rather result of bit wise XOR operation between KEY_{PD} and KEY_{SH} that is KEY_{XOR} which needs to is sent to the receiver along with the encoded image.

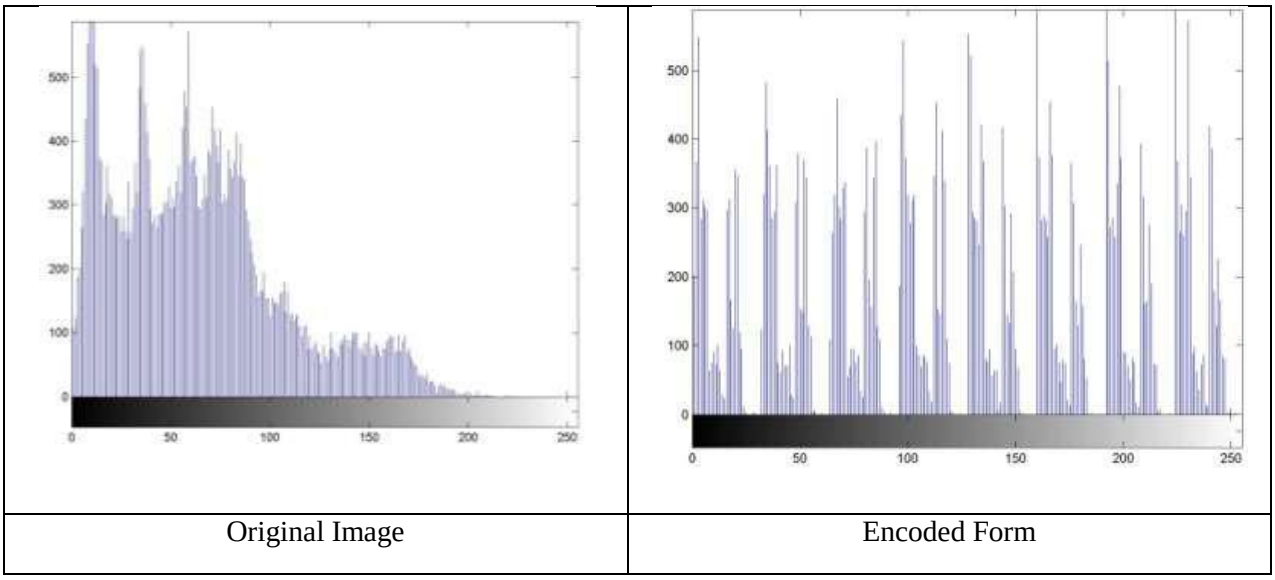
Receiver side will perform the XOR operation between KEY_{PD} and KEY_{XOR} to recover the KEY_{SH} .Now receiver has both the key that is KEY_{PD} and KEY_{SH} for decoding.

4. Experimental with MATLAB:

To examine the result which obtained from the experimental according to algorithm proposed here in the study. We are taking some standard images and apply the algorithm and received the details of changes by the help of MAT Lab tools / software support.

Image 1 (Original Image and its Transformation in Encoded From)

	
Original Image	Encoded Form



Original Image	Encoded Form

Image 1 : (Histogram of the Original and encoded Image)

5. Comparison with Existing Algorithms:

Table provides the comparison of the proposed algorithm with the existing algorithms and also provides key size and block used for effectively implementing the algorithm.

Algorithm	Plain Text	Cipher Text	Key size	Number of Rounds	Encoding of secret key	Advantages
DES Algorithm	64 Bits	64 Bits	56 Bits	16 Rounds	Encoded with message and passed.	1. Less number of Computations. 2. Simple and Fast. 3. Cryptanalysis is difficult.
3 DES Algorithm	64 Bits	64 Bits	168 Bits	48 DES Rounds	Encoded with message and passed.	1. More Reliable. 2. Longer key length. 3. Cryptanalysis is difficult.
AES Algorithm	128 Bits	128 Bits	128/192/ 256 Bits	10/12/14 Rounds respectively.	Encoded with message and passed.	1. Reliable. 2. Longer key length supported.
Blow fish Algorithm	64 Bits	64 Bits	32-448 Bits	16 Rounds.	Encoded with message and passed.	1. Fast and secure. 2. Compact.
RC 5 Algorithm	32/64/ 128 Bits	32/64/128 Bits	0-2040 Bits	Variable.	Encoded with message and passed.	1. Simple and fast. 2. Data dependent rotations. 3. Adaptable to processors of different word length.
RSA Algorithm	Minimum 512 Bits	Minimum 512 Bits	512-1024 Bits	Variable	Different keys for encoding and decoding.	1. Offering high-performance. 2. Delivering broad platform support.
Proposed Randomized Algorithm	128 Bits	128 Bits	48/36 Bits	Variable	Randomly Generated at both ends	1. Random generation of secret key. 2. No requirements of passing and encoding the key. 3. Less number of Computations.

Table 1: Comparison from other algorithm

6. CONCLUSION:

On comparing with the existing algorithm it is being found that the secret key size is minimum for the randomize algorithm so a lesser time is consumed in order to encrypt a message with the algorithm and decreasing reliability is managed by randomly generation of key on both the ends. So the method given in the study is acceptable for the implementation of further action.

REFERENCES:

1. Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010.
2. Mohammad ShahnawazNasir, Prakash Kuppuswamy "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm "International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.
3. Preeti poonia and Praveen Kantha, " Comparative Study of Various Substitution and Transposition Encryption Techniques", International Journal of Computer Applications (0975 – 8887) Volume 145 – No.10, July 2016
4. Satish Kumar Garg" Modified Encryption and Decryption Using Symmetric Keys at Two Stages: Algorithm SKG 1.2" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 6, June 2014 ISSN: 2277 128X.
5. Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile ComputingIJCSMC, Vol. 4, Issue. 8, August 2015.
6. Senthil, K., K. Prasanthi, and R. Rajaram . "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research(ICCIC), 2013 IEEE International Conference on. IEEE,2013.
7. SomdipDey "An Integrated Symmetric Key Cryptographic Method Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm" I.J.Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.
8. William Stallings "Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.