ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

RSS Blowfish Block Encryption Technique for Secure Image Cryptography

Amandeep Kaur[1], Gurjeet Singh[2]

Student, Electronics and Communication, Amritsar College of Engineering and Technology, Amritsar, Punajb, India[1]

Assistant Professor, Electronics and Communication, Amritsar College of Engineering and Technology, Amritsar, Punjab, India[2]

Abstract: In the modern world, the requirement for information security has become a necessity with the progress in the exchange of data and communications through the electronic system. Due to multimedia growth the image security while transmission is major issue various complex cryptography technique are used for image security. The technique is proposed for image encryption and decryption with random selective selection and Blowfish algorithm the technique select refine part and encrypt decrypt block .the encryption and decryption time of proposed technique is better and Encryption and decryption results calculated by proposed technique is better as compared standard methods

Keywords: Cryptography, RSA, RSS Blowfish

I. INTRODUCTION

Image encryption is noted recently that the use of computer networks is developing rapidly throughout the world; the maximum data is transferred through the Internet. The data is transferred in diverse formats i.e. Pictures, audio, and other multimedia. But the pictures were broadly used in our lives. This concept ends with the mainly comprehensively used image we use, and more security will be needed. Real data be supposed to be specified to the real person in real time, and that is what data was sent must be exactly the data was received. Security image has turn into a foremost concern in the digital environment. The fundamental things that security must achieve are: the reliability and privacy (CIA). As given within Fig 1, Data protection is an essential cause. Sent on public networks or information sent must have trustworthy safety with encryption process. Watermark information must be included into such an approach that this should not be detectable and removable even after many false or benign attempts [1]

There are numerous ways that coding can shield images. The picture is encrypted and decrypted therefore it can be accessed Use also ensures that the image reaches its target without any change. Evaluation of the Protocol on encryption and decryption rules for image transfer [2]

A. Methods of Encryption

The algorithm for distribution and getting are the foremost method that must involve. The encryption algorithm is derived in two steps; they are encryption and decryption [3]. The key elements in the encryption process are keys and algorithms. Algorithms are defined as complex formulas that state the rules of how the plain text encryption of the text keys is probably the random bit strings that are used by algorithms. Decoding and encryption. The keys are used by the data sending person is caller secret keys. Sender and received use these secret keys. If two users would like to exchange data using secret key encryption, they be required to obtain a duplicate of the identical key. If someone wants to communicate with another, it needs three separate keys, one for each person. It's probably effortless, but if you desire to exchange data with hundreds[3] How to transfer the accurate key to the succeeding individual in a secure approach. It is not safe to send the key by mail or email to get it to the user, because the key will not be confined and can be intercepted and easily used by potential attackers can provide secret symmetric keys, But cannot run, since there is no approach to show by the encryption that has already sent a message if two people apply the identical key.[3]

B. Asymmetric Key Encryption

The Algorithm with identical key is also recognized as asymmetric key algorithm. Identical key encryption was first displayed publicly, describing the two primary keys that the parties can securely communicate on an unsecured communication channel not including secret key. They have developed a problem of spreading secret keys using two keys as an alternative of a only key. Public key, which can be recognized by each one, and a private key, which must stay not to be disclosed and only known by the holder

DOI 10.17148/IJARCCE.2018.7911

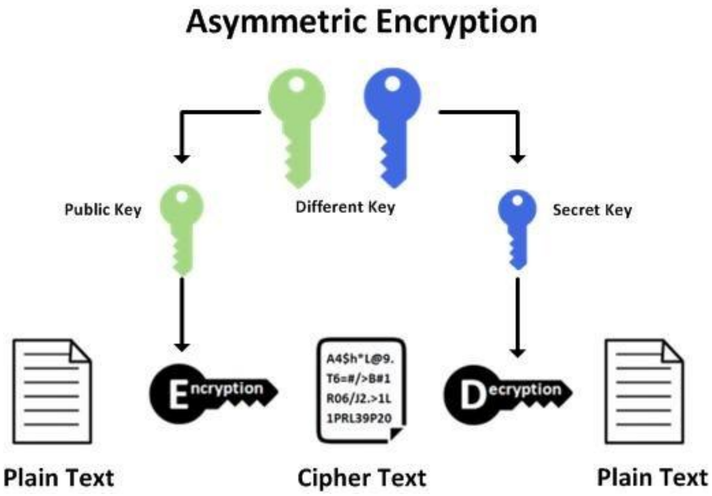

Fig1 Asymmetric Key Encryption

C. Symmetric Key Encryption

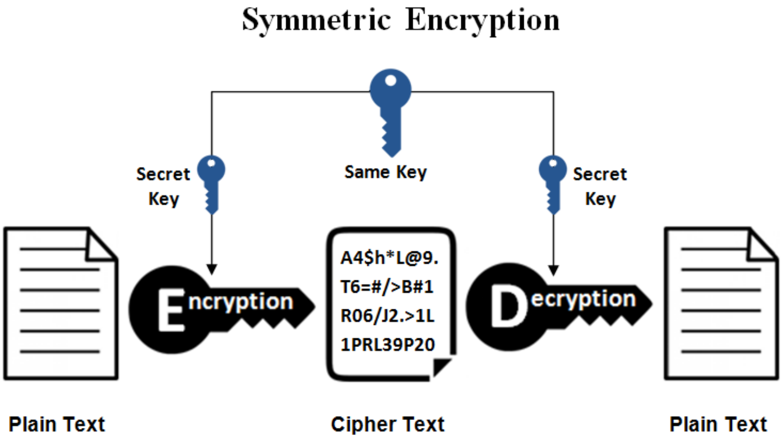

Fig2 symmetric Key Encryption

The same key is used by sender and receiver in symmetric Cryptography

D. Image Security Parameters

In general, excellent encryption technology qualifies collection of safety standards and some of them are as

A. Large Key Space: An enormous key space is necessary for various attacks for better results

B. Key Sensitive: It confirms that the arrangement will generate a absolutely inverse result, despite the change in the key [6]. Therefore, encryption expertise must be key-sensitive.

C. Uniform Histogram: The regularity allocation specification is generated by histogram for persistent pixels and density evaluation .Thus, the image code must be a unified graph to be protected from the known attack plain text [4, 5].

II. PROPOSED METHOD

This work mainly focuses on enhancing encryption process with Random selective block encryption and Blowfish Algorithm

A. **Random Selective Block Encryption:** This new algorithm proposed for Random selective block encryption is the code block. The records are divided into set of Pixels of identical length. Some pixel blocks are selected and just the selected pixel sets are encrypted the symmetric key technique is used in this algorithm for Encoding and decoding are used by the identical key in both parts. Random the randomly selected region of image is taken for compression of image .the selected refined region is further process for reducing PSNR,MSER while with encryption and decryption process. Since selective area is taking so better result will be performed

DOI 10.17148/IJARCCE.2018.7911

I. Blowfish Algorithm

Blowfish decryption: The bloated fish algorithm is one of the symmetric block encryption algorithms that are conceived as a quick alternative to the existing RSA algorithms, the Blow fish algorithm consist of two part a key-expansion part and a data-encryption part: the main part of the attachment and the data encryption part. It encrypts the data by using the Block encryption method, which divides the text into 64-bit blocks before it is encrypted. It consist of changeable length key starting 32 bits to 448 bits in length, which means the flexibility of the security force image encryption using algorithm-based transformation algorithm block the new transformation to be used by the conversion before encryption, where the innovative image is separated into a random number of blocks that are mixed the arrangement of processing and encryption techniques is used to expand the protection level of encrypted images.

Blowfish is a symmetric block encryption algorithm

a. Blowfish uses 32 bit processor for encrypting data using 26 hours per clock per byte
b. Blowfish require memory not as much of 5 k
c. With 32-bit operand blowfish algorithm uses lookup table, OR and addition

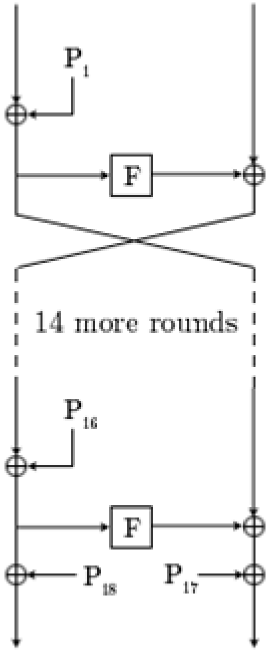

Fig3 Feistel structure of Blowfish

II. Description Blowfish Algorithm

The 64-bit data is encrypted by blowfish algorithm by using feistel network .algorithm functions in two parts

a) Key-Expansion: The Blowfish converts the 448 key bits to a string of 4168 -byte sub-Key set. The large sub keys are generated by blowfish for encryption and decryption for any data. With 18,32- bit subkey of p-array

Four 32 boxes having 256 entries

P1, P2, P3, P4………….P18

S1,0, S1,1,………. S1,255
S2,0, S2,1,……….. S2,255
S3,0, S3,1,……….. S3,255
S4,0, S4,1,………... S4,255

a) Sub key Generation:
Step1: start with P-array and then the four S-boxes
Step2: XOR P1, XOR P2 with first, second 32-bits of the key correspondingly, iterate unless P-array has been XORed with key bit
Step3: apply Blowfish algorithm, for all zero encryption by the sub keys from steps (1) and (2).

Step4: Array P1 and P2 are exchanged with the step (3) results.
Step5: use customized subkeys Encrypt (3) results with Blowfish algorithm
Step6: finally replace P3 and P4 with step (5) results.

b) Data Encryption: Blowfish follow Feistel system With 16 rounds and 64 bit data elements, x[11]

Algorithm

```
Divide x into two 32-bit halves: $x_L$, $x_R$
For i = 1to 16:
$xL = X_L$ XOR $P_i$
$xR = F(X_L)$ XOR $x_R$
Swap $X_L$ and $x_R$
Swap $X_L$ and $x_R$ (Undo the last swap.)
$x_R = x_R$ XOR $P_{17}$
$x_L = x_L$ XOR $P_{18}$
Recombine $x_L$ and $x_R$
```

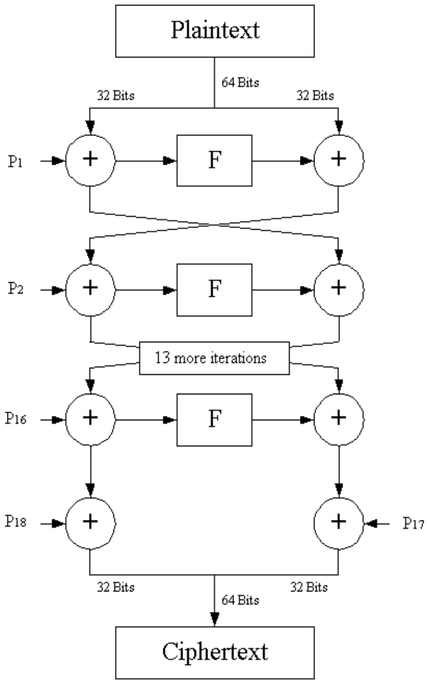

Fig4 Blowfish Encryption [11]

III. SIMULATION RESULTS

1. Encryption Time: the proposed technique work faster as it work on refined random selective selection and it perform faster encryption The below Fig1 and table1 shows the time taken to encrypt images with proposed technique RSS Blowfish and previous technique RSA AlGamal the result show that execution time taken by proposed technique is less as compared to previous technique. The proposed technique perform better as compared to previous technique

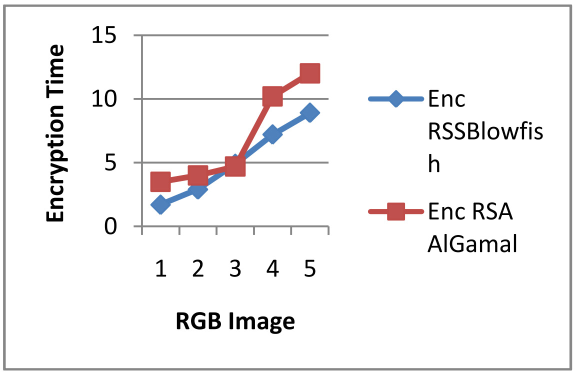

Fig5Encryption time Comparision

Rgb Image	Enc RSS Blowfish	Enc RSA AlGamal
1	1.7	3.5
2	2.9	4
3	4.9	4.7
4	7.2	10.2
5	8.9	12

Table 1Encryption time Comparision Table

2. Decryption Time: the proposed technique work faster as it work on refined random selective selection and it perform faster Decryption faster and it is difficult to decrypt images by intruders while transmission The below Fig2 and table12 shows the time taken to Decrypt images with proposed technique RSSBlowfish and previous technique RSA AlGamal the result show that execution time taken by proposed technique is less as compared to previous technique. The proposed technique perform better as compared to previous technique in decryption process

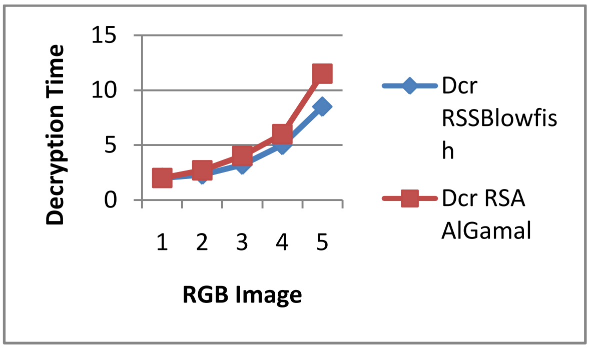

Fig6Decryption time Comparision

Rgb Image	Dcr RSS Blowfish	DCR RSA Algamal
1	2	2
2	2.3	2.7
3	3.2	4
4	5	6
5	8.5	11.5

Tabel12Decryption time Comparision Table

Peak Signal Noise ratio: The peak signal ratio for various images with proposed and previous technique are calculated the results values shown in fig3 and table 3 shows that result produced by proposed technique for PSNR after encryption and decryption are better as compared to previous technique which shows proposed technique is much favorable as compared to previous technique while securing images

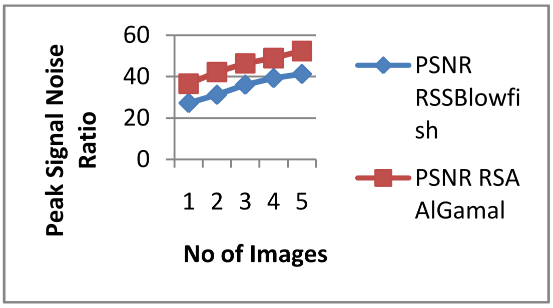

Fig7 PSNR time Comparision

Rgb Image	PSNR RSS Blowfish	PSNR RSA AlGamal
1	27.1	36.5
2	31.1	42.2
3	36	46.3

4	39.2	48.9
5	41.2	52.3

Table3 PSNR time Comparision

CONCLUSION

In the modern world, the requirement for information security has become a necessity with the progress in the exchange of data and communications through the electronic system. Due to multimedia growth the image security while transmission is major issue various complex cryptography technique are used for image security. **.** The selective random blocks are generated which are encrypted .the proposed work faster and better as compared to previous technique because encryption on part of blocked image relevant to entire image is easier .the proposed technique show better result

REFERENCES

[1]. Renuka.S.Mathapati and Jagadeesh.Pujari, “Digital Video Watermarking”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, ISSN: 2277 128X,pp.1-8, 2012 .

[2]. S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan,” Image Scrambling Algorithm Based on Random Shuffling Strategy”3rd IEEE Conference on Industrial Electronics and Applications, 2008,pp. 2278 – 2283.

[3]. Bai Ying Lei, I.Y.Soon and Zhen Li, “Blind and robust audio watermarking scheme based on SVD-DCT”, Signal Processing, vol. 91, 1973-1984, 2011

[4]. Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya” A Survey On Different Image Encryption and Decryption Techniques.” International Journal of Computer Science and Information Technologies, Vol. 4, pp.113-116 , February. 2013.

[5]. Xu Shujiang Wang Yinglong, Guo Yucui Wang Cong,“A Novel Chaos-based Image Encryption Scheme”,International Conference on Information Engineering and Computer Science (ICIECS) 2009, 19-20, pp: 1- 4, Dec. 2009

[6]. Ritu Gupta, Pulkit Mundra, Shikha Karwal and Abhilasha Singh, “DWT-SVD Based Watermarking Scheme of JPEG Images Using Elliptic Curve Cryptography”, Department of Information Technology, 2016.

[7]. J.J. Amador, R. W.Green “Symmetric-Key Block Cipher for Image and Text Cryptography”: International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[8]. Praloy Shankar De, Prasenjit Maiti,” DEDD Symmetric-Key Cryptosystem”, International Journal of Advanced Computer Research (IJACR),Volume-3 Number-1 Issue-8 March-2013.

[9]. Dr. Alaa Kadhim, Rand Mahmoud Mohamed, Visual Cryptography For Image Depend on RSA & AlGamal Algorithms, International Conference on Multidisciplinary in IT and Communication Science, 2016.

[10]. H. Gilbert, M. Minier, “A collision attack on 7 rounds of Rijndael”, In The third Advanced Encryption Standard Candidate Conference, pages 230– 241, NIST, April 2000.