IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM

Mrs. Smita Desai[1], Chetan A. Mudholkar[2], Rohan Khade[3], Prashant Chilwant[4]

[12,3,4]*Department of Electronics, Padmashree Dr.D.Y.Patil Institute of Engineering and Technology Pimpri Savitribai Phule Pune University, Pune, (India)*

ABSTRACT

With the progress in data exchange by electronic system, the need of information security has become a necessity. Due to growth of multimedia application, security becomes an important issue of communication and storage of images. This paper is about encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. The proposed algorithm is designed and realized using Visual basic.

Keywords: Block Cipher, Cryptography, Feistel Network, Image Decryption, Image Encryption

I. INTRODUCTION

Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement. Many image content encryption algorithms have been proposed such as DES, 3DES, blowfish, AES, etc. Blowfish algorithm is highly secured because it has longer key length (more no of key size). The main aim behind the design of this proposal is to get the best security/performance tradeoff over existing ciphers. To achieve this result we are going to compare different parameters such as processing time, bandwidth, correlation, entropy etc of above mentioned algorithms.

II. LITERATURE SURVEY

After the survey of various methods used for image encryption we came through a few of these like Image encryption using AES, DES,

2.1 DES algorithm using Transportation Cryptography Techniques

Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now a days the advancement in the computational power the DES seems to be weak against the brute force attacks. To improve the security of DES algorithm the transposition technique is added before the DES algorithm to perform its process. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm.

2.2 Image Encryption Using Block-Based Transformation Algorithm

Here a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish is used. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique.

III. BLOCK DIAGRAM

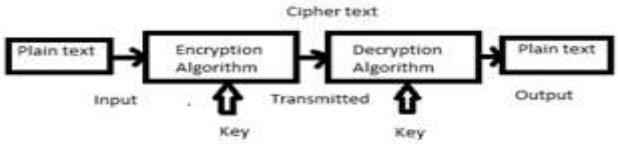


Fig: Encryption/Decryption Process

IV. BLOWFISH ALGORITHM

- Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms.
- Blowfish is a symmetric block encryption algorithm designed in consideration with

✓ Fast: it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte
✓ Compact: it can run in less than 5K of memory
✓ Simple: it uses addition, XOR, lookup table with 32-bit operands
✓ Secure: the key length is variable, it can be in the range of 32~448 bits: default 128 bits key length
✓ It is suitable for applications where the key does not change often, like communication link or an automatic file encrypter.
✓ Unpatented and royalty-free.

*Symmetric algorithms: use the same key for encryption and decryption

*Feistel Network is the fundamental principle that is based on splitting up the block of N bits in two halves, each of size N/2(N must be even).

V. DESCRIPTION OF ALGORITHM

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follow the Feistel network and this algorithm is divided into two parts.

i. Key-expansion: It will converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes

ii. Data-Encryption: It is having a function to iterate 16 times of network. Each round consists of a key-dependent permutation, and a key- and data- dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

5.1 Key Generation

- Blowfish uses large number of sub keys. These keys are generating earlier to any data encryption or decryption.
- The p-array consists of 18, 32-bit sub keys: P1,P2,……,P18
- Four 32-bit S-Boxes consists of 256 entries each:

  S1,0, S1,1,……. S1,255

  S2,0, S2,1,…….. S2,255

  S3,0, S3,1,…….. S3,255

  S4,0, S4,1,……... S4,255

5.2 Steps to Generate Sub Keys

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3).

2) XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; For example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

VI. BLOCK DIAGRAM OF DATA ENCRYPTION

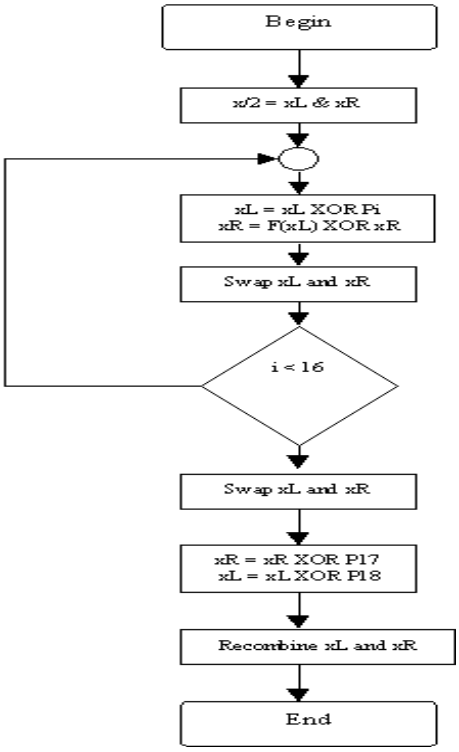
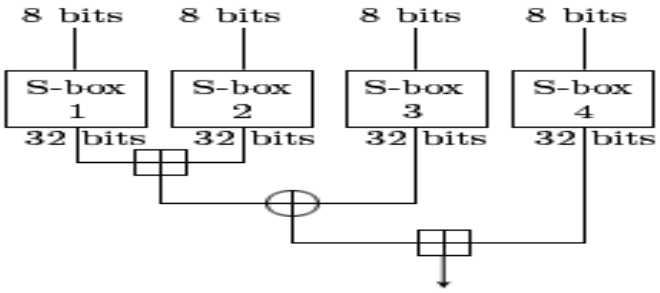


Fig. Block Diagram of Data Encryption

VII. FUNCTION F



Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, x.

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}

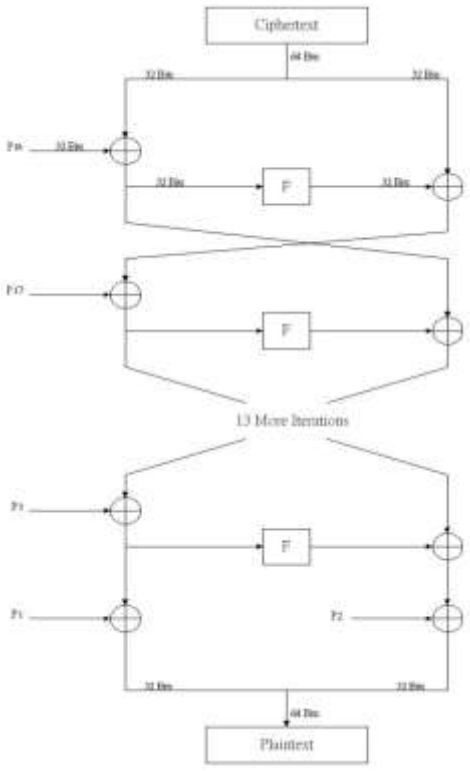
$x_L = x_L$ XOR P_{18}

Recombine x_L and x_R

VIII. BLOCK DIAGRAM OF DATA DECRYPTION

Decryption is exactly the same as encryption, except that P1, P2 ..... P18 are used in the reverse order.

F = ((S1[a] + S2[b] mod 2^{32}) XOR S3[c]) + S[d] mod 2^{32}



IX. SIMULATION AND RESULT

In this paper we have simulated the image processing part of Encryption and decryption in Visual Basic software. Here we would be taking an image & obtaining the matrix and pixels of the chosen image & then we would be encrypting the image matrix using blowfish algorithm. The result shows the original image, encrypted image and the decrypted image. The text in the image will be hidden using a specific key and image hidden with a data is encrypted and decrypted by a 32 bit iteration loop.

ALOGRITHM	CREATED BY	KEY SIZE(BITS)	BLOCK SIZE(BITS)
DES	IBM IN 1975	56	64
3DES	IBM IN 1978	112 OR 168	64
RIJNDAEL	JOAN DAEMEN & VINCENT RIJMEN IN 1998	256	128
BLOWFISH	BRUCE SCHNEIER IN 1993	32-448	64

Fig. Comparison of Algorithms on the Basis of Block Size

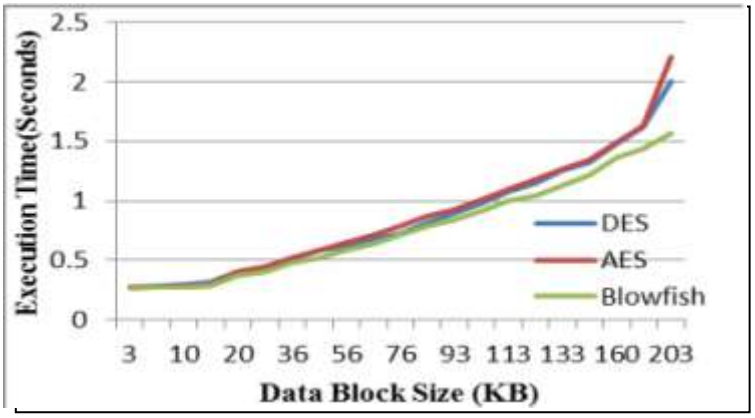


Fig. Comparison of Execution Time

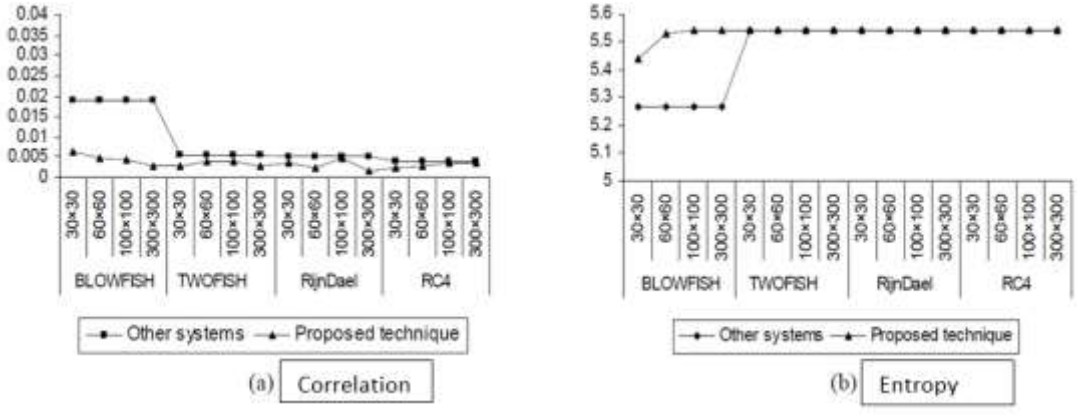


Fig. Correlation & Entropy

X. CONCLUSION

In this paper we have used the blowfish algorithm for encrypting an image for secure transmission over the internet. To achieve this result to be true, we are comparing different parameters such as processing time, bandwidth, correlation, entropy etc of above mentioned algorithms with the other algorithms such as AES, DES, RijnDael. Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of

rounds. Hence if the number of rounds are been increased then the blowfish algorithm becomes stronger. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm. It takes much less time for processing than any other encryption techniques. Also all types of image sizes & format can be encrypted (.jpg, .bmp). By using this algorithm, lower correlation & higher entropy can also be achieved.

REFERENCES

[1] Network Security and Cryptography, Bernard Menezes, IIT Bombay, Powai Mumbai.

[2] Sombir Singh , Sunil K. Maakar, Dr.Sudesh Kumar, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[3] DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering.

[4] Mohammad Ali Bani Younes and Aman Jantan ,Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[5] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[6] P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications', IEEE Transactions on Consumer Electronics, voI.46,no.3,pp.395-403, Aug.2000.

[7] Ketu File white papers, “Symmetric vs Asymmetric Encryption”, a division of Midwest Research Corporation.

[8] Tingyuan Nie and Teng Zhang,“ A Study of DES and Blowfish Encryption Algorithm”, IEEE, 2009

[9] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004.

[10] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229-234.