IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB

Pia Singh
Prof. Karamjeet Singh

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 MATLAB.

KEYWORDS: Cryptography, Image encryption, Decryption, Blowfish, Block Cipher.

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. The field of encryption is becoming very important in the present era. 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.
Many image content encryption algorithms have been proposed. 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.

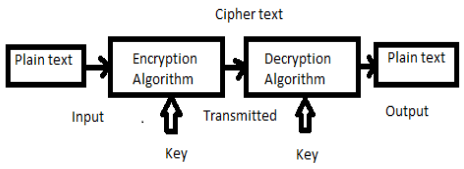

Fig: Encryption/Decryption Process.

So in this paper we are implementing blowfish algorithm which is strongest and fastest in data processing/storing compare to other algorithms. Blowfish algorithm is highly secured because it has longer key length (more no of key size). The philosophy of proposal algorithm is to use the full menu of "Strong operations" supported in modern computers to achieve better security properties and provide high speed. The main aim behind the design of this proposal is to get the best security/performance tradeoff over existing Web Images.

II. BACKGROUND

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Encryption is the process of transforming the information for its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. The security of images has become more and more important due to the rapid evolution of the internet in the world today. The security of images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there

is no single encryption algorithm satisfies the different image types.

In 1993, Bruce Schneier published the Blowfish block cipher. At this time, the current Data Encryption Standard (DES) was known to be vulnerable to crypto analysis and brute-force attacks. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date, the security of Blowfish has not been compromised. Blowfish Algorithm is a **Feistel Network**, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

Blowfish is a symmetric block cipher that encrypts data in 8- byte (64-bit) blocks. The algorithm has two parts, key expansion and data encryption. Key expansion consists of generating the initial contents of one array (the P-array), namely, eighteen 32-bit sub keys, and four arrays (the S boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish can have a key that ranges from 32 to 448-bits. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a cipher based on Feistel rounds. No attack is known to be successful against this. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one.

III. EXISTING TECHNIQUES

There are many image encryption algorithms which are available such as Baker's Transformation,in this Baker's map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc. But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

DATA ENCRYPTION STANDARD (DES):

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

TRIPLE DES (TDES):

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. TDES uses three round message This provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is thatcit is too time consuming.

ADVANCED ENCRYPTION STANDARD (AES):

AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds.

BLOWFISH:

Bruce Schneier designed blowfish in 1993 as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors.

IV. PROPOSED TECHNIQUE

In 1993, Bruce Schneier[1993] published the Blowfish block cipher. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date, the

security of Blowfish has not been compromised. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

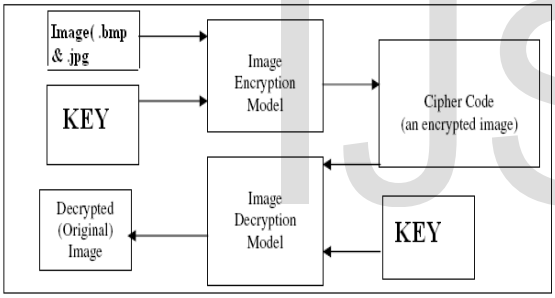

FIGURE:PROPOSED ARCHITECTURE

Encryption Process:

Data image as a plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the blocks length of Blowfish algorithm.

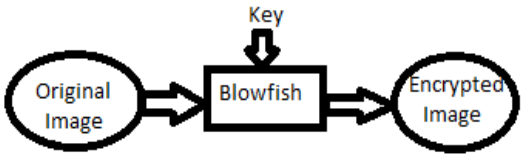

FIGURE: IMAGE ENCRYPTION

Image header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in row order from left to right with each row representing one scan line of the image and the rows of the image are encrypted from top to bottom.

Decryption Process:

The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom.

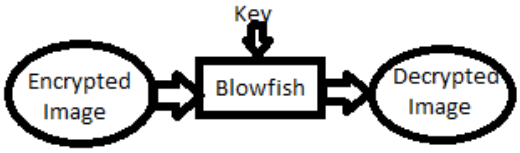

FIGURE: IMAGE DECRYPTION

The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

The basic algorithm for Blowfish is illustrated as follows:

Divide X into two 32-bit halves XL and XR
For i=1 to 16:
XL = XL Pi
XR = F (XL) XR
Swap XL and XR
End for
Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.

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

TABLE: COMPARISON OF VARIOUS DIFFERENT ALGORITHMS

V. SIMULATION AND RESULT

In this paper we have simulated the image processing part of Encryption and decryption in MATLAB software. Here we would be taking an image. Firstly we would be 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 and display in MATLAB. We will clearly see that the decrypted image is same as the original image.

FIGURE: Display window in MATLAB

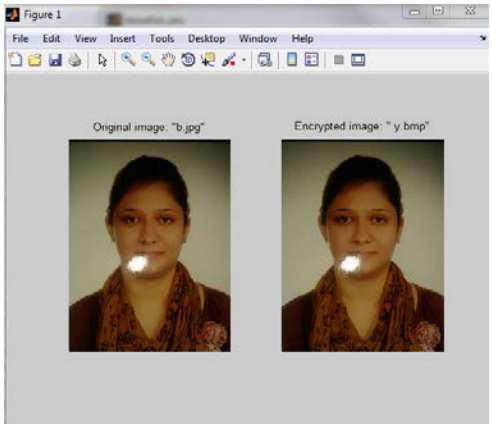

FIGURE: Original image is encrypted and message is hidden.

Display Panel of Output that consist the 16 iterations loop, OR, XOR Commands and the algorithm code with a key that Encryptes and Decryptes the image that consists of an hidden text.

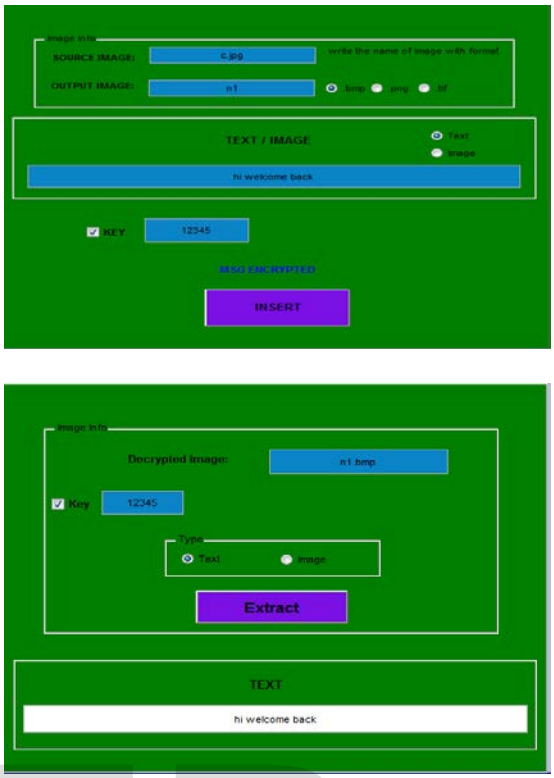

FIGURE: Input and Output window of MATLAB.

VI. CONCLUSION

Both colour and black & white image of any size saved in tagged image file format (TIF), Bit map (bmp), Portable network graphics (PNG), Joint Photographic Experts group (jpg), ect. can be encrypted & decrypted using blowfish algorithm. Histogram of encrypted image is less dynamic and significantly different from the respective histograms of the original image. 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.

VII. REFERENCES

1. Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology*, ISSN: 2231-280, July to Aug Issue 2011.

2. Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

3. Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http:// www. schneier.com/ blowfish.html.

4. W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," *Pakistan Journal of* Information *and Technology*. Vol. 2.

5. H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.

6. C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.

7. M. Ali BaniYounes and A. Jantan, 2008,Image encryption using block-based transformation algorithm,in IAENG International Journal of Computer Science, Volume 35, Issue 1.

8. Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).

9. Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).

10. Li. Shujun, X. Zheng "Cryptanalysis of a chaotic imagevencryption method," Inst. of Image Process. Xi'anvJiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002.

11. 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.

12. Ketu File white papers, "Symmetric vs Asymmetric Encryption", a division of Midwest Research Corporation.

13. Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009

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

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