A Symmetrical key Cryptography Analysis using Blowfish Algorithm

Priya Thakur[1]
PG Student
Department of Computer Science & Engineering
Arni University, Indora (H.P), India

Anurag Rana[2]
Assistant Professor
Department of Computer Science & Engineering
Arni University, Indora (H.P), India

Abstract: **Due to the growth of multimedia applications, the need of information security has been become a necessity in this modern technology. The encryption and decryption is used to securely transmit data in open network. The encryption will hide the information that is not visible to anyone using a key. The different techniques should be used to protect confident image data from unauthorized access. This paper is about encryption and decryption of image using a symmetric key called as 64 bit blowfish is designed in the MATLAB software. This proposed algorithm will increase the security and improve performance by reduces the encryption and decryption time. This algorithm uses a variable key of size 448 byte that provide more reliable and secure than any other algorithm. In this, four S-boxes lookup, multiplication as well as fixed and data dependent rotation will be used.**

Keywords: Cryptography, Symmetrical Key, Blowfish Algorithm Encryption And Decryption Etc.

I. INTRODUCTION:

Providing security and protecting data has become a very difficult task in this world. Every organization today must have different policies regarding data security .In order to provide security, certain algorithms and tools should be implemented. 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 and decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc [2]. Cryptography plays a very vital role in keeping the message safe when the data is transmitted. Most of it was used during wars to send messages in hidden format [1]. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end. Cryptography converts the original message in to non-readable format and sends the message over an insecure channel. The people who are unauthorized to read the message try to break the non-readable message but it is hard to do it so. The authorized person has the capability to convert the non-readable message to readable one [3]. The information is not only text, but also audio image and other multimedia images have been widely used in our daily life. The digital images are commonly used are represented in 2-D array. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary [12]. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products [9]. Encryption and decryption of images using a secret –key block cipher called 64- bits blowfish which is an evolutionary improvement over DES, 3DES etc designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs the Feistel network which iterates simple function 16 times [4]. Specifically; in this algorithm, a combination of four S- boxes lookups, multiplications as well as fixed and data dependent rotations will be used. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

II. CRYPTOGRAPHY:

Cryptography is the technique to convert the message, which is called Plain text, into coded message ,known as encrypt text, from sender and transmit it to receiver that converts (decrypt) the message into readable format (Plain text) after receiving it to avoid the message from getting stolen, damaged or lost and in order to protect it. The figure 1 given below describes the simple encryption and decryption process in the cryptography. In this, the sender will provide plain text at the sender side and with the help of algorithm this plain text will be converted into the chipper text. This process is called as encryption. Then the message is transmitted to the receiver side where the person at the receiver side will collect the chipper text and converted into the original message with the decryption process. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key"[12]. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially

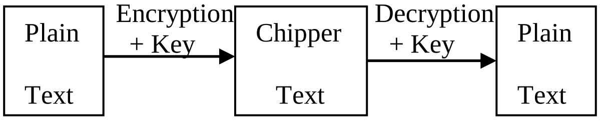


Figure1: Encryption and Decryption process in Cryptograph

broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. There are various types of cryptography algorithm depending on the key used in the cryptography. Cryptography is divided in two types first is symmetric key cryptography (sender and receiver shares the same key) and the second one is asymmetric key cryptography (sender and receiver shares different key) [6]. Symmetric systems contain Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) and Blowfish algorithm use an identical key for the sender and receiver. Symmetric key cryptography is also called as secret key and Asymmetric key cryptography is called as public key cryptography [5].

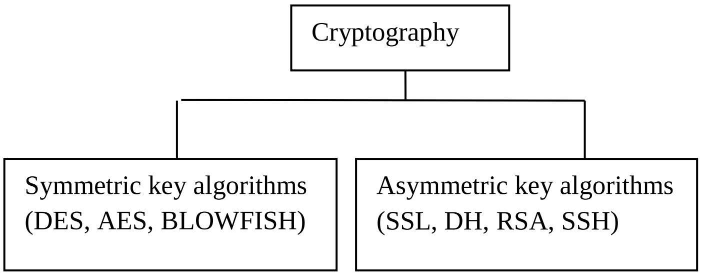

Cryptography
Symmetric key algorithms (DES, AES, BLOWFISH)
Asymmetric key algorithms (SSL, DH, RSA, SSH)

Figure 2: Types of Cryptography Techniques and their algorithms

Symmetric key ciphers are implemented as either block ciphers or stream ciphers [7]. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. Asymmetric key algorithms, the sender and the receiver both use different keys for encryption and decryption purposes. Asymmetric key used are SSL, DH, RSA and SSH algorithms.

III. BLOWFISH ALGORITHM:

Blowfish is a symmetric-key block cipher and included in a large number of cipher suites and encryption products. This algorithm is a 64-bit block cipher technique where a message is divided into multiple blocks of data which has fixed length. It uses same secret key of variable length for both encryption as well as decryption of the messages [8]. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. It is very popular in cryptographic software because it is available to everyone. It is the fastest encryption algorithm with the speed of 26 clock cycles per byte and secure due to variable length secret keys [9].Blowfish uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak keys problem [4].The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes [11]. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key-expansion and data-dependent substitution. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round Feistal network [10].

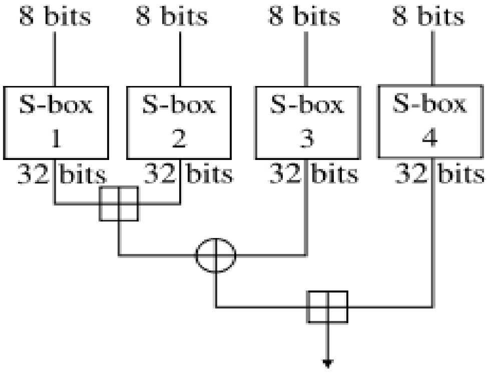


Figure 3: Round function (Feistel function) of Blowfish [9]

All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Each line represent 32 bits. There are five sub-key-arrays: one 18-entry P-array to avoid confusion with the Plaintext and four 256-entry S-boxes (S0, S1, S2 and S3).Every round *r* consists of 4 actions: First, XOR the left half (L) of the data with the rth P-array entry. Second, use the XORed data as input for Blowfish's F-function, Third, XOR the F-function's output with the right half (R) of the data, and last, swap L and R. The F-function splits the 32-bit input into four eight- -bit quarters, and uses the quarters as input to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output [13]. After the 16th round, undo the last swap, and XOR L with K18 and R with K17 (output whitening). Decryption is exactly the same as encryption, except that P1, P2..... P18 are used in the reverse order. This is not so obvious because XOR is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm. The advantages of the blowfish algorithms are that it has been accepted as one of the strong encryption techniques. It is patent as well as royalty free. It can be used by any user.

IV. RESULTS:

In this paper we have simulated the image processing part of Encryption and decryption in MATLAB software. This method of encryption can be applied to any of the formats of images like jpg, tif, ppm, pgm, png from the browser option. We are using the JPEG image format in this work. The size of using images is different every time.

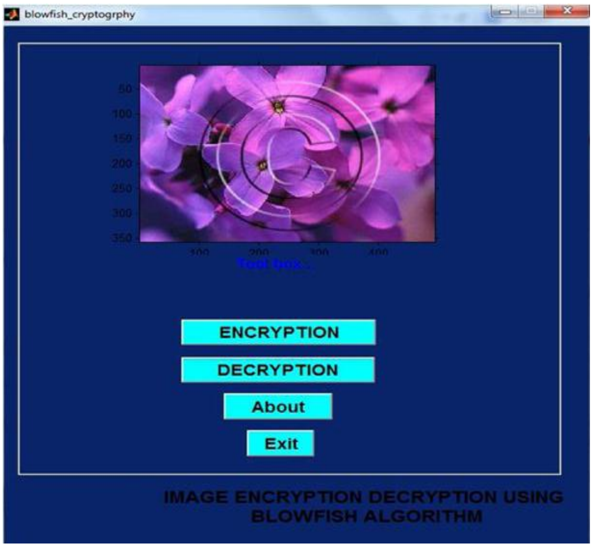
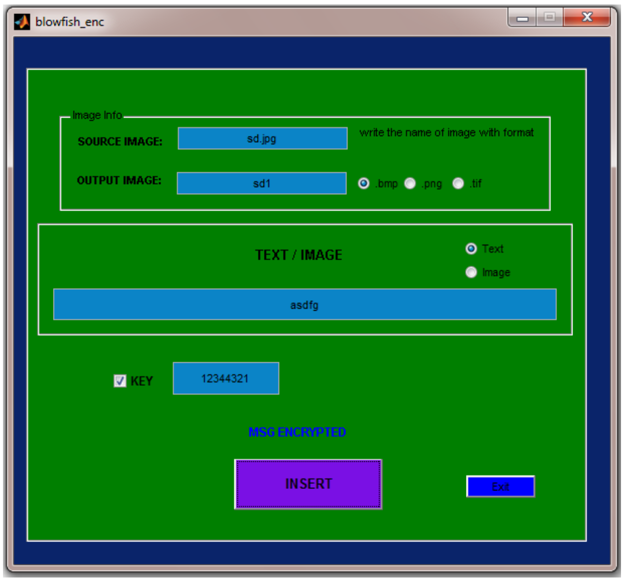


Figure 4: image encryption decryption using blowfish algorithm

The original image is converted into any image format. JPEG is an international image compression standard and has been widely applied to image compression. Since JPEG requires 64 element quantization table for encoding/decoding, our scheme can be applied to jpeg. The figure 4 shows the basic image encryption and decryption using blowfish algorithm. Here we would be taking an image of format .jpeg in this paper because the .jpeg has high resolution and better results.

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. The blowfish encryption process and the text insert along with symmetrical key is shown by the figure 5.The text in the image will be hidden using a specific key and image hidden with 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.



SOURCE IMAGE: sd.jpg

OUTPUT IMAGE: sd1 ● .bmp ○ .png ○ .tif

● Text ○ Image

asdfg

☑ KEY 12344321

MSG ENCRYPTED

Figure 5: Blowfish Encryption Process and Key Insert

In this paper, the original image taken is 'sd.jpg' and by using blowfish algorithm and by insert text along with key, the encrypted image is 'sd1.bmp' which is shown by figure 6. The original text is hidden inside the sd1.bmp image. By using decryption process, the original message is taken out from the image using the same key which is inserted at the time of encryption which is shown by the figure 7.This method will be fast and very safe .The encryption and decryption time is very less.

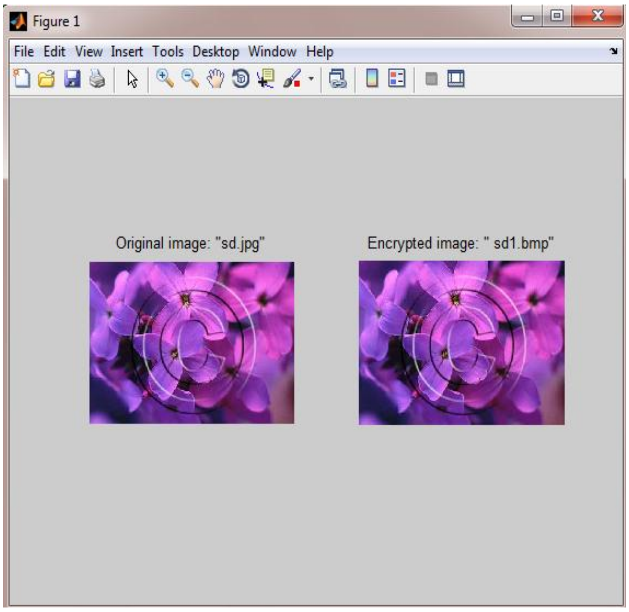
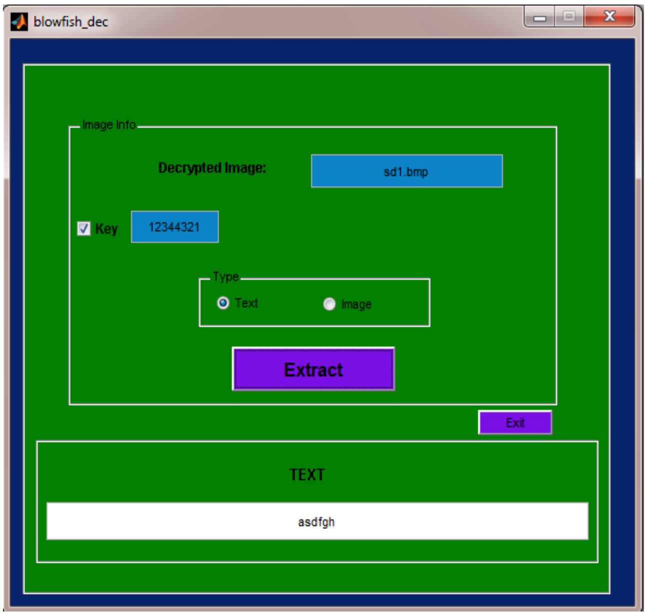


Figure 1
File Edit View Insert Tools Desktop Window Help
Original image: "sd.jpg"
Encrypted image: " sd1.bmp"

Figure 6: Original image and the Encrypted image



Decrypted Image: sd1.bmp

☑ Key 12344321

● Text ○ Image

asdfgh

Figure 7: Original Message is decrypted by using Same Key

With the proposed algorithm, the encryption process is very fast than previous algorithms. The encryption time for various image size using blowfish algorithm is shown by figure 8 and the decryption time is also reduced by using this algorithm in MATLAB software which is shown by figure 9, hence the process is secure and very fast.

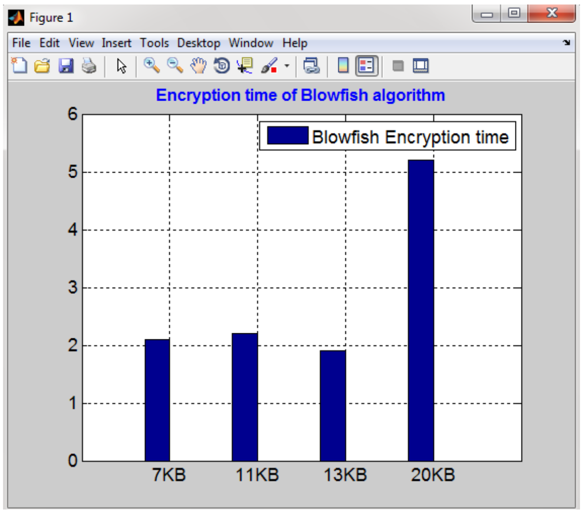


Figure 8: Encryption time of blowfish algorithm

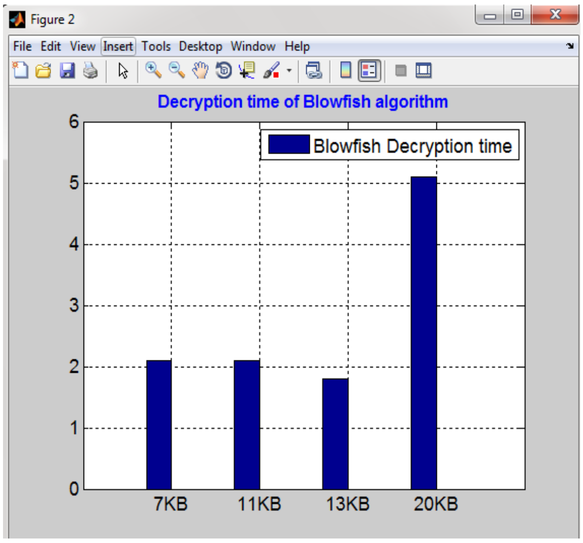


Figure 9: Decryption time of blowfish algorithm

V. CONCLUSION:

The presents simulation results showed that blowfish has a better performance than other common encryption algorithms used. The encryption and decryption rate is fast than any other algorithms. Both color 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), etc. can be encrypted & decrypted using blowfish algorithm. we have proposed and implemented a new approach to further enhance the existing algorithm to achieve better results in terms of parameters such encryption time, decryption time. Better key length will provide better symmetric algorithm implementation and security. The security of proposed cryptosystem is high but hardware complexity also increases when compared with other cryptosystems. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm.

VI. REFERENCES:

[1] Rajesh R Mane A, “Review on Cryptography Algorithms, Attacks and Encryption Tools”; IJIRCCE, Vol. 3, Issue 9, September 2015.

[2] Mrs. Smita Desai, Chetan A. Mudholkar, Rohan Khade, Prashant Chilwant, “Image Encryption and Decryption Using Blowfish Algorithm”; IJEEE, ISSN- 2321-2055 (E),Volume 07, Issue 01, Jan-June 2015.

[3] Anjaneyulu GSGN, Pawan Kumar Kurmi, Rahul Jain, “Image Encryption and Decryption Using Blowfish Algorithm with Randomnumber Generator”; IJPT, Vol. 6, Issue No.3, 7164-7170, 2014.

[4] Anjula Gupta, Navpreet Kaur Walia, “Cryptography Algorithms: A Review”; IJEDR, Volume 2, Issue 2, ISSN: 2321-9939, 2014.

[5] Ayushi, “A Symmetric Key Cryptographic Algorithm”; International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.

[6] M.Sambasiva Reddy and Mr.Y.Amar Babu, “Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, page 3341-3347, July 2013.

[7] Baraka H., El-Manawy H. A., and Attiya A. “An Integrated Model for Internet Security Using Prevention and Detection Techniques”. IEEE Journal of Computer and Communication, Vol. 99, PP. 25-33, 1998.

[8] Akshit Shah, Aagam Shah, Prof. Tanaji Biradar, “Image Encryption and Decryption using Blowfish Algorithm in MATLAB” ; IJEECS ,ISSN 2348-117X, Volume 4, Issue 11, Nov. 2015.

[9] https://en.wikipedia.org/wiki/Blowfish_(cipher)

[10] Ms NehaKhatri Valmik, Prof. V. K Kshirsagar, “Blowfish Algorithm”; OSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, Volume 16, Issue 2, PP 80-83, 2014.

[11] Patterson and Hennessy, “Computer Organization & Design: The Hardware/ Software Interface”, Morgan Kaufmann, Inc. 1994.

[12] https://en.wikipedia.org/wiki/Cryptography

[13] "Cryptography: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) - Schneier on Security". *www.schneier.com*. Retrieved 2015-12-31.