ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Review on Cryptography in Image Using Blowfish Algorithm

Smruti M. Patole[1], Seema S. Patil [2]

PG Student, Department of E&TC, A.M.G.O.I. Faculty of Engineering, Shivaji University, Maharashtra, India[1]

Associate Professor, Department of E&TC, A.M.G.O.I. Faculty of Engineering, Shivaji University, Maharashtra, India[2]

ABSTRACT: With the progress in communication technology, the necessity of information security has become a global issue. Due to advancement in multimedia application, security becomes an important issue of communication and storage of data. This paper is about cryptographic analysis of data using 64-bits Blowfish which is a secret key block cipher having a variable key size up to 448 bits designed in order to secure communication and improve its performance. It iterates simple function 16 times by employing Feistel network. The blowfish algorithm runs faster and prevents unauthorized attack than the popular existing algorithms. Working environment for proposed system is MATLAB.

KEYWORDS: Cryptography, Image encryption, Decryption, Secrete Key Generation, Blowfish Algorithm.

I. INTRODUCTION

Most initial computer application had very little security. This continued for number of years until the importance of data was truly realized. Until then, computer data was considered to be useful, but not something to be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. People realized that data on computers is an extremely important aspect of modern life. Therefore various areas in security began to gain prominence. Two typical examples of such security mechanisms were are follows:

- Provide user id and password to every user, and use that information to authenticate a user.
- Encode information stored in database in some fashion, so that it is not visible to users who do not have right permission.

Cryptography is art of achieving security by encoding messages to make them non-readable. We are living in the information age. We need to keep information about every aspect of our lives. In other words, information is an asset that has a value like any other asset. As asset information needs to be secured from attacksIn the current technology world, data transmission of various multimedia like sensitive images, video, text is very important and security is major concern in any field. Security is very important, as illegal users may hack the sensitive data.During transmissions of data or information, there are chances that data may hack. Cryptography provides a solution for this problem. The main goals behind using Cryptography include Confidentiality, Integrity, Authentication, and Non-Repudiation are as follows:

- Confidentiality: Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.
- Data Integrity: Data integrity provides a means for detecting whether data has been manipulated in an unauthorized manner. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.
- Authentication: Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Authentication service has two variants: Message authentication and Entity authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

- Non-Repudiation**:** Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

II. RELATED WORK

In [1] authors presents a comparative study of different key algorithms like, AES, DES, 3DES, Blowfish and RSA.Each algorithm has been compared on different set of parameters. From the results it has been found that among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient algorithms. The speed and power consumption of these algorithms are better compared to the others. In case of asymmetric encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security. In [2] authors presented a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. There is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. In the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used.In [3] authors present an encryption algorithm has been designed and developed using blowfish method with supplementary key in java. Various images are used in experiments and performance measures are recorded. In addition to that security factor is also analyzed.In [4] authors developed a Blowfish encryption algorithm for information security. In the proposed Blowfish algorithm reduce rounds of algorithm and proposed single blowfish round. The design simulation is done by Xilinx ISE software using the language of VHDL .In [5] authors present the comparison between two cryptographic algorithm AES and Blowfish algorithm on the basis of ARM implementatiom.LPC 2148 from NXP Philips family kit is used for implementation. In Embedded system security blowfish is suitable. For comparison, authors considered points like memory size, encryption cycle, and decryption cycle for both algorithms on ARM7 etc .In [6] authors implement an Blowfish Algorithm using WDDL Logic style. In the implementation bottom-up approach is used.

III. COMPARATIVE STUDY

Cryptography, a word with Greek origin, means “secret writing”. However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. The main work of the cryptography is to send the messages between receiver and the sender, in a way that prevents other participants from reading the messages Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving two distinct mechanisms: symmetric-key encryption, asymmetric-key encryption.

A. SYMMETRIC-KEY ENCRYPTION:

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.
Persons using symmetric key encryption must share a common key prior to exchange of information. Keys are recommended to be changed regularly to prevent any attack on the system. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), AES, and BLOWFISH.

- **DATA ENCRYPTION STANDARD (DES) :**

56-bit key is used in DES and 16 cycle of each 48-bit sub keys are formed by permuting 56-bit key. Order of sub keys is reversed when decrypting and the identical algorithm is used. Block size of 64-bit is made from L and R blocks of 32-bit. [6]

- **TRIPLE DES (3DES):**

Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force. [6]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

- **ADVANCED ENCRYPTION STANDARD (AES) :**

Advanced Encryption Standard, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. Brute force attack is the only effective attack known against this algorithm. AES encryption is fast and flexible. [6]

- **BLOWFISH :**

Blowfish is 64-bit block cipher- used to replace DES algorithm. Ranging from 32 bits to 448 bits, variable-length key is used. Variants of 14 round or less are available in Blowfish. Blowfish is unpatented and license-free and is available free for all uses. Blowfish is one of the fastest block ciphers developed to date. Blowfish suffers from weak keys problem, still no attack is known to be success. [6]

B. ASYMMETRIC –KEY ENCRYPTION:

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext. It requires putting the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption. . A few well-known examples of symmetric key encryption methods are: Rivest Shamir Adlemen (RSA), Diffie-Hellman and Digital Signature Algorithm.

- **RSA:**

The RSA Algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman, who first published the algorithm in April, 1977. The RSA Algorithm is public key cryptography and it ensures that whilst an encryption key is Publicly revealed, it does not reveal the corresponding decryption key. Typical encryption techniques use mathematical operations to transform a message (represented as a number or a series of numbers) into a cipher text. [6]

- **DIFFIE-HELLMAN:**

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography and is generally referred to as Diffie-Hellman key exchange. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is Limited to the exchange of secret values. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

- **DIGITAL SIGNATURE:**

The most important development from the work on public-key cryptography is the digital signature. The digital signature provides a set of security capabilities that would be difficult to implement in any other way. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message. The digital signature standard (DSS) is an NIST standard that uses the secure hash algorithm (SHA).

IV. PROPOSED ALGORITHM

In this proposed model, image security has been obtained by encrypting and decrypting image using cryptography. It is based on Blowfish algorithm with additional secret key to provide extra security while sending and receiving images and sensitive data. This proposed model is designed to process any type of images (i.e .jpg, .gmp, .tiff, .png, etc). Proposed system is designed to process various types of images for different parameters of measure.This system basically use the Blowfish encryption .This algorithm is a 64-bit block cipher with a variable length key. This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement. It is a 64 bit block cipher and it is fast algorithm to encrypt the data. It is variable length key block cipher up to 448 bits. Blowfish contains 16 rounds. Each round consists of XOR operation and an F function. The design of the proposed model is given in the Fig.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

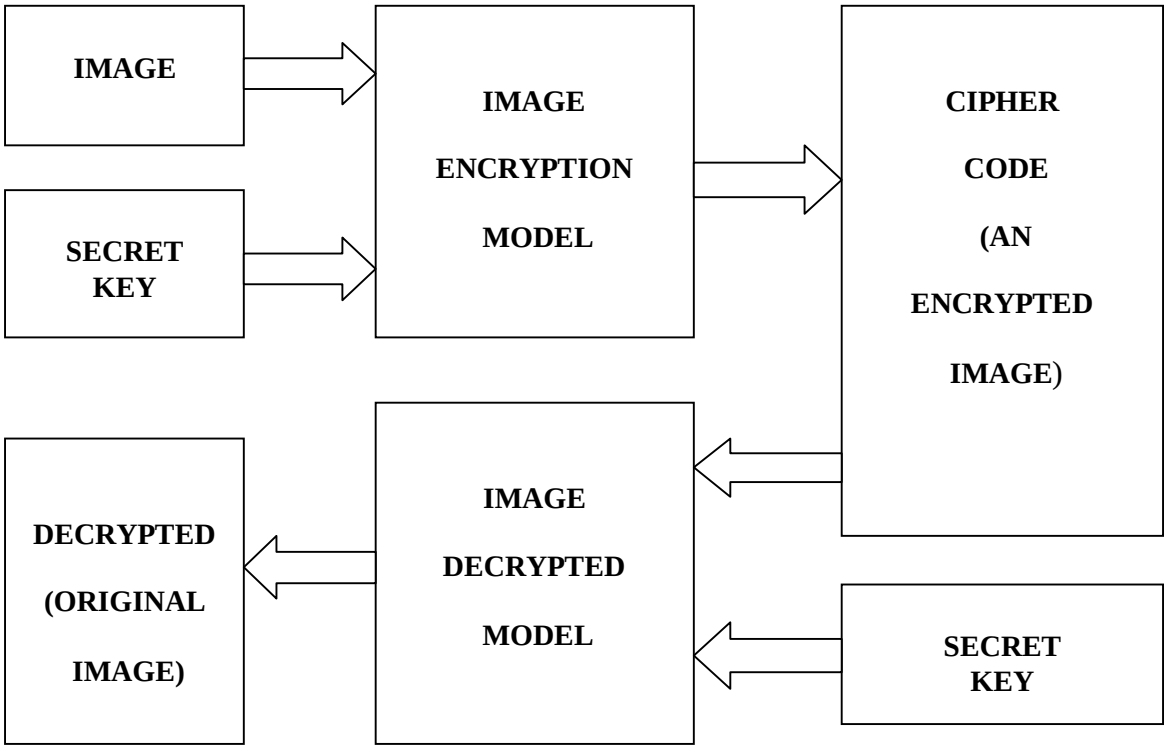

Fig. BLOCK DIAGRAM OF PROPOSED SYSTEM

IMAGE: This is the original intelligible message or data that is fed into the algorithm as input.

ENCRYPTION MODEL: The encryption model performs various substitutions and transformations on the image. In the encryption model blowfish algorithm is used

SECRET KEY: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

CIPHER CODE: This is the scrambled message produced as output. It depends on the image and the secret key. For a given message, two different keys will produce two different cipher codes.

DECRYPTION MODEL: This is essentially the encryption model run in reverse. It takes the cipher code and the secret key and produces the original image. In the decryption model blowfish algorithm is used.

This proposed model is designed to process any type of images (i.e. .jpg, .gmp, .tiff, .png, etc). There are three main steps in this work as follow:

• Key Generation and Expansion: Key Size of 64 Bit is generated. Many operations like XOR, XNOR, Circular shifting are performed to make the strong key. Hence higher security is provided.

• Encryption of Image: Block size is also 64 Bit. Read function in MATLAB is used to read this image. Encryption is used to convert plain image into cipher image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

• Decryption of Image: It is reverse process of encryption.

A. KEY GENERATION AND EXPANSION

Key expansion is the process of sub key generation. Image Block size is 64 bit and key size also 64bit.Keys are generated before the image encryption and decryption process. There is a P array and four 32-bit S boxes. The P array contains 18 32-bit sub keys and out of four S boxes, each S box contains 256 entries. Blow Fish uses a large number of sub keys. These keys must be pre - computed before any data encryption or decryption**.** The algorithm generates sub keys as follows:
The P-array consists of 18 32-bit sub keys:
P1, P2... P18.
There are four 32-bit S-boxes with 256 entries each

S0,0,	S0, 1...	S0,255;
S1,0,	S1, 1...	S1,255;
S2,0,	S2, 1...	S2,255;
S3,0,	S3, 1...	S3, 255.

- **Generating the Sub keys :**

The sub keys are calculated in the following way.
1. Initialize P-array and four S-boxes with a fixed string. This string contains the hexadecimal digits of pi (less the initial 3): P0 = 0x243f6a88, P1 = 0x85a308d3, P2 = 0x13198a2e, etc.
2. XOR P0and the first 32 bits of the key, XOR P1and the second 32-bits of the key, and so on for all bits of the key. Repeatedly continue through the key bits up to the whole P-array has been XORed with key bits.
3. Encrypt all-zero string using Blowfish algorithm, with the sub keys given in steps (1) and (2).
4. Replace P0 and P1 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
6. Replace P2 and P3 with the output of step (5).
7. Continue the process, exchanging all entries of the P array, and then all four S-boxes.
In total, 521 iterations are required to generate all required sub keys. Applications can store the sub keys rather than execute this derivation process multiple times. [3]

B. ENCRYPTION OF IMAGE

The Encryption of Blow Fish algorithm precedes the following steps.
Step 1: Initialize S Box and T Box as arrays.
Step 2: Convert the matrix Inverse to Transpose and store in T Box.
Step 3: The input is a 64-bit data element, x.
Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL
XOR Pi xR = F (xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the cipher image. [3]

C. DECRYPTION OF IMAGE

Decryption process precedes the following steps.
Step 1: Initialize S Box and T Box as arrays.
Step 2: Secret key comparison between original key which is created while encryption.
Step 3: The input is a 64-bit data element, x.
Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

XOR Pi xR = F (xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the original image. [3]

V. CONCLUSION

A result from a comparative study and literature survey of blowfish algorithm is states that the blowfish algorithm is best for data (e.g. image) security as compared to DES, 3DES, AES, RSA etc. The above mentioned system inspires to make an attempt to develop the existing algorithm which encrypt and decrypt images of various file formats LIKE .jpg, .gmp, .tiff, .png, etc in MATLAB. Blowfish algorithm can't be easily broken by the hackers until they find the correct combinations. This is more difficult to form the exact combinations of the lock. To make the algorithm stronger number of rounds has been increased. It takes less time to encrypt and decrypt the image than any other algorithms.

REFERENCES

1. Ankita Verma, Paramita Guha, Sunita Mishra,'' Comparative Study Of Different Cryptographic Algorithms'', International Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 5, Issue 2, March - April 2016.
2. Milind Mathur,Ayush Kesarwani,"Comparison Between DES , 3DES , RC2 , RC6 , Blowfish And AES ", Proceedings Of National Conference On New Horizons In It - Ncnhit 2013.
3. Kanagalakshm, M.Mekala,"Enhanced Blowfish Algorithm For Image Encryption And Decryption With Supplementary Key", International Journal Of Computer Applications (0975 – 8887), Volume 146 – No.5, July 2016.
4. Saikumar Manku And K. Vasanth,'' Blowfish Encryption Algorithm For Information Security'', Arpn Journal Of Engineering And Applied Sciences, Vol. 10, No. 10, June 2015.
5. Ms. Pallavi H.Dixit , Dr.Uttam L. Bombale , Mr. Vinayak B.Patil ," Comparative Implementation Of Cryptographic Algorithms On Arm Platform", International Journal Of Innovative Research In Science,Engineering And Technology, Vol. 2, Issue 10, October 2013.
6. M.Dinesh And Dr.P.Suveetha Dhanaselvam," Real Time Image Encryption And Decryption Using Blowfish Algorithm", International Journal Of Emerging Technology In Computer Science & Electronics (Ijetcse) Issn: 0976-1353 Volume 22 Issue 2 – May 2016.
7. Pia Singh, Prof. Karamjeet Singh," Image Encryption And Decryption Using Blowfish Algorithm In Matlab", International Journal Of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
8. Bruce Schneier, "The Blowfish Encryption Algorithm, http:// www. schneier.com/ blowfish.html".

BIOGRAPHY

Ms. Smruti M. Patole did her diploma (E&TC) from Government Polytechnic; Kolhapur in the year 2012.She did her B.E (E&TC) from S.D.G. Cha Trusts G.O.I., Atigre in the year 2015. She is pursuing her M.E. (Electronics and Tele-communication) from A.M.G.O.I. faculty of engineering, Vatar tarf Vadgaon. She has attended number of workshops on various subjects.

Mrs. Seema S. Patil did her B.E (E&TC) from TKIET, Warananagar in the year 2004. She is pursuing her M.E. (Electronics and Tele-communication) from RIT, Isalampur. She has a total of 12 years of experience in teaching. She has presented 9 papers in International Journal .She has attended number of workshops on various subjects. At present she is working as Associate Professor at A.M.G.O.I. faculty of engineering.