International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

COMPARATIVE STUDY ON BLOWFISH AND TWOFISH ALGORITHMS FOR IMAGE ENCRYPTION AND DECRYPTION

Chadalavada Lasya Chowdary[1], Pavithra Nallamothu[2], Marthala Charan Reddy[3], Burra Vijay Babu[4]

[1]Lasya student of B.Tech Computer Science and Engineering, K L University, Vijayawada, Andhra Pradesh, India
[2]Pavitra student of B.Tech Computer Science and Engineering, K L University, Vijayawada, Andhra Pradesh, India
[3]Charan student of B.Tech Computer Science and Engineering, K L University, Vijayawada, Andhra Pradesh, India
[4]Vijay Babu: Professor, Dept. of Computer Science and Engineering, K L University, Andhra Pradesh, India

---

Abstract - *Web and System applications are growing very fast and the requirements to secure such applications is also being expanded. One among the requirements is Image security. As number of web assaults have been increasing image security has became the greatest concern. To prevent such assaults, Encryption algorithms are very useful. Encryption algorithms can guarantee protection, privacy and data security for making web a safer place. The two main fundamental characteristics of any encryption algorithm is its speed and security. In this paper we have compared the speed of two encryption algorithms Blowfish and Twofish by encrypting and decrypting different types of image files. Through different sizes of image files we have analyzed the encryption and decryption speed of both the algorithms. From the results we have found that Blowfish takes less time to encrypt and decrypt the image file when compared to Twofish. Blowfish algorithm is better when compared to Twofish as far as the encryption and decryption speed is considered.*

Key Words: **Blowfish, Twofish, Encryption, Decryption, Image.**

1. INTRODUCTION

Now-a-days the number of organizations have been increasing rapidly and a huge amount of data is being generated by them every day on the internet and they store it in the cloud. Data has been the greatest resource for an association and to maintain its privacy, validation and access control has to be redistributed. To secure the data and to maintain its privacy we are encrypting the data. Encryption is a procedure which is used to convert unique message or a plaintext into a ciphertext and transmits the data securely and safely over the cloud. They are two types of encryption algorithms. Symmetric-key encryption and Assymmetric -key encryption. In Symmetric key encryption we use only one key to encrypt and decrypt the data. Examples are AES, DES, 3DES, Blowfish, Twofish etc..

For Assymmetric encryption algorithm we use two keys i.e. a private key and a public key. For encrypting the data we use a public key and for decrypting the data we use a private key. Example for asymmetric encryption algorithm is Diffie Hellman (DH). In this paper we are going to implement the Blowfish and Twofish algorithms. By using these two algorithms we are going to encrypt and decrypt the various sizes image files. We know that blowfish algorithm is strongest among all the algorithms.

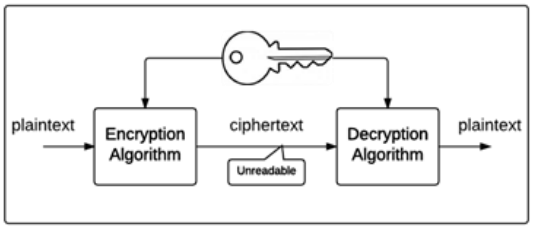

Fig -1: Encryption/Decryption Process

1.1 OVERVIEW OF TWO ALGORITHMS:

Blowfish: It is one of the best among symmetric key encryption algorithms. It was developed by Bruce Schneier in 1993. It consists of a variable key length of most extreme up to 448 bits. It's block size is of 64-bits.This algorithm consists of two stages. The first one is key expansion phase, In this stage 448bit keys is changed over into sub keys of 4168 bytes in total. The second phase is encryption phase, in this phase a function is iterated 16 times and by using the xor operation the encrypted text is obtained. Blowfish has been using in many applications now a days and it has became the strong encryption algorithm.

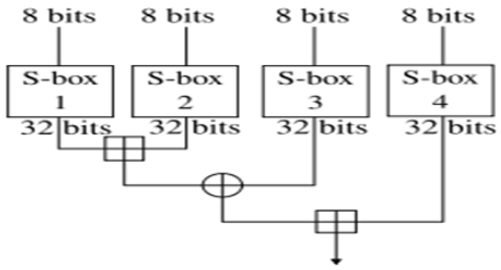

Fig -2: Blowfish Encryption Scheme

Twofish :- A Symmetric-key encryption algorithm which has a block size of 128 bits with variable key length up to 256 bits. It is highly secured and more flexible. It works well with 8 bit smart card processors, Large processors. It consists of total of 16 rounds, predicting atleast 32 bits of Non trivial data in every round.

Given a,b as two inputs, the 64 bit is divided into half i.e.32 bits PHT can be defined as:

a' = a+b mod (2^32).

b' = a + 2b mod(2^32).

PHTmeansa pseudo hadamard transfosm which is used for a simple operation, which runs quickly in the software to give two inputs a,b and it can be executed in teo opcodes on the modern microprocessors.

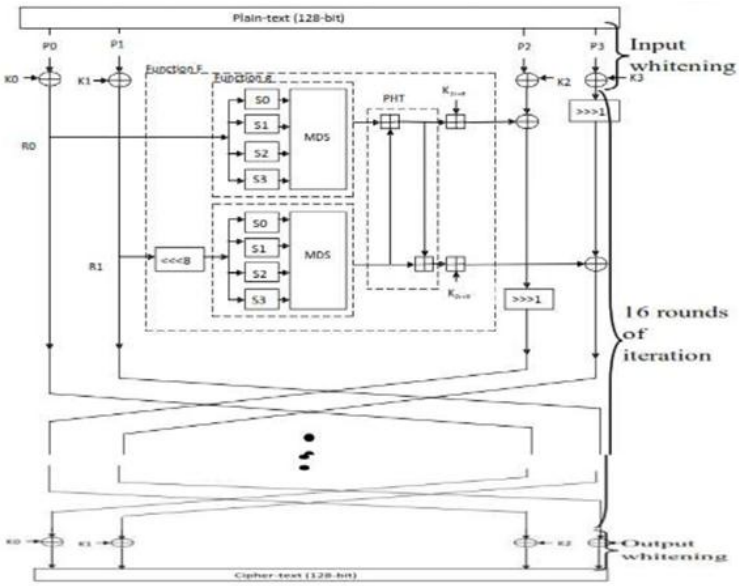

Fig -1: Encryption/Decryption Process

2. LITERATURE SURVEY

M Panda and Nilesh Amarbhai in [1] has described the Symmetric key encryption algorithms on different aspects of files. He demonstrated that among all symmetric algorithms they have compared, AES and Blowfish have taken less time to encrypt and decrypt for all different types of text, image and video files. Bruce Schneieri [2] has analyzed Twofish encryption algorithm on different types of text files. He explained the working principle of twofish algorithm with a complex-key schedule. Deepali in [3] has analyzed the speed of encryption on Twofish and Blowfish algorithms on different types of text documents and had confirmed that for encrypting the text file requires less time for twofish when compared with blowfish. According to the performance of these two algorithms, they concluded that if we increase the size of the data then the time taken to encrypt the files also been increasing. Shun Lung in [4] has proposed modified twofish algorithm. They used a 256-bit size instead od 128 bits. Srividhya in [5] has described twofish algorithm for image encryption and decryption using 128- bit block size. Pla Singh[6] has proposed the blowfish algorithm for encryption and decryption of Images.

3. PROPOSED MODEL

For the encryption and decryption of Images we have used two encrypting algorithms blowfish and twofish. Blowfish is a 64-bit block cipher which accepts a 32-bit variable length key. Blowfish algorithm is used to encrypt the 64-bits of raw data into a cipher text. This algorithm is more efficient and secured. Here in this project we take image as a plaintext. With the help of encryption key, the key that is generated by using blowfish algorithm the original image data is divided into blocks. Image header is prohibited for the encryption and the beginning of the bitmap pixel starts directly after the header of the document. The byte pixels is stored in row-wise that to from left to right in an array where each row represents one scan line of image. For Image the rows encryption starts from top to bottom.

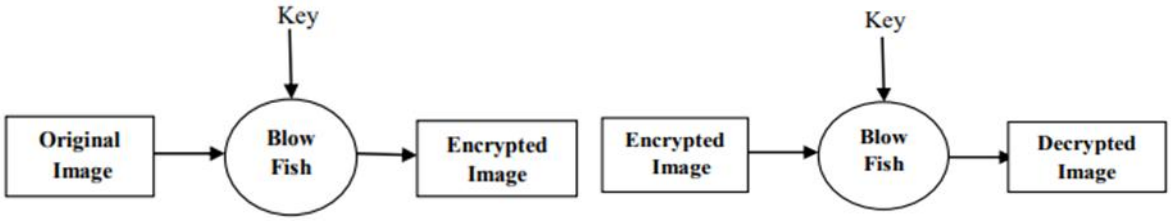

Image encryption using Blowfish Algorithm

Image decryption using Blowfish Algorithm

For blowfish decryption, same process has to be applied as encryption. But here we take encrypted image as the input and the same encryption key when we used during the process of encryption. Here the encrypted image is again divided into same bits block length from top to bottom. After the entry of first block into decryption with the help of encryption key the image decryption starts but here the sub keys have been reversed. This process continues with the other blocks of image also from top to bottom. Hence the encryption and decryption of a image using blowfish have been completed. Try the same process with different sizes of images and note down the time that has taken to encrypt and decrypt the image using Blowfish.

The Basic algorithm of Blowfish encryption and decryption is

Let x be a 64-bit input data element, let Xl, Xr be the half of the size of data element i.e. 32-bit.

For j = 1 to 16:

Xl = Xl ^ Pi;

Xr=F(Xl) ^ Xr;

Now Swap Xl and Xr;

End for;

Again swap Xl and Xr;

Then Xl = Xl ^ P18 and Xr = Xr ^ P17;

Then at last combine both Xl and Xr for the encrypted text(Cipher text).

For decryption we apply the same process But the P1,P2,.. subkeys we have to send in reverse order.

Image encryption and decryption using twofish:

Twofish is a Symmetric key encryption algorithm and 128-bit block cipher which accepts variable length key of 128 bits, 192 bits and 256 bits. In this algorithm the input is the image file and the encryption key i.e. the key that is generated using twofish algorithm. The image file is divided into 128 different blocks of sub images. After the completion of image encryption the encrypted image will be turned in to some gray colour. The 128 sub images will be located randomly at different positions. After all the 128 sub images will be merged in to one image, a single encrypted image.

Fig-6: Image Encryption And Decryption Using Twofish Algorithm

For decrypting the image the user has to send the encrypted image and same key that is used for encryption for the decryption process. Again in this step the Image has been divided into 128 sub images of different blocks. After completion of dividing the image in to 128-bits of sub images, all these sub images are merged in to one decrypted image i.e. Original Image. After completing the encryption and decryption of image take down the time it has taken. Test with different types of image files and compare it with the blockfish algorithm encryption and decryption timings.

By comparing both the results we found that the time taken by twofish algorithm to encrypt and decrypt the image is more when compared with blowfish algorithm for encrypting and decrypting the image. But when we use these two algorithms for encrypting the data file the twofish algorithm requires less time when compared with blowfish algorithm.

4. RESULT

In this paper we compared the blowfish and twofish algorithms for image encryption. For that we encrypted and decrypted the different types of image files ranges between 1 KB to 1000 KB and we have calculated the time for both encryption and decryption.

Image size (In Kb)	Blowfish	Twofish
1.1	0.015	0.65
5.3	0.016	0.62
100.2	0.02	0.60
501.1	0.04	0.69
1000	0.046	0.49

Table.1 Time comparison Between Blowfish and Twofish

Below graph represents the Encryption and decryption time comparisons of blowfish and twofish. Twofish requires more time to encrypt and decrypt the image file than Blowfish.

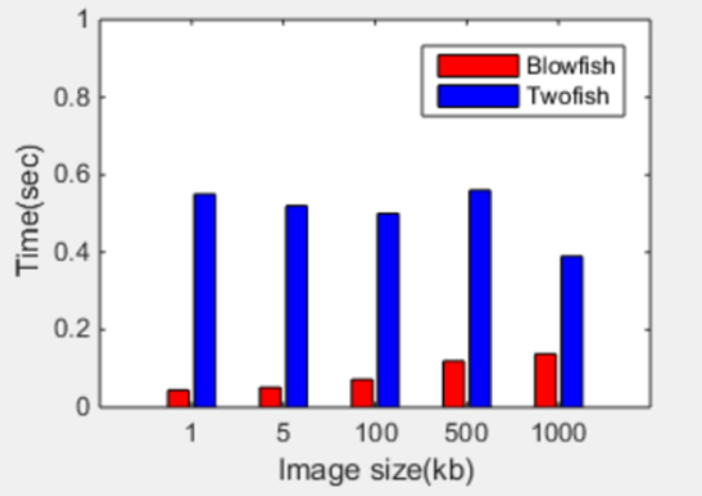

Chart -1: Graph illustrates Time Comparisons between Blowfish and Twofish

5. CONCLUSION

In this paper, we have discussed about the two most symmetric encryption algorithms – Blowfish and Twofish. From the results we found that for the Image encryption and decryption twofish requires more time when compared with blowfish algorithm. Hence we conclude that the blowfish algorithm is the best technique to use for image encryption when compared with twofish.

6. FUTURE ENHANCEMENT

In future we intended to enhance the performance of encryption and decryption time of image files and video files using symmetric key encryption algorithms like AES,DES,3DES, Blowfish and Twofish. And also by Comparing the data files using Assymmetric algorithms.

REFERENCES

[1] M. Panda, "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, 2016.
[2] Schneier, J. Kelsey, D. Whiting, D. Wagner,C. Hall, and N. Ferguson, "TwoFish: A 128-bit Block Cipher", AES submission, june 1998.
[3] Deepali D. Rane," Superiority of Twofish over Blowfish", 2016 International Journal of scientific research and management (IJSRM).
[4] Shun-Lung & Wuu, Lih-Chyau & Jhang, Jhih-Wei. (2007). "A new 256-bits block cipher - Twofish256". ICCES'07 - 2007 International Conference on Computer Engineering and Systems. 166-171. 10.1109/ICCES.2007.4447043.
[5] Srividhya G, Manikandan K -"Image Encryption and Decryption Using Twofish Algorithm", iammanicse – April 2019.
[6] Pia Singh & Prof. Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm" , International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[7] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.
[8] Shiho Moriai, Yiqun Lisa Yin. "Cryptanalysis of Twofish (II)".Technical Report, IEICE, ISEC2000-38, 2000.
[9] Dr. S.A.M Rizvi, Dr. Syed Zeeshan Hussain et.al "Performance Analysis of AES and TwoFish Encryption Schemes", International Conference on Communication Systems and Network Technologies 2011.
[10] Nikhil Joshi, Jayachandran Sundarajan et.al. "Tamper Proofing by Design using generalized involution-based concurrent error detection for involutional Substitution Permutation and Feistel Network" IEEE Transaction on Computer, October 2006.
[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] H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.