International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Image File Encryption using Symmetric Key Algorithms

N. K. Barpanda[1] , M. Panda[2] , A. Panda[3]

1.Reader, Electronics, SUIIT,Sambalpur University

2.Assistant Professor , Computer Science, SUIIT, Sambalpur University

3.Assistant Professor,EEE, SUIIT,Sambalpur University

ABSTRACT

Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. It is a process of making information indecipherable to an unauthorized person. There are different encryption algorithms used for these purpose. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This paper provides a fair comparison of some symmetric key cryptographic ciphers (AES,BLOWFISH, DES ,T.DES) on the basis of encryption and decryption time with different sizes of image files using Java as the programming language.

***Keywords— DES, 3DES,Blowfish, AES, Performance metric*.**

I.INTRODUCTION

Security plays an important role in our life as well as in the area of networking for transmission of data from one device to other. One of the primary reasons that intruders are successful is that most of the information they acquire from a system is in a form that can be read and comprehended. Cryptography is a science of secret writing. It provides a method for securing and authenticating the transmission of information across insecure communication channels. In cryptography, the data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising the plaintext in such a way that hides its substance is called encryption. Encrypting plaintext makes the information in unreadable form called cipher text. The process of converting cipher text to its original information is called decryption. A system that performs encryption and decryption is called cryptosystem. On the basis of key used, cipher algorithms are classified as asymmetric key algorithms, in which encryption and decryption is done by two different keys and symmetric key algorithms, where the same key is used

for encryption and decryption [1]**.** The main goal of cryptography is to keep the data secure from unauthorized access [2].Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES,3DES etc. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [3]. We here focus only on symmetric cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption, in contrast to asymmetric key cryptography. The main objective of this paper is to analyze time taken for encryption and decryption by some commonly used symmetric key cryptographic algorithms for different sizes of image files using java programming language.

II.CRYPTOGRAPHIC ALGORITHMS

This section provides information about the various symmetric key cryptographic algorithms to be analyzed for performance evaluation, to select the best algorithm to provide security for data. Symmetric key cryptographic ciphers come in two varieties, stream ciphers and block ciphers. Block Ciphers operate with a fixed transformation on large blocks of plain text data while stream ciphers operate with the time varying transformation on individual plain text bits. There are different symmetric cryptographic algorithms in the literature [4] [5]. Out of them, the algorithms listed in the Table 1 are selected for detailed study in this paper.

Table 1.CRYPTOGRAPHIC ALGORITHMS INFORMATION

Scheme	Algorithm	Structure	Contributor	Key Length	Rounds	Block Size
DES	Symmetric	Balanced Feistel network	IBM75	56 bits	16	64 bits
3DES	Symmetric	Feistel network	IBM78	168, 112 or 56 bits	48	64 bits
AES	Symmetric	Substitution-permutation network	Rijndael	128, 192, 256 bits	10 or 12 or 14	128 bits
BLOWFISH	Symmetric	Feistel network	Bruce Schneier	32-448 bits	16	64 bits

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

a).Evaluation Parameters

In this paper, analysis is done with following metrics under which the cryptosystems can be compared.

Encryption time- The time required to convert plaintext to cipher text is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment we have measured encryption time in milliseconds. Encryption time impacts performance of the system. This time must be less making the system fast and responsive.

Decryption time- The time to recover plaintext from cipher text is called decryption time. The decryption time is desired to be less similar to encryption time to make system responsive and fast. Decryption time impacts performance of system. In our experiment, we have measured decryption time is milliseconds.

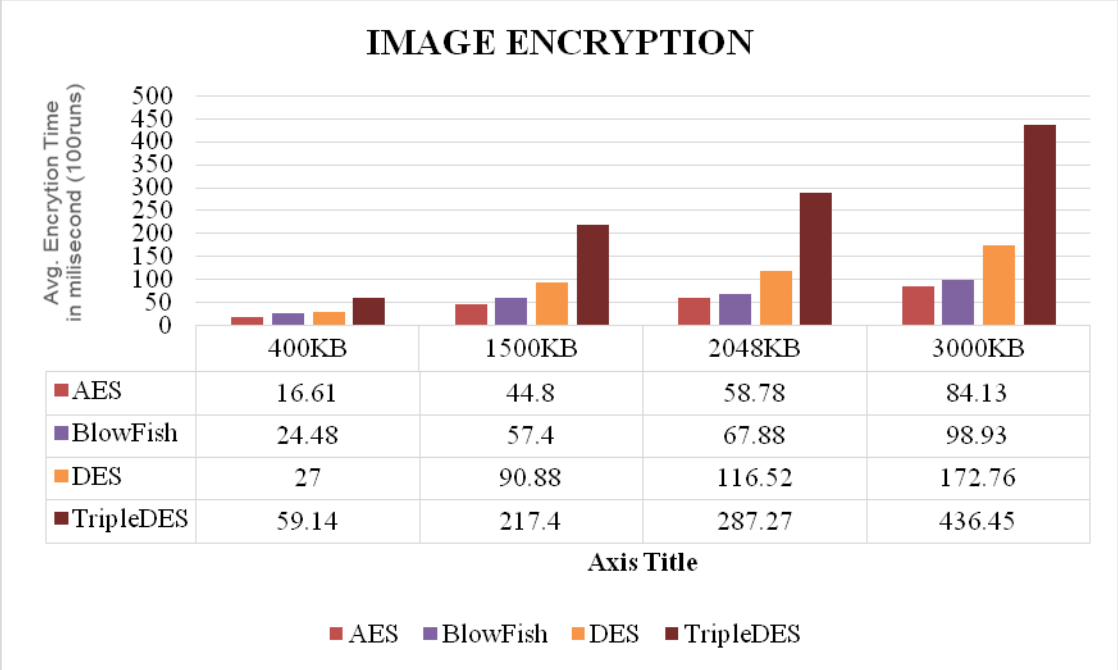
b) Evaluation Platforms

The encryption algorithms are evaluated considering the following system configuration.

1.Software Speciation: Experimental evaluation on Geany with Java Development Kit 8, Windows 8Pro64 bit Operating System.

2. Hardware Speciation: All the algorithms are tested on Intel® Core™ i3 2328M (2.20 GHz) processor with 2GB of RAM with 160GB HDD

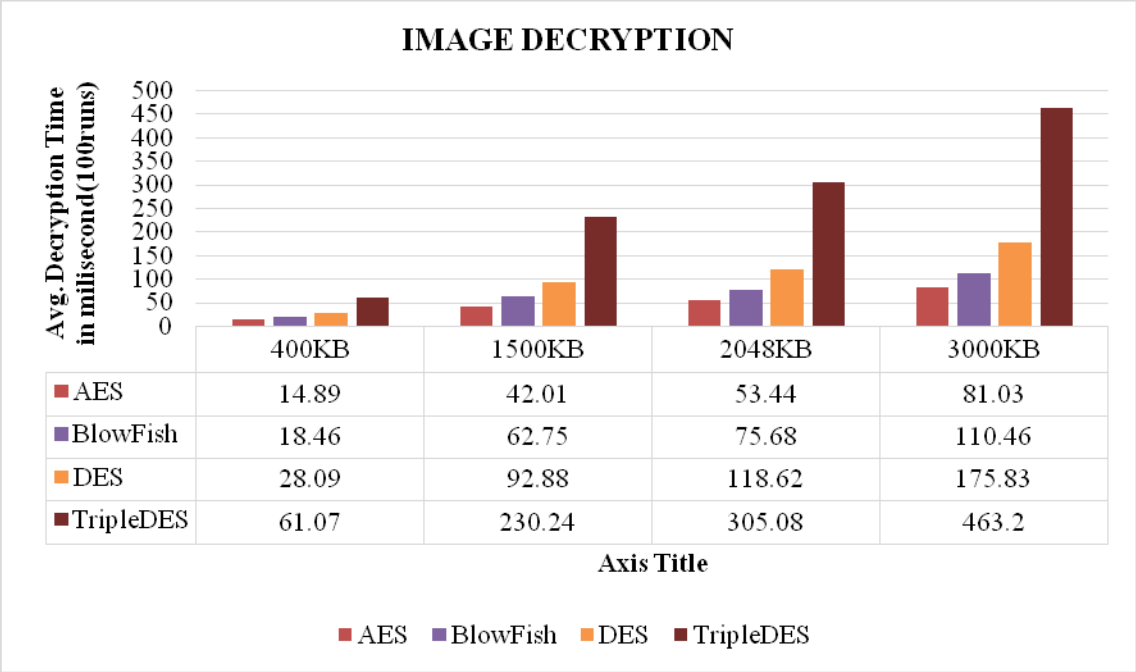
IV. SIMULATION RESULTS AND ANALYSIS



	400KB	1500KB	2048KB	3000KB
AES	16.61	44.8	58.78	84.13
BlowFish	24.48	57.4	67.88	98.93
DES	27	90.88	116.52	172.76
TripleDES	59.14	217.4	287.27	436.45

Fig-1: Encryption Time of Different Algorithm for Image Files

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354



.Fig.-2: Decryption Time of Different Algorithm for Image Files

Image File Size	ALGORITHMS							
	AES		BLOWFISH		DES		T_DES	
	Average Encryption time(MS)	Average Decryption Time(MS)	Average Encryption Time(MS)	Average Decryption time(MS)	Average Encryption time(MS)	Average Decryption time(MS)	Average Encryption time(MS)	Average Decryption time(MS)
400kb	16.61	14.89	24.48	18.46	27	28.09	59.14	61.07
1500kb	44.8	42.01	57.4	62.75	90.88	92.88	217.4	230.24
2048kb	58.78	53.44	67.88	75.68	116.52	118.62	287.27	305.24
3000kb	84.13	81.03	98.93	110.46	172.76	175.83	436.45	463.2

V.CONCLUSION AND FUTURE WORK

We have done the analysis of execution time of different algorithms in terms of encryption time and decryption time with different sizes of image files . The results shows that AES algorithm is the best as compared to other algorithms (Blowfish, DES and Triple DES). After AES, Blowfish algorithm performs better as compared to the DES and Triple DES. From this analysis we also conclude that Triple DES algorithm is worst as compare to the other algorithms as it takes a lot of time to encrypt as well as decrypt an image.

The future work can be done to compare performance of these algorithms on audio and video files

REFERENCES

[1]. Jonathan Knudsen, Java Cryptography, 2nd Edition, O'Reilly, 2011.

[2]. Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", International journal of network security vol.10,No.3,pp,216-222,May 2010 .

[3]. Hardjono, "Security In Wireless LANS And MANS,"Artech House Publishers 2005.

[4]. Jonathan Knudsen, Java Cryptography, 2nd Edition, O'Reilly, 2011.

[5] Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition, Tata McGraw Hill, 2012.