Implementation of Image Cryptography Algorithms: A Review

Harpreet Singh[#1], Dr.Naveen Dhillon[*2], Sukhpreet Singh Bains[@3]
[1]M. Tech, Department of ECE, RIET, Phagwara, Punjab, India
[2] HOD, Department of ECE, RIET, Phagwara, Punjab, India
[3] AP, Department of ECE, RIET, Phagwara, Punjab, India

Abstract- *Cryptography techniques plays important role in image security systems in communication. There are many cryptographic algorithms are used to protect or hide confidential data from unauthorized access. Encryption is used to protect data in networks in unreadable form. On the other way, Decryption is used to access unreadable form to original form. This paper consists of comparison between four most common Encryption/Decryption algorithms: DES, 3DES, AES AND BLOWFISH in terms of showing these parameters: block size, correlation, entropy values, key size, rounds, time consumption and throughput of algorithms. The results show that Blowfish algorithm is more suitable than other algorithms for protection of confidential data.*

Keywords **–** Cryptography, Image Encryption, Cipher, Blowfish

I.INTRODUCTION

In cryptography, Encryption/decryption is the process of encoding information in such a way that unauthorized networks cannot read it, but only authorized can. Symmetrical algorithms can be transmit data over the networks in two ways: block ciphers and stream ciphers .Block cipher are the groups of fixed length blocks of image example –DES, AES and Blowfish .Stream cipher is used to transmit one bit at a time example RC4.Blowfish is encryption /decryption algorithm is more suitable than AES, DES algorithm which consumes less power consumption, low correlation between pixels and variable key length and entropy values.

II. DIFFERENT COMPARED ALGORITHMS:

DATA ENCRYPTION STANDARD (DES)

Data encryption standard was the first encryption standard to be published by NIST (National institute of standard and technology). It was designed by IBM based on their Lucifer cipher. DES became a standard in 1974 and it was adopted as a national standard in 1997. DES is a 64-bit block cipher under 56 bit key. There are many attacks recorded against the weaknesses of DES which makes it insecure block cipher. This standard is public.

TRIPLE DES (TDES)

The triple DES (3DES) algorithm is considered as a replacement message which provides TDES as a strongest encryption algorithm which is hard to break because of its combinations. Two different keys for the algorithm can also be used which reduces the memory requirement of keys. But this algorithm has a drawback that it is very time consuming.

ADVANCED ENCRYPTION STANDARD (AES)

This algorithm is also called as Rijndael which is also known as Rain Doll algorithm. It was developed by two scientists Joan and Vincent Rijmen in 2000. Rijndael key and block length is 128 bit which performs 9 processing rounds. If the bit of the key is increased processing rounds are incremented automatically. This symmetric block can encrypt data of 128 bits using keys 128, 192 or 256. A well known attack i.e. Brute force attack i.e. Brute force attack is the only attack against this algorithm.

BLOWFISH

This is symmetric block cipher that is effectively used for encryption and securing the data present in the image. Bruce Schneier designed blowfish in 1993 as a fast, free algorithm. A variable length key is used from 32 bits to 448 bits making it ideal for securing data. This kind of algorithm is license free and is available free for all users. No attack is useful against this algorithm. The elementary operations of Blowfish algorithm include table lookup, addition and XOR. This algorithm has Feistal rounds. This algorithm has 64 bit block and is used as the replacement for DES. This is fast and can encrypt on 32 bit microprocessor. This algorithm is quite

compact. The blowfish algorithm used for image encryption decryption has a look up table of Correlation and an Entropy value of the algorithm is as shown in the table below.

SYSTEM	CORRELA-TION	ENTROPY
BLOWFISH(448)	0.0189	5.2703
TWO FISH(256)	0.0054	5.5437
RIJN DAEL (AES256)	0.0051	5.5436
RC4(2048)	0.0038	5.5437

Table: Comparison between algorithms in terms of correlation and entropy

SYSTEM	NUMBER OF BLOCK	COORELATION	ENTROPY
BLOWFISH(448)	30X30	0.0063	5.4402
	60X60	0.0049	5.5286
	100X100	0.0044	5.5407
	300X300	0.0028	5.5438
TWO FISH(256)	30X30	0.0026	5.5437
	60X60	0.0040	5.5439
	100X100	0.0041	5.5438
	300X300	0.0029	5.5438
RIJN DAEL(AES 256)	30X30	0.0034	5.5440
	60X60	0.0024	5.5439
	100X100	0.0049	5.5438
	300X300	0.0016	5.5439
RC4 (2048)	30X30	0.0024	5.5438
	60X60	0.0026	5.5437
	100X100	0.0034	5.5439
	300X300	0.0034	5.5438

Table: Comparison between algorithms based on different number of blocks

ALGORITHM	KEY SIZE	BLOCK SIZE	ROUNDS
DES	56 BITS	64 BITS	16
3DES	112 BITS OR 168 BITS	64 BITS	48
AES	128 BITS,192 BITS,256 BITS	128 BITS	10,12,14
BLOWWFISH	32-448 BITS	64 BITS	16

Table: Comparison of Des, Aes, 3des, Blowfish

III.GRAPHS OF THE ENCRYPTED/DECRYPTED IMAGES:

Experimental results shows time consumption graphs and throughput of different algorithms based on different text size and blocks

(i)Time Consumption:

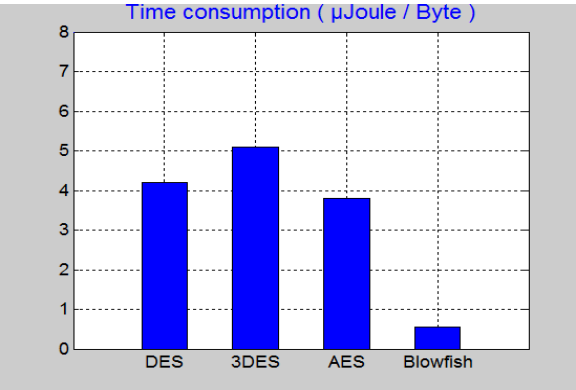

FIGURE:Time consumption graph showing the strength of Algorithms

(ii) Throughput:

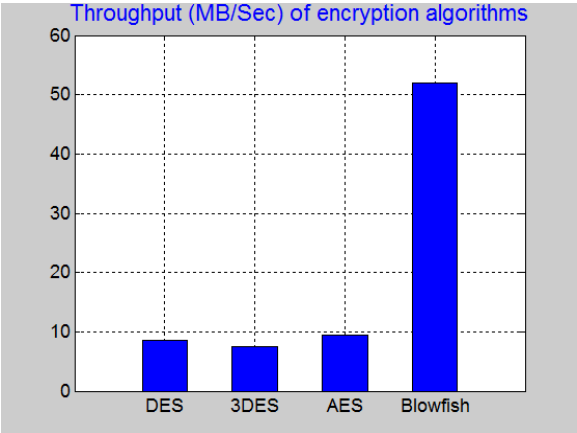

FIGURE:Throughput graph of Algorithms

(IV) CONCLIUSION

Today ,In digital world ,security of confidentail data is more important issue in open networks access.In this paper we surveyed work on different algorithms in cryptography.there are many techniques for securing the imge data .from above description in this paper we conclude that all algorithms are good for image encryption and decryption and have their own advantages and disadvantages, these also gives better performance at their levels so that unauthorized access cannot be occur in secured data.

REFERENCES

[1] Image Encryption and Decryption using blowfish algorithm, World Journal of Science and Technology, Pg: 151-156.
[2] A Modified Approach for Symmetric Key Cryptography based on Blowfish Algorithm, Volume-1, Issue-6, and Pg: 79-82.
[3] A study of New Trends in Blowfish Algorithm, Volume-1, Issue-2, Pg: 321-326.
[4] Privacy and Authentication: An Introduction to Cryptography, proceeding of the IEEE, Volume- 67, Number-3.
[5] Image Security using Encryption based Algorithm, International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP), Pg: 110-112.
[6] A New Encryption Algorithm for Image Cryptosystems, The Journal of Systems and Software, Pg: 83-91.
[7] Introduction to Cryptography, IEEE, Pg: 144-146.
[8] Encryption and Decryption of Digital Image using Color Signal, Volume-9, Number-2, Pg: 588-591.