Performance Analysis on Image Encryption Techniques

[1] Parekh Devangi Sunilkumar, [2] Prof.M. B. Chaudhari
[1] Student, Department of Computer Engineering, GEC, Gandhinagar, India.
[2] Professor, Department of Computer Engineering, GEC, Gandhinagar, India.

Abstract- Due to the rapid growth of digital communication and multimedia application, security becomes a crucial aspect of communication and storage of data as well as images. Encryption of images is one of the well known techniques for secure image transfer. In encryption techniques different algorithm are used like symmetric, Asymmetric and hash function. A number of chaos based algorithm are used rapidly in image encryption. Image encryption algorithms are mostly used in medical science, military applications. In this paper we study some image encryption mechanisms like chaos based algorithm, AES, DES, RSA, Blowfish etc...We aim to frame this paper as literature survey of some image encryption techniques.

General Terms- Image security, image encryption, image processing.

Keyword- Cryptography, Image Encryption, Chaotic , AES,RSA.

I. Introduction

The Internet and information technology are sprouting swiftly. As a result, people are widely using digital media for communication. For instance; image, audio, and video. Images occupy the copious fraction of multimedia. Images play a significant role in communication, for example; military, national-security agencies and diplomatic affairs. Since, these images may carry highly confidential information, so these images entail extreme protection when users amass somewhere over an unreliable repository. Furthermore, when people wish to transfer images over an insecure network, then it becomes crucial to provide an absolute protection. In brief, an image requires protection against various security attacks. The primary intention of keeping images protected is to maintain confidentiality, integrity and authenticity.

Different techniques are available for making images secure and one technique is encryption. Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image, which is usually a reverse execution of the encryption process.

For illustration, Figure 1 represents a primary image; a user operates an encryption technique and produces a secrete image; Figure 2 shows an encrypted image that is the output of an encoding process. On the other hand, when a receiver gets this hidden image, he applies the decryption process and recovers the original information. Figure 3 illustrates the recovered image.

Fig.-1

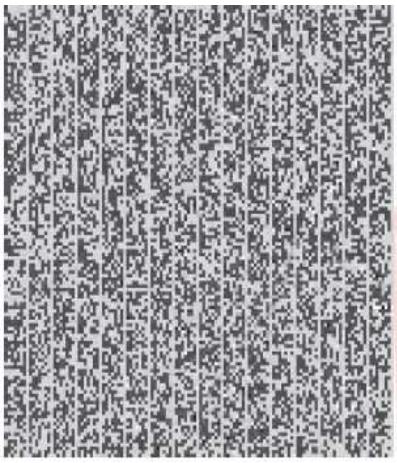

Fig.-2

Fig-3

A digital image can be considered as a two dimensional matrix or a square array of numbers. The elements of this array are called pixels. The value of these pixels are digital numbers and since we can show it as a matrix that each pixel can be denoted by a position as (row, column). By encrypting an image, it is meant to apply a symmetric or asymmetric encryption algorithm on an input image to be converted into a cipher image using either symmetric or asymmetric keys. Symmetric ciphers only use one key for encryption and decryption processes while asymmetric ciphers use two different key pairs (*i.e.*, public and private keys).

An encryption/decryption algorithm is considered as strong while it can resist against most well known attacks such as known-plaintext and cipher text-only attacks . One of the most important topics in exchanging sensitive information over the digital media is to provide security for images. Thus encryption methods are necessary to provide a robust secure environment for both data and images.

II. Literature Review

In this section we are presenting some image encryption algorithm with some experimental parameter. We will also describe their working principals.

A) Chaos base algorithm:

The chaos property describes randomness or unpredictable behaviour for the system. Chaos theory has been established since 1970s by many researchers. Chaos theory has been used for many years in cryptography. The algorithms include image encryption algorithms, hash functions, secure pseudo-random number generators, stream ciphers, watermarking and Steganography are also using chaos based algorithm.

The randomness behaviour is mostly used in cryptographic algorithm.Gernarlly.In cryptography encryption algorithm are there. So as we know in encryption algorithm there are mainly two type of algorithm. Symmetric key algorithm and Asymmetric key algorithm. In symmetric key algorithm same key is used for encryption and decryption. If anyone can predicate the key then whole algorithm will fail. In this case we can use the randomness behaviour of chaotic system.

The basic encryption process for chaotic key based algorithm can be described as follow[2]:

Assume: Size of plain text=M*N, Select 8 bit two keys (key1 and key2) and initial condition is x(0).

Make a chaotic sequence by, $\{x(i)\}^{MN/8-1}_{i=0}$(Assume M N| 8).

Generate a pseudo-random binary sequence by, $\{b(i)\}_{i=0}^{2MN-1}$ from the 16-bit binary representation of x(i) = O.b(16i + O)b(16i + 1) . . b(16i + 15). Once {b(i)} is generated, the encryption process as follows:

For the plain-pixel

f(x,y)(O ≤ x ≤ M – 1, 0 ≤y ≤ N-1), the corresponding cipher-pixel f'(x, y) is determined by the following rule:

$$f'(x,y)= \begin{cases} f(x,y) \text{ XOR keyl}, & b'(x,y)=3 \\ f(x,y) \text{ XNOR keyl}, & b'(x,y)=2 \\ f(x,y) \text{ XNOR key2}, & b'(x,y)=1 \\ f(x,y) \text{ XOR } \mathbf{key2}, & b'(x,y)=\mathbf{0} \end{cases}$$

where b'(x, y) = 2 x b(l) + b(l + **1)** and ***1*** = x * N + y. The decryption procedure is just like the encryption[2].

B) Cryptographic algorithms:

Cryptography, in modern days is considered grouping of three types of algorithms. They are:

1) Symmetric-key algorithms

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys[3]. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Examples of popular symmetric-key algorithms include Twofish, AES, Blowfish, CAST5, Kuznyechik, RC4, DES, and Skipjack. .

We choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data[3]. In symmetric cryptosystems, the longer the key length, the stronger the encryption.

AES is most frequently used encryption algorithm today this algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.

In AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straight related to the length of the key used to secure the communication. AES allows choosing a various type of bits like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.So,we will discussed the AES working principle in detail[3].

AES algorithm:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES)[4]. It is found at least six time faster than triple DES.

The features of AES are as follows

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

1) Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations)[4].

AES consist of following round:

1. Byte Substitution (Sub Bytes)
2. Shift rows
3. Mix Columns
4. Addroundkey

- In Byte substitution round 16 byte input are substituted by fixed table called s-box. The result shows as 4*4 matrixes.
- In this round, each of the four rows of the matrix is shifted to the left.
- Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new byte.
- The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text.

Below fig.-4 shows the whole process (Encryption and decryption) of AES algorithm.

2) Asymmetric-key algorithms

Asymmetrical cryptography is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve (EC), Diffi-Hillman (DH), El Gamal etc.

In Asymmetric key algorithm widely RSA algorithm is used so in next section we briefly discuss about RSA algorithm[5].

The process of RSA algorithm:

RSA cryptosystem uses the mode n, the smallest nonnegative complete the remaining lines of operation, where n is the product of two different primes p and q. RSA algorithm is described as following. First, the generation procedure of keys is as follows,

1) Randomly generates two primes P and Q of length K / 2 bit ;

2) Calculate the public key publicKey=P*Q; (public Key's length is k-bit).

3)Generate a random encryption key keyE, 2<=keyE<= Ø(n)-I, where GCD(keyE, Ø(n))=I;

This is the necessary and sufficient conditions for solvability of the decryption key keyE * keyD mod Ø(n)=I, Ø(n) is known as the Euler function of n, the value is Ø(n)=(P- 1)*(Q l)

4) Calculate the decryption key, keyD=keyE-l mod (n) ,keyE-l is inverse for the decryption key keyD. The formula of the original equation is keyE * keyD mod Ø(n)=1.[5]

Now, the public key, encryption key and decryption key are all created.

Then, the process of encryption of the plaintext and decryption of ciphertext is as follows:

1) Encryption: C = MkeyE mod publicKey; where M is plaintext, C is ciphertext.

2) Decryption: M = CkeyD mod publicKey; in which M plaintext, C is cipher text.

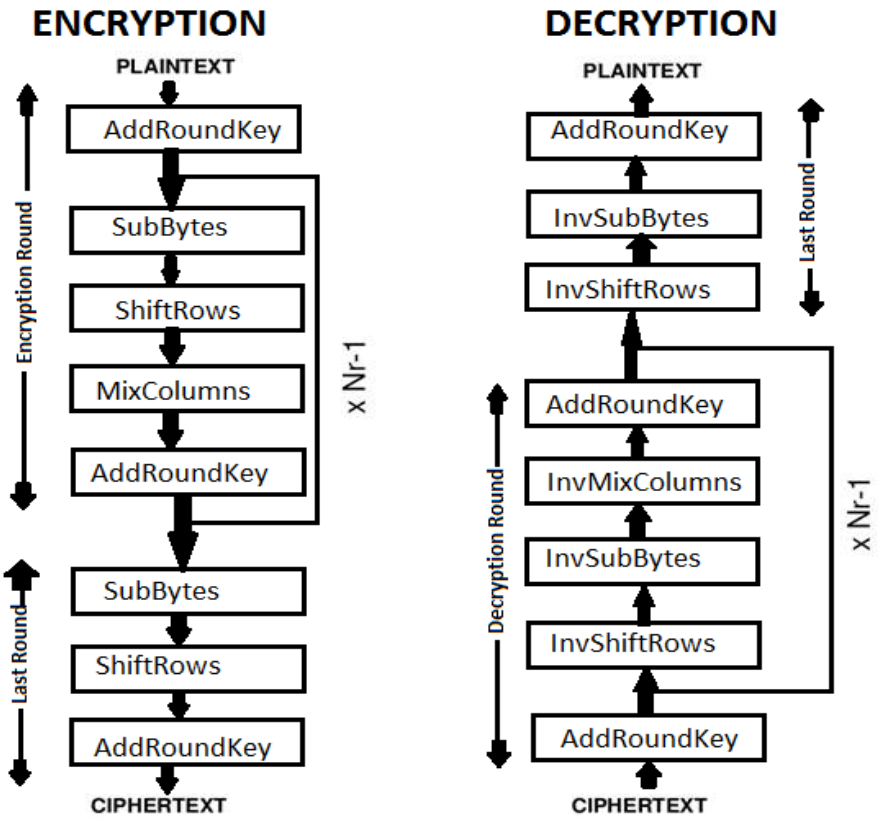

Fig.-4: Process of AES Algorithm

3) Hash functions

The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It contains algorithms like Message Digest, Secure Hash Algorithm.

Hash functions are used as tool to protect the data integrity. Cryptographic hash function mainly used in digital signature schemes. A hash function is any function that can be used to map data of arbitrary size to data of a fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashe[6].

Example of hash function:

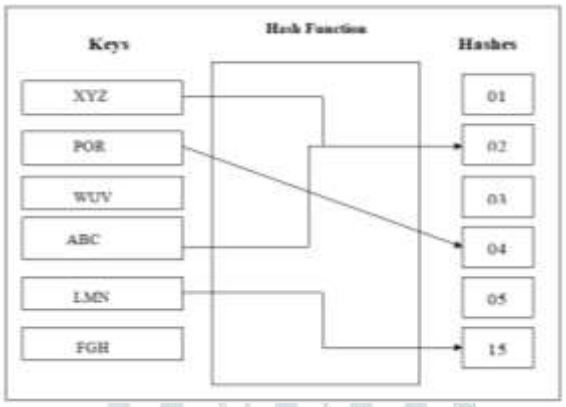

Fig. -5- Hash function.

Above diagram (Fig. -5) show that, A hash function that maps names to integers from 0 to 15. There is a collision between keys "XYZ" and "

Some co re:

- Divisi er: Computes hash value from key using the % operator.
- Truncation of Character/Digit Extraction: It works based on the distribution of digits or characters in the key. More evenly distributed digit positions are extracted and used for hashing purposes.
- Foldir s splitting keys into two or more parts and then c ng the parts to form the hash addresses.
- Mid-S ey squared and the middle part of the result taken a ash value.

Hash function provides only certain security property hence it can be only used for digital signatures, authenticatic ge integrity.

III. Performance evaluation:

In above section we learn about the different type of cryptographic algorithm en also discuss example of each cryptographic algorithm. Now we are going show some performance evaluation of different encryption alg g some parameters.

1) Data Transfer rate

The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time.

The best data transfer rate is DES but the strength of security is weaker than RSA. Because of the difference between key transmission method of symmetric and asymmetric algorithms, Chaos has medium properties between asymmetric and symmetric algorithms.

Cryptographic Methods	Data transfer rate(KBs^{-1})
DES	14185.12
AES	4706.88
Chaos	4087.28
Blowfish	259.33
RSA	23.67

Fig.-6- DTR in KBs^{-1} [7].

2) Key length, Round, speed and security:

The below table gives the comparison of various factors for Symmetric and Asymmetric encryption algorithm. The RSA is asymmetric key algorithm. The remaining methods are belonging to symmetric key algorithm. The asymmetric algorithms are slower then symmetric algorithms. The symmetric algorithm provides better security. Hence, every algorithm has its own advantage and disadvantages.

Factors	RSA	DES	3DES	AES
Created By	Ron Rivest,Adi Shamir and Leonard Adleman In 1978	IBM IN 1975	IBM IN 1978	Vincent Rijmen,Joan Daemen in 2001
Key Length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits(k1,k2 and k3) 112 bits(k1 and k2)	128,192 or 256 bits
Round(s)	1	16	48	10-128 bit key,12-192 bit key,14-256 bit key.
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Very Slow	Fast
Security	Least Secure	Not Secure Enough	Adequate Security	Excellent Security

Fig.- 7: Comparison table[8]

IV. Conclusion

As the objective, this paper presents the comparative performance result between symmetric key cryptography algorithms (Ex: DES, AES and Blowfish), Asymmetric key cryptography algorithms (Ex: RSA) and chaotic based algorithm. In above all type of algorithm the best algorithm are described in detail with diagram. Then the performance evaluation of AES, RSA and chaotic based algorithm described. Mainly the data transfer rate (Speed), security and Key Length factors have been compared for the above mentioned algorithms. From the throughput it is measured, a) DES's data transfer rate is better than AES and chaos. b) Encryption time/speed of symmetric algorithm is better than asymmetric algorithms. c) Security factor of AES algorithm is higher than others.

V. References:

[1] Banavath Dhanalaxmi, Srinivasulu Tadisetty,-"Multimedia Cryptography- A Review" IEEE International Conference on Power, Control, Signals and Instrumentation Engineering,ICPCSI-2017.

[2] Shujun Li I, Xuan Zheng ,-" CRYPTANALYSIS OF A CHAOTIC IMAGE ENCRYPTION METHOD",IEEE,2002.

[3] D. S. Abdul. Elminaam, H. M. Abdul Kader, M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" Communications of the IBIMA Volume 8, 2009.

[4] Sneha Ghoradkar, Aparna Shinde-"Review on Image Encryption and Decryption using AES Algorithm", IJCA ,National Conference on Emerging Trends in Advanced Communication Technologies-2015.

[5] Xin Zhou, Xiaofei Tang, -" Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE,2011.

[6] Edem Swathi, G. Vivek, G. Sandhya Rani, -" Role of Hash Function in Cryptography", IJAERS(Researchgate) ,2016.

[7] Nilar Thein, Hanung Adi Nugroho, Teguh Bharata Adji, I Wayan Mustika,-"Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes", IEEE, 2017.

[8] Gurpreet Singh, Supriya.-" A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[9] Jolly Shah and Dr. Vikas Saxena, -"Performance Study on Image Encryption Schemes",IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[10] Manju Kumari . Shailender Gupta . Pranshul Sardana,- "A Survey of Image Encryption Algorithms", Springer Nature 2017.

[10] Omar Farook Mohammad, Mohd Shafry Mohd Rahim,Subhi Rafeeq Mohammed Zeebaree,Falah Y.H. Ahmed, -"A Survey and Analysis of the Image Encryption Methods",international Journal of Applied Engineering Research,Volume 12,December 2017.

[11] Das, P. K., Kumar, M. P., & Sreenivasulu, M.-"Image Cryptography: A Survey towards its Growth". Advance in Electronic and Electric Engineering, 4(2), 179-184,-2014.