Comparative Study Of Efficient Data Hiding Techniques

Lalan kumar¹, Deepanjali Mishra¹, Ayush Kumar³, Amit Kumar⁴, Ashish Bajpai⁵

¹Asst.Professor,Dept. of Master of Computer Application,G.L.Bajaj Institute of Technology and Management,Gr.Noida,UP,India
²,³Scholar,Dept. of Master of Computer Application,G.L.Bajaj Institute of Technology and Management,Gr.Noida,UP,India
⁴Asst.Professor,Dept. of Master of Computer Application,KIET Group of Institutions,Ghaziabad,UP,India
⁵Asst.Professor,Dept. of Computer Science,KIET Group of Institutions,Ghaziabad,UP,India

Email: lalankumar100@gmail.com, deepanjali.mishra110@gmail.com, ayushkumar.aptech@gmail.com, amit.kumar.mca@kiet.edu, ashish.bajpai@kiet.edu

Abstract. Data security is one of the fundamental concerns when it comes to modern networking and information sharing as any breach or data loss can end up causing major losses in terms of credibility, personal data and/or law suites. This paper studies data encryption and decryption techniques using algorithms like DES algorithm, 3 DES algorithm, AES algorithm and RSA algorithm. Cryptography was introduced for data security while transmitting data. However, only cryptography cannot give a robust security approach; as a result, a disorganized message can still be snooped [9]. This leads to a desire for information security. There are several techniques available, among those have taken a few of them and will review them considering cryptography measures. We will analyse the algorithm mentioned above, and try to find out better among them.

Keywords: Cryptography, Stream Cipher, Block Cipher, AES Algorithm, DES, 3DES, RSA.

1. Introduction

Cryptography is a technique of secure communication over a network. Cryptography is constructing rules and regulations to secure our data in transmission and prevent it from third party access. In the modern era, cryptography is synonymous with “Encryption” [2]. Cryptography is one of the ways in which we can approach data security. Currently, we've many secure strategies for cryptography. These techniques can be employed to hide digital information in the form of audio or visual signals that is in the form audio, still pictures or moving pictures which are in turn a collection of a number of pictures like GIF or a video.[6] The approach is to employ all of them alongside additional security levels and to stimulate a significantly secure system for masking information. The primary focus of this research
is to review algorithms and to figure out more efficient algorithms which can hide sensitive data and text by means of cryptographic techniques [11]. The performance of an algorithm is measured in terms of various attributes like payload capability, stress taking power, time complexity, security as well as visual capability and quality.

2. Cryptography

Cryptographic techniques can be employed to encrypt information in such a way that it can only be decrypted by using the generated key, hence only the original owner or the person who holds the key can access the information. This, in turn, makes it more secure and provides data authenticity.[5] Cryptographic techniques have a huge role in maintaining data security, integrity, authenticity and confidentiality. There is a constant threat of data getting tampered either intentionally or unintentionally, some cryptographic techniques can be employed to detect any tampering that has happened to data after the transfer [12]. Cryptography can be done in many ways, either by a traditional approach or by a modern approach. Cryptography can be classified as an art of secret writing. Cryptography scrambles data into intangible form during transmission, to prevent it from unauthorized access [15]. Classification of cryptographic techniques are mentioned below-

2.1 Types of cryptography

The traditional approach makes use of the same key to cypher as well as decipher the text; it can be done by two methods.

2.1.1 Substitution method [2]: -
In the substitution method, one alphabet is substituted by another. For example

Original text - "HOTEL"
Cipher (Encrypted) text- "GNSDK"

In the above example, plain text alphabets get substituted by its preceding alphabet.

2.1.2 Transposition method [2]: -

In this method letters of the word got shuffled. For example: -

Original text- "HOTEL"
Cypher (Encrypted) text - "LETOH"

This approach sends the secret key over the compromised channels. Later, Modern cryptography came into existence to increase the security level. In the modern approach, encoding and decoding are done by using different keys which are known as the public and private keys. It can directly manipulate the data. It is also done in two ways.

2.1.3 Symmetric Cryptography [2]: -

In this approach the same key is used by the sender as well as receiver to encode and decode data respectively. It can be employed to maintain the confidentiality of the information by means of
encoding and decoding. It makes use of the same approach in both directions. It is known to be the
fastest technique for cryptography. *Another name for this approach is Private Key cryptography.*

### 2.1.4 Asymmetric Cryptography [2]: -

In this approach, a pair of different keys are used to encode and decode and to communicate between
sender and receiver. Another term that we can use to address Asymmetric cryptography is Public Key
Cryptography. Any information that is encrypted using Asymmetric cryptography using one type of
key can only be decoded by employing the other type of the key.

![Figure 1. Types of Cryptography](image)

#### 2.2 AES algorithmic rule for Cryptography

AES stands for Advanced Encryption Standard. It was originally named as Rijndael algorithmic rule, a
radially symmetrical block cypher that uses method information. It is widely adopted for symmetric
cryptography. The input and output sequences have a fixed length of input, output, and therefore each
bit sequence containing the cypher key 128, 192 or 256 bits for the Rijndael area unit [4]. Generally,
the ciphertext length can be of any of the above mentioned three values except for Advanced
Cryptography Normal (AES). The only allowed length is 128 [3]. This encryption works on a single
block at a time. The AES algorithm is a mathematical description of hiding data and making it secure.
AES is nearly six times faster than DES [13]. This algorithm belongs to Symmetric cryptography as it
employs the same key for encryption as well as decryption. The AES algorithmic rule comprises
various groups of process steps for a wide number of iterations, these steps are also known as rounds
[7].

**Sub-Byte:** There is a substitute for every single memory unit within the substitution box.

**Shift-Row:** Each byte in the last three tuples area unit is shifted left to another range of offsets.
Mix Column: every column is increased by a renowned matrix. Product of that with one implies that exploit unchanged, by two implies that the computer memory unit has been shifted towards the left and by three implies that the computer memory unit has been shifted towards the left then activity XORing with the early un-shifted price.

Add-Round-Key: XORing with particular information and therefore the subkey. In resultant spherical, there exists no merged Column step. It takes ten rounds for these stages to complete. In turn, it becomes troublesome for the wrongdoer to get any data concerning the starting content from the encrypted image.

2.3 Security style

Security [3] is the main concern. So that we can prevent our data by some unauthorized access and provide it with authenticity. Our style can be subdivided into two different modules [3].

1. Crypt Module
2. Decrypt Module

2.4 HIDING THE TEXT

2.4.1 Crypt Module:
In the Crypt Module, the following steps are taken into consideration for encryption.[8]

1. Insertion of text for encoding [8]
2. Implement the AES algorithm using 128 bits key (key 1) [8]
3. A well hexadecimal cypher text is formed [8]

2.4.1.1 Data Extraction

2.4.2 Decrypt Module

This employs inverse AES to decrypt the encrypted data. The data is encrypted by AES cryptography. The steps square measure Add-Round-key, inverse sub byte victimization inverse Substitution-box, inverse shift-row wherever the bits square measure is shifted towards right in a cyclic fashion, inverse mix-column step victimization reverse Permutation-box, and Add-Round-key [1]. The constituent values of each block are found in the form of collections[8], then for each block, if the worth of this value is higher when compared to the edge worth then the data is encrypted in the block and is then extracted by Xor-ing the initial bits and the bits recovered after the decryption. Finally, the extracted bits are then merged to get the key knowledge, as well as the recovered data, is then collected to create the initial data.

3. Data Encryption Standard (DES)
DES is a 64-bits block cipher technique by Horst Feistel. As it uses Symmetric-key encryption. This implies that both the sender as well as the receiver need to have the information of the key to be able to access the data. This technique became the first technique to be ever approved by the United States Government of public disclosure. In DES algorithm 56 bits are used for encoding and decoding and while the remaining eight bits are used to make sure the data hasn’t tampered during transmission (These bits are employed for parity bit checking).

![DES Encryption Diagram](image)

*Figure 3. DES Encryption*

Each of the 64 bits blocks of data is encrypted by completing sixteen different rounds of encryption. Data encryption works 8 bits (one octet) are used to do parity check for error identification and to check key’s integrity. As DES actually used 56 bits so according to permutation calculation it would take a maximum of 256 tries to find the correct key. At one time DES was a predominant algorithm but now it became outdated as it uses symmetric key encryption and decryption.

4. DES – Triple Data Encryption Algorithm

This is an upgraded version of DES. Although it uses the algorithm it provides more protected encryption. It was first published in 1995[10]. Triple DES provides protection against such attacks. Triple DES is also known as T-DES. The simple DES encryption algorithm is employed by the T-DES algorithm with thrice the enhanced security of encrypted text [14].
5. Triple DES Structure

This approach encrypts the same data twice as many times by employing DES. In turn, the encryptions are more resistant against interruptions. Triple des encrypts its blocks of information in forty-eight cycles which is thrice as much compared to DES and It also has a key period of 168 bits. Sixty-four bits are employed by T-DES for encryption [10]. It uses 3 precise keys k1, k2, k3 (all are fifty-six bits).

It provides adequate security for encryption

Cipher text =EK3(DK2(EK1(plaintext)))
It means EK3=encryption with k3
DK2=decryption with K2
Ek1=encryption with k1

For Decryption
Plain Text=DK1(EK2(DK3(ciphertext)))
It means DK3=Decryption with k3
EK2=encryption with K2
Dk1=Decryption with k1

6. RSA Algorithm stands for (Rivest-Shamir-Adleman Algorithm)

RSA came into existence in 1977. This algorithm Asymmetric cryptography. This algorithm makes use of two different keys for encryption as well as decryption that is the public key for the encryption and a private key for the decryption. This private key is called a secret key. RSA is a four-step algorithm, these four steps areas:
1. Generation of the given keys
2. The decryption of the given keys
3. Encrypting the given data.
4. Decrypting the given key.

6.1 Key generation

1. Two prime numbers a and b are selected
2. Calculate \( n = a \times b \)
3. Calculate \( \varphi(n) = (a - 1) \times (b - 1) \)
4. Select e in a way that $1 < e < \phi(n)$ and e and n are co-prime.
5. By keeping in mind the formula $(d \times e) \mod \phi(n) = 1$, the value of d is calculated.

6.2 Key distribution
The receiver sends its public key to the sender after mutual concern by a reliable or not the secret medium
- The public key $(e, n)$
- Receiver also has its private key which is never distributed.
- Secret Key $(d, n)$

6.3 Encryption
$C = m^e \mod n$ and decryption $m = cd \mod n$

6.4 Decryption
$C^d = (m^e)^d = m \mod n$

We have studied 4 algorithms now we compare these algorithms to find out which is more effective and efficient.

**Table 1. Comparison table**

| PARAMETER | DES | Triple DES | RSA | AES |
|-----------|-----|------------|-----|-----|
| Origin of algorithm | It originated in 1970 by IBM and was published in 1977. | Triple DES came into existence in 1995 | Ron Rivest, Shamir & Leonard Adleman in 1978 | In year 2001 on November 26 by Vincent Rijmen and Joan Daemen |
| Block Size | 64-bit | 4-bit | Variable block size | 128bit, 192bit, 256bit |
| Rounds | 16 rounds | 48 rounds | 1 round | 10, 12, 14 rounds |
| Possible keys | $2^{56}$ (56 is usable bits) | $2^{112}$ | Variable possibilities | $2^{128}, 2^{192}, 2^{256}$ |
| Encryption speed | Very slow (3 times of DES) | Slower than AES | Faster |
| Security | Less secure | One and only problem in . | Least secure | Much secure |
| Cryptanalysis Resistance | It is not immune to differential | Vulnerable to differential, Any attacker with malicious intentions can access the data by using a brute force attack. | It is susceptible to attacks like brute force attack and the timing | It is immune to differential |
Encryption

Primitive

Substitution, permutation
Substitution, permutation
Mathematical functions
Substitution, shift, bit mixing

Hardware and Software Implementation

Implementation is better in hardware than software.
Software implementation accomplished
Not efficient
Better in both

Algorithm Structure

Feistel Network
Feistel Network
Asymmetric Cryptosystem
Feistel Network

Attacks

Brute Force attacks
Key attacks
Brute force attack, timing attack
Side Channel Attacks

Flexibility

Low
Known for its flexibility
High
High

7. CONCLUSION

In this comparative study, we have studied four encryption algorithms and analysed them. We have found that every technique has its own strength. We have reached to a conclusion every algorithm depends upon its key management, type of encryption and decryption, block size, possible keys, encryption speed. Power consumption is directly proportional to key length and data length that is why short data length is advisable. All the algorithms perform some mathematical operations on keys. More numbers of keys have more bits which lead to increased encryption time. From the above analysis, we observed that the AES algorithm is better among these four in terms of security, speed of encryption. So, this review we have concluded that the AES encryption algorithm is the best among the algorithms that have been studied in this study. This algorithm is more secure and faster. However, this algorithm still has a wide scope of improvement.

REFERENCES

[1] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .
[2] William Stallings:” Cryptography and network Security: Principles and Practices”
[3]Advance Encryption Standard, [Online], Available:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[4] M. M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, and M. Z. I. Shamsuddin, “Information Hiding using Steganography”, IEEE 0-7803-7773-March 7, 2003

[5] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton.

[6] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to Steganography. IEEE SECURITY & PRIVACY

[7] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, 1996

[8] Dr. Bhushan Kapoor, Dr. Pramod Pandya, in Cyber Security and IT Infrastructure Protection, 2014

[9] W. Stallings, "Cryptography and Network Security: Principles and Practice", (1999), Prentice-Hall, New Jersey.

[10] A Review and Comparative Analysis of Various Encryption Algorithms by Rajdeep Bhanot1 and Rahul Hans2

[11] Behrouz A Forouzan, Debdeep Mukhopadhayay “Cryptography and network security “

[12] Cryptography by Solie Tech

[13] Modern cryptography: Theory and practices by Mao 2004 edition

[14] An Introduction to Cryptography Mohamed Barakat, Christian Eder, Timo Hanke September 20, 2018

[15] Lecture Notes on Cryptography (S. Goldwasser and M. Bellare)