January-February 2020
ISSN: 0193-4120Page No. 6682- 6685

Provision of Security to Images using Triple Des Algorithm

Chow dam Bhavan[1], Sashi Rekha[2]
[1]Department of Computer Science and Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
[2]Associate Professor, Department of Computer Science and Engineering, Saveetha School of Engineering Saveetha Institute of Medical and Technical Sciences, Chennai, India
[1]Chowdambhavana@Gmail.Com, [2]Sashirekhak.Sse@Saveetha.Com

Article Info
Volume 82
Page Number: 6682 - 6685
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 01 February 2020*

Abstract
In the present world with the quick improvement of different media innovations, increasingly more sight and information are being created and transmitted in different formats like text, audio, video, images etc. And furthermore, there are security issues during the exchange of these secret media documents. It turns out to be a lot simpler to alter, adjust and copy the unique data. The digital data is anything but easy to duplicate and circulate, therefore security and privacy of these multimedia file i.e., an image, is a significant issue in the cutting edge world, and furthermore it has gotten an important to locate the suitable assurance techniques in order to guarantee the information trustworthiness and provide data integrity. Hence to provide security to these files, Cryptography algorithms are used. The algorithms used are DES and TRIPLE DES and the performance of the algorithms are compared for better protection to the files.

Key Words: Cryptography, DES, Triple DES, Security

1. Introduction

Cryptography is a procedure of encoding and decoding information to shield it from unfortunate individuals like hackers by renovating it into a format non recognizable by its assailants during data transmission. Cryptography essentially is the hiding the information present in the data, similar to content, picture, sound, video so forward to make the information misty, imperceptible or indiscernible all through transmission or capacity known as secret composing or secret writing. The most objective of cryptography is keeping data secure from unapproved aggressors. Some of the most common cryptographic algorithms used are AES, DES, SHA, MD5, etc...

Every algorithmic rule has its own blessings and problems. If an image is applied with DES algorithm, first it changes over the pictures into bytes of information and afterward the bytes are changed over into bits of information The 64-bit byte code is then iterated utilizing the initial and final permutations. The outcome will be as bits which is inclined to both brute force attack and analytical attack. To keep away from this attack, the Triple DES algorithm is utilized.

For the encryption procedure it at first encrypts the information utilizing only one key and afterward decrypts the information utilizing another distinctive key and afterward at long last encrypts the information again utilizing another key. For the decryption procedure it is the turnaround of the encryption procedure it at first

January-February 2020
ISSN: 0193-4120Page No. 6682- 6685

decrypts the figure information utilizing one key, at that point encrypts the information utilizing another key and afterward at last decrypting the information back to its unique structure utilizing another diverse key. Using DES, the security provided to the images is reliable but use of Triple DES algorithm makes the Images Secure as it takes 3 keys to encrypt and decrypt the image. The DES algorithm uses 64, 56, bit keys depending upon the usage.

2. Objective

The main objective is to provide security to the multimedia file which is an image using Triple DES algorithm. The objectives to be satisfied are

- **Authentication:** Authentication means identifying each other that is the sender and receiver confirm that they are the right parties that has to send and receive the data.
- **Secrecy or Confidentiality:** Ensures that the information send over the internet or through any other process, is safe from any attackers
- **Integrity:** Ensures that the data is unchanged while sending it over the internet and no modification of the data is being done by unauthorized users or hackers
- **Non-Repudiation:** It means that the sender cannot deny the fact that he/she is responsible for the data sent to the receiver.
- **Service Reliability and Availability:** Involves the availability of the service provided to the customer 24/7.

3. Existing System

AES (Advanced Encryption Standard):

Advanced Encryption Standard is a symmetric-key block cipher that utilizes keys of 128, 192, and 256 bits, and encrypted and decrypted information in blocks of 128 bits (16 bytes). A Public-key cipher utilizes a blend of keys. For the information being provided to the system, symmetric key ciphers utilize a key similar to that of public key cipher to encrypt and decrypt. The AES algorithm will turn into the verifiable standard for encrypting a wide range of electronic data, replacing DES. Information encrypted by AES is unbreakable from inside the feeling that famous cryptography attack will rework the AES cipher text while not utilizing a brute force search through all feasible 256 piece keys. Famous applications like WhatsApp use the AES algorithmic rule in 128 bytes in conjunction with SHA.

Symmetric Encryption:

Concealing the data with one key is symmetric. One among the most ideal manners by which to attempt to do cryptography is through symmetric cryptography. Here, a letter or differ concurs with another letter or range inside the cryptography code. We will take any composed information or data and substitute letters and numbers for their coded partner, as an outcome encryption of the content or the information provided occurs. And utilizing a comparable system, the principal content is shaped back with a comparable key.

Asymmetric Encryption: Asymmetric cryptography might be a comfortable and smooth way which will be suitable to encode information that you essentially will be accepting. It's customarily done electronically. A public secret key is offered out to whomever you wish. They're ready to encrypt data with the use of the key and send it to you. That is normally completed once composing messages or emails. This means encryption of the information with the general public key, it will simplest be scan by decrypting with the personal key has.

4. Proposed System

Utilizing Triple DES despite the fact that it runs multiple times more slow than DES, yet is substantially more secure whenever utilized appropriately. The methodology for decrypting something is equivalent to the technique for encryption, with the exception of it is executed backward i.e. is in reverse direction. In DES, information that is provided to the algorithm is encrypted and decrypted in 64 - bit chunks. The information key for DES is 64 bits in length; the real key utilized by DES is just 56 bits long. The slightest significant (right-most) piece in every byte is a parity bit, and ought to be set such that there are constantly an odd number of 1s in each byte. Just the seven most noteworthy bits or the significant bits of every byte are utilized as these parity bits are disregarded, bringing about a key length of 56 bits. This implies the viable key quality for Triple DES is really 168 bits in light of the fact that every one of the three keys contains 8 equality bits that are not utilized during the encryption procedure.

TEST Engineering & Management

January-February 2020
ISSN: 0193-4120Page No. 6682- 6685

System Architecture

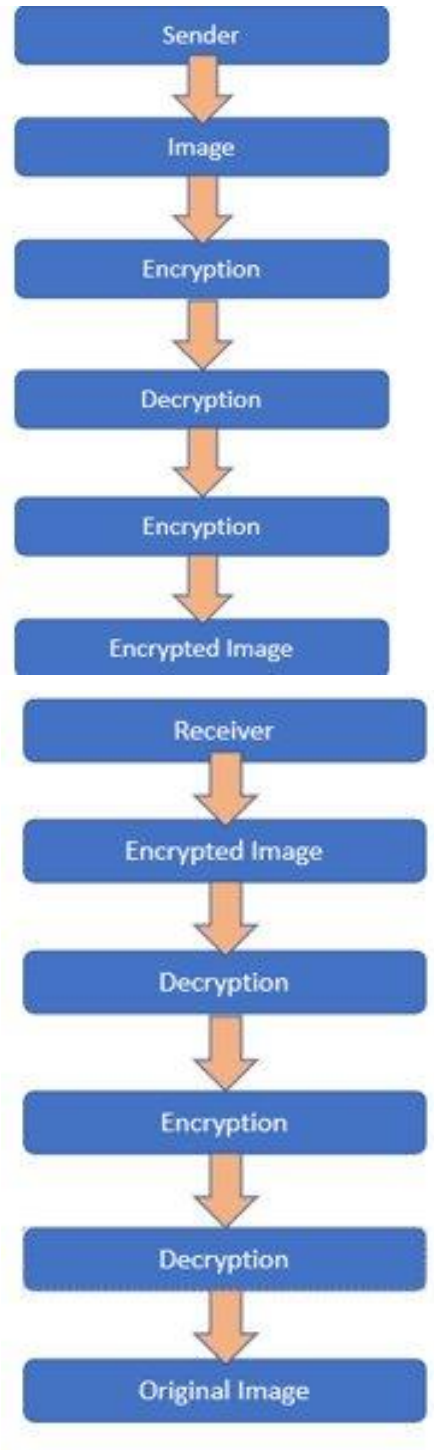

Figure 1: System Architecture

5. Methodology

Use of Triple DES algorithm while sending the media files over the internet. Comparison of the performance of the DES and the triple DES algorithm includes the implementation of the DES algorithm and Triple DES, which encrypts the image to an invalid image format. DES algorithm uses 64-bytes to convert mage into bytes using an 8 bit key to encrypt and decrypt. Similarly Triple DES is the process of using DES 3 times. Triple DES Encryption includes EDE form and Decryption includes DED form that is, E stands for Encryption and D stands for Decryption. Usage of same Key while Encrypting and Decryption.

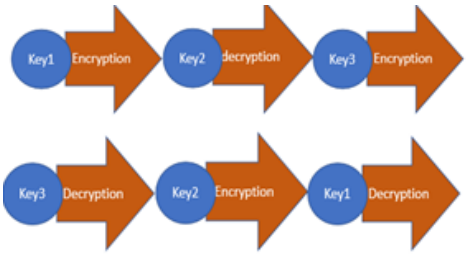

Figure 2: Triple DES Algorithm

The above Figure 2 as appeared in Triple Data Encryption Standard (DES) is a sort of cryptography technique which uses block cipher algorithm. Here the block cipher algorithms are used thrice to every datum block. The key size is expanded in Triple DES to guarantee extra security through encryption abilities. Each square contains 64 bits of information. Three keys are alluded to as pack keys with 56 bits for each key. There are three entering alternatives in information encryption measures:

- Independent keys or free keys
- Among the three keys, key 1 and key 2 be the independent keys
- Each of the keys is different and identical

The usage of different keys to encrypt makes the process of encryption slow, but the security provided saves the file from it's attackers. If the keys used to encrypt are same the time taken can be reduced but it is not efficient as the usage of different keys.

6. Result

Includes the implementation of DES algorithm successfully to encrypt an image. The Security provided is Secure and the performance of the system is measured. In this, the encrypted image has to be used to decrypt with the same key. The Encrypted and the Decrypted images are stored in the bin of the java application. This process can be integrated in the different software to provide security. along with the encrypted image the key has to be sent to the receiver to decrypt the file at the sender's side. This can reduce the attacks on the confidential information that has been sent over internet.

January-February 2020
ISSN: 0193-4120Page No. 6682- 6685

Figure 3: Encrypted Image

Figure 4: Decrypted Image

7. Conclusion

Due to a boom within the technology, the utilization of emails and transfer of knowledge over the web has magnified loads. Because of this, there's increase in hacking the users' info and intrusion attacks. This have an effect on the information confidentiality, therefore there's a necessity to secure the users knowledge being transferred over the web. Triple-Des shall give a higher-quality cryptography method wherever des provides better performance in cryptography and secret writing method. This turns into a major imperfection when we are running various procedures over a system. It must be ensured that information or the picture being moved between the sender and the beneficiary ought not be show to both the sender and collectors. The time will be expanded for Triple-DES process the future work would likewise concern the better confirmation of value and execution for a wide range of interactive media information. The future work would include encryption of videos and sound records, with a cross foundation using various cryptographic algorithms.

Reference

[1] Aamer Nadeem, "A Performance Comparison of Data Encryption Algorithm," IEEE 2005.

[2] Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1.

[3] Aman Kumar, Sudesh Jakhar, Sunil Maakar, "Distinction between Secret key and Public key Cryptography with existing Glitches", Volume: 1, 2012.

[4] Data Encryption Standard (DES), FIPS PUB 46-3 - 1999.

[5] Feistel, Cryptography and Computer Privacy, Scientific American, Volume: 28, No.5, 1973.

[6] Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.

[7] Aliza Sarlan, "To propose prediction analysis algorithm based on k-means and SVM Classification," IIRJET, vol. 4, no. 1 cs. 13-17. Sept 2018.

[8] Hussain A., Surendar A., Clementking A., Kanagarajan S., Ilyashenko L.K. (2019). Rock Brittleness Prediction Through Two Optimization Algorithms Namely Particle Swarm Optimization And Imperialism Competitive Algorithm. Engineering with Computers. Vol 35. Issue 3. Page 1027-1035