FIANZA: The Secure Data Transfer

Hardik Thakkar
Shah & Anchor Kutchhi Polytechnic.
Mumbai, India.
hthakkar8@gmail.com

Viraj Chheda
Shah & Anchor Kutchhi Polytechnic.
Mumbai, India.
chhedavd@gmail.com

Yash Bhanushali
Shah & Anchor Kutchhi Polytechnic.
Mumbai, India.
yashbhadra@gmail.com

Mrs. Jyoti Bansode
Shah & Anchor Kutchhi Polytechnic.
Mumbai, India.
jyoti.bansode@sakp.ac.in

***Abstract*:**-Ever since humans started to communicate via written word, a need was felt that could keep our data away from prying eyes. However at first as the number of people who could read, there was no need to encode our data. As the number of people who could read increased so did the opponents who could read, thus need for security was felt while communicating. This need lead to rise of cryptography as well as steganography. These methods have evolved with time and are still relevant. However with increase in computing power, only a single layer of security is not enough to keep our data secure. To keep our confidentiality intact, we can use the existing algorithms for cryptography and steganography to keep the data in such a way that it cannot be accessed or read by unauthorized persons. In this paper, we have proposed a system to utilize cryptography algorithm and a steganography algorithm and combine them to achieve our goal of maintaining confidentiality and privacy.

Keywords:*-Cryptography , Steganography , Data Security, DES.*

*****

I. INTRODUCTION

As we move towards the era where everything is online and interconnected, the very fundamental right of data privacy is being compromised. Further confidentiality is lost in a number of ways, in some cases the data sender and receiver may not even realize that they are not the only ones who can see the data which was communicated. It is important that data is kept secure and the nature of communication should not be known to anyone outside the intended receivers. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect military messages, E-mails, credit card information, corporate data, personal files, etc. [1]

Cryptography is essentially a method of converting the data from its normal understandable form to a form which is non-understandable without secret knowledge. The data in its non-understandable form is called cipher text. Only those who have the secret key or passphrase, can covert the cipher text back to understandable form which is also known as plain text.

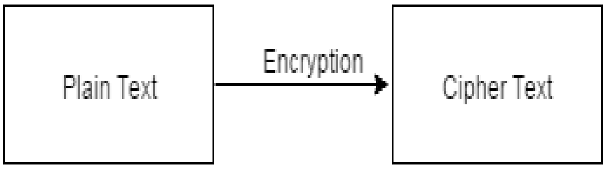

Figure 1. Cryptography Flow for Encryption

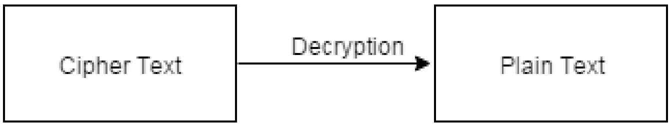

Figure 2. Cryptography Flow for Decryption

Steganography is the art of hiding data within a carrier file of some sort. Steganography hides the very existence of the real communication and instead the eavesdropper will only see the cover file being transmitted. The cover file can be of numerous types, how the data will be hidden depends on which type of steganography is used. For example, in image steganography, the image is interpreted as a stream of bits and the bits are manipulated to hide the data while in audio steganography, the data is hidden by modifying audio signals.

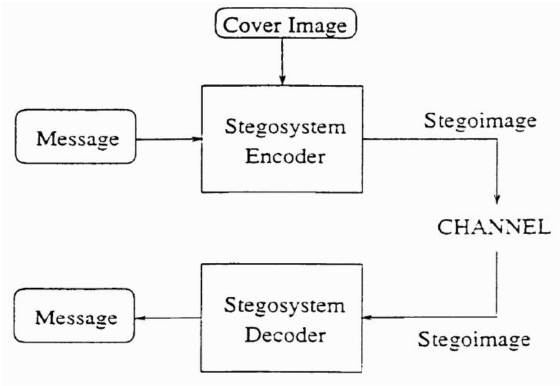

Figure 3. Image Steganography Flow [1]

However with the amount of processing power available and numerous ways in which privacy is compromised just using one of the aforementioned methods is not enough. Hence it is necessary to use a combination of these two methods to provide unbreakable security. The cryptography algorithms and steganography algorithms can be used in tandem to achieve this goal.

LITERARY SURVEY

However with the amount of processing power available and numerous ways in which privacy is compromised just using one of the aforementioned methods is not enough. Hence it is necessary to use a combination of these two methods to provide unbreakable security. The cryptography algorithms and steganography algorithms can be used in tandem to achieve this goal.

II. LITERATURE SURVEY

To get an air tight system, it is necessary to ensure that the algorithms chosen are very strong and give the desired results. There are numerous cryptography and stegnography algorithms are now available for use according to requirements of the one who is implementing the system.

2.1 Cryptographic Algorithms

Four of the most famous algorithms for cryptography are AES, 3DES, DES, Blowfish.

2.1.1 Advanced Encryption Standard (AES)

The AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen [4]. It was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001[5]. The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption. In AES encryption the block is 128 bits or 16 bytes, in length. The term “rounds” refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key. AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm[6].

2.1.2 Data Encryption Standard (DES)[7]

The DES is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data . Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

1. Expansion: the 32-bit half-block is expanded to 48 bits using the expansion permutation, denoted E in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 * 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.

2. Key mixing: the result is combined with a sub key using an XOR operation. Sixteen 48-bit sub keys—one for each round—are derived from the main key using the key schedule (described below).

3. Substitution: after mixing in the sub key, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES—without them, the cipher would be linear, and trivially breakable.

4. Permutation: finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box. This is designed so that, after permutation, each S-box's output bits are spread across four different S boxes in the next round.

2.1.3 Triple DES [8]

In cryptography Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:

1. All keys being independent
2. Key 1 and Key 2 being independent keys
3. All three keys being identical

The triple DES key length contains 168 bits but the key security falls to 112 bits.Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys

1. Encryption using the first secret key
2. Decryption using the second secret key
3. Encryption using the third secret key

2.1.4 Blowfish[12]

Blowfish is a symmetric block cipher that takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is a block cipher that encrypts data in 8-byte blocks. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a variable-length key of at most 56 bytes into several subkey arrays totaling 4168 byte. Blowfish has 16 rounds. Each round consists of a key-dependent permutation, and a key and data dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Given below is a comparison of these algorithms in relation to time required and the size of data.

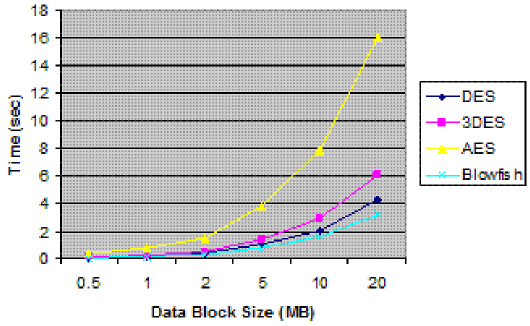

Figure 4. Comparison Chart of Cryptography Algorithms [2]

After studying the differences, it is clear that 3DES is best choice for our application as it requires less time for large files and also it provides a very high security cover from attacks. While blowfish may seem the clear winner from the comparison, it is relatively new algorithm and there is a chance that a few unseen security flaws may come to fore in the future.

2.2 Stegnography Algorithm

Mutiple options are also available in the Stegnography Algorithms. Some of them are LSB, DCT, DWT.

2.2.1 Least Significant Bit Algorithm[9]

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. In this work, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR) The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same

2.2.2 DCT[10]

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the data is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the watermark in a middle frequency band does not scatter the information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted.

2.2.3 DWT[11]

The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science.DWT performs wavelet analysis, it is is advantageous as it performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

For the steganography algorithm, the below comparison of algorithms was studied:

Table 1: Parameters analysis of steganography Methods [3]

Features	LSB	DCT	DWT
Invisibility	Low	High	High
Payload capacity	High	Medium	Low
Robustness against image manipulation	Low	Medium	High
PSNR	Medium	High	Low
MSE	Medium	Low	High

From above table it can be deduced that LSB algorithm provides the most consistent performance throughout all parameters. Also the payload capacity is higher than most algorithms.

3DES and LSB Algorithms provide the most consistent performance in their respective categories and hence a combination of these two algorithms is suitable while combining stegnography and cryptography principles.

III. PROPOSED SYSTEM

In this proposed system when we need to transfer data from source to destination, we need provide security by the combination of Encryption and Stegnography. During Encryption, the text and key which will be provided and the encrypted text will be generated. Further this encrypted text and an image will be provided to stegnography mechanism. As a result, stegoed image will be generated. During Decryption, generated stegoed Image will be provided to the steganalysis, and the encrypted text will generated. This encrypted text and key will help the decryption mechanism to generate decrypted text or plain text.

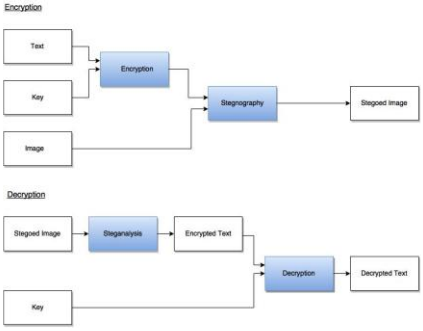

Figure 5. System Architecture

3.1 Modules

3.1.1 Encryption

Step 1: Accept the data to be encrypted from user and the corresponding keys from user.
Step 2: Encrypt the user data using Triple DES algorithm for encryption.
Step 3: Accept the image from user in which data will be hidden.
Step 4: Hide the data in image using Least Significant Bit algorithm for steganography.
Step 5: Save the image after steganography process.

3.1.2 Decryption

Step 1: Accept the image from user.
Step 2: Unhide the data from image using Least Significant Bit algorithm for steganography.
Step 3: Accept the key from user.
Step 4: Decrypt the data using Triple DES algorithm for decryption.
Step 5: Show to user, the decrypted data.

3.1.3 Stegnography

Step 1: Convert cover image to streams of binary bits.
Step 2: Convert each character of the secret message to ASCII value.
Step 3: Use two adjacent bits to hide one character.
Step 3.1: Convert the ASCII value of character to 4-bit number
Step 3.2: AND the upper values of image binary and ASCII value.
Step 3.3: AND the lower values of image binary and ASCII value.

3.1.4 Steganalysis

Step 1: Take two adjacent pixels from the stegoed image.
Step 2: Shift the first pixel by 4 to right.
Step 3: Perform AND operation with 15 to the second pixel
Step 4: ADD the result of step 2 and 3 together.

IV. CONCLUSION

The proposed implementation of Fianza- The Secure Data Transfer provide high-speed performance with very compact software implementation. Analysis and survey done for our project which is presented here shows that Fianza will establish a highly impenetrable layer of security which will provide data security and privacy for the foreseeable future. It will provide an inclusive package for all the security needs of the client as two robust tools of cryptography and steganography are included in one software.

V. FUTURE WORK

Some additional features can be introduced in future to make it even more versatile. In future a host of new algorithms can be introduced to make Fianza more user friendly by giving user the choice of algorithms. A few candidates for cryptography are AES, Blowfish, RSA etc while Blind Hide, BattleSteg can be used for Steganography. Browser plugins, mobile apps can be introduced to take Fianza to multiple platforms which will truly make it versatile and the give user a larger freedom.

REFERENCES

[1] ”Two new approaches for secured image steganography using cryptographic techniques & type conversions” by Sujay Narayana and Gaurav Prasad published at Signal and Image processing: an international journal(SIPIJ) Volume 1, No.2 December 2010.

[2] http://www.cse.wustl.edu/~jain/cse56706/ftp/encryption_perf/

[3] ”A Review of Comparison Techniques of Image Steganography” by Stuti Goel, Arun Rana, Manpreet Kaur published at “IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48”.
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[4] ”AES Implementation and Performance Evaluation on 8-bit Microcontrollers “ by Hyubgun Lee, Kyounghwa Lee, Yongtae Shin presented at “(IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009”

[5] Introduction to AES Encryption by Townsend Security https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf

[6] FIPS PUB 46-3, Data Encryption Standard http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[7] ”Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System” by Karthik .S , Muruganandam .A, presented at “International Journal of Scientific Engineering and Research (IJSER) Volume 2 Issue 11, November 2014”

[8] “Least Significant Bit algorithm for image steganography” by Champakamala .B.S, Padmini.K, Radhika .D. K published at “International Journal of Advanced Computer Technology (IJACT) ISSN:2319-7900”

[9] “Watermarking Digital Image and Video Data” by G. Langelaar, I. Setyawan, R.L. Lagendijk, published at “IEEE Signal Processing Magazine, Vol 17, pp 20-43.”

[10] “A DWT Method for Image Steganography” by Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay at “International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June ”

[11] https://www.schneier.com/cryptography/archives/1995/09/the_blowfish_encrypt.html