Advance Image Encryption using Cryptography and Steganography: A Combine Approach

Sudhans Shekher Panday[1], Mohammad Mustafa Ali[2], Ankesh Jaiswal[3], Amogh agarwall[4], Hritik Somvanshi[5], Aditya Kumar[6]

[1]Prof. CSE Dept, Lovely Professional University, Jalandhar, India
[2-6]Lovely Professional University, Jalandhar, India

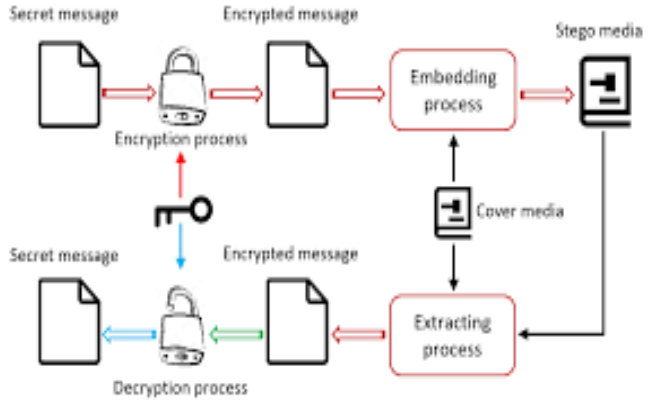
Abstract **-** This paper proposes a security technique for confidential data that combines three techniques: first, image compression based on wavelet transformation, which compresses the confidential image and reduces its size, and second, cryptography based on symmetric key, which encrypts the confidential image, and the third method is steganography, which uses the least significant bit (LSB) to embed encrypted data within a cover picture. As a result, the suggested technique's goal is to ensure that the reconstructed cover image is secure and of high quality.

Index Terms- Encryption, Cryptography, Steanography, Security, Blow fish, LSB AAlgorithm.

I. INTRODUCTION

Information security is incomplete without steganography and cryptography. Cryptography is the science of encrypting and decrypting data using mathematics; the data is converted into some other gibberish form, and then the encrypted data is sent. Steganography is the practice of encoding/embedding secret information in cover media in such a manner that an eavesdropper will not suspect you. When a message is encrypted and hidden using a steganographic method, it adds an extra layer of security and eliminates the risk of the hidden message being discovered. The main goal of this paper is to provide two levels of security through a two-step process in which the message bits are scrambled in a random A 2D Arnold Cat Map is used to generate the letter, which is then encrypted and covered behind a cover image using the basic LSB technique. Two common quality measurements to measure the difference between the cover-image and the stego-image are MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio). The results showed that the proposed technique outperforms simple LSB in terms of PSNR and MSE.

This paper's main goal is to design and develop a secure and efficient symmetric cryptography method for encrypting secret data in order to implement steganography.



II. CRYPTOGRAPHY ALGORITHM

Information protection can be described as a set of measures, procedures, and techniques used to prevent and detect unauthorized access to computer network resources, as well as troubleshooting, disclosure, perturbation, and modification. Enhancing the work's anonymity, eligibility, and dependability necessitates a significant amount of effort to enhance existing approaches while still testing new ones.

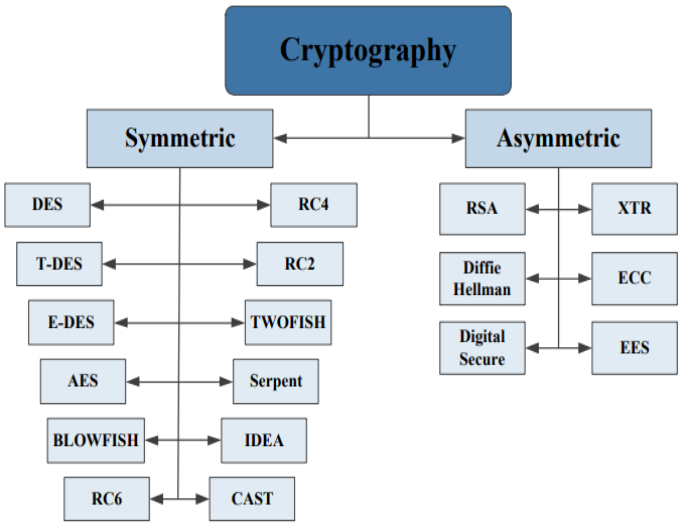
As a result, encoding has been proved to be one of the most effective tools for securing information since the ancient Romans used similar techniques to ensure the protection of their valuable knowledge and records. The method of transforming the shape of data into symbols using nonsensical codes is known as data encoding.

Identical key cryptography is a method of encoding and decoding that relies entirely on a single key. The same key is used for both the encryption and decryption processes in this process. To communicate the hidden key, the sender and recipient must use a secure connection.

Block and stream cyphers are two types of double cypher modes that are tackled by a symmetric algorithm. The block cypher operates on fixed-length groups of bits, known as fragments, without using a symmetric key to convert them. A set of block cyphers manages a stable form.

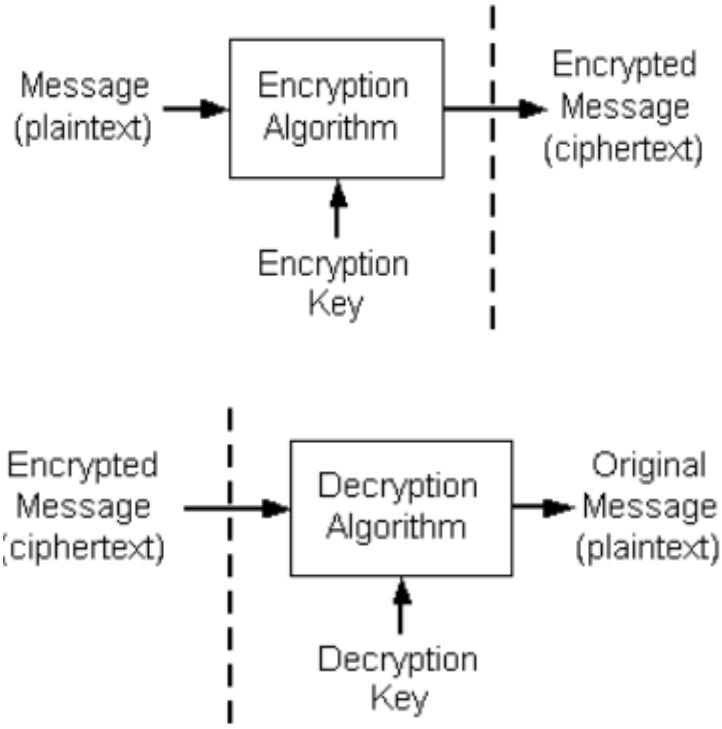
It consists of a number of identical processing rounds, each of which involves a substitution on one half of the information being processed, followed by a permutation that combines the two halves. Since the simple key increases in size, the multi-label keys are used for each round.

A symmetric key cryptography algorithm is one that needs two separate keys, one of which is secret and the other is public [1]. They are mathematically related, despite the fact that they are not the same.The public key is used to encrypt plain text, and the private key is used to decrypt cypher text. The asymmetric encoding strategies in [2] are approximately 1,000 times slower than symmetric encoding, making them unsuitable for encoding large volumes of data.



III. ENCRYPTION AND DECRYPTION:

Encryption transforms a database into unreadable text. Decryption is the method of converting cypher text to plain text in the opposite direction of encryption. A cypher is a series of two algorithms that are used to construct the encoding and decoding operations. The algorithm and a key are in charge of a cipher's lengthy operation. It's a message, a short string of symbols, that would decipher the encrypted data.



IV. USE OF CRYPTOGRAPHY

Cryptography is used to achieve many goals and some of the goals are the following list shows:: • Authentication: is the process of offering identity to a person to break special resource using keys.

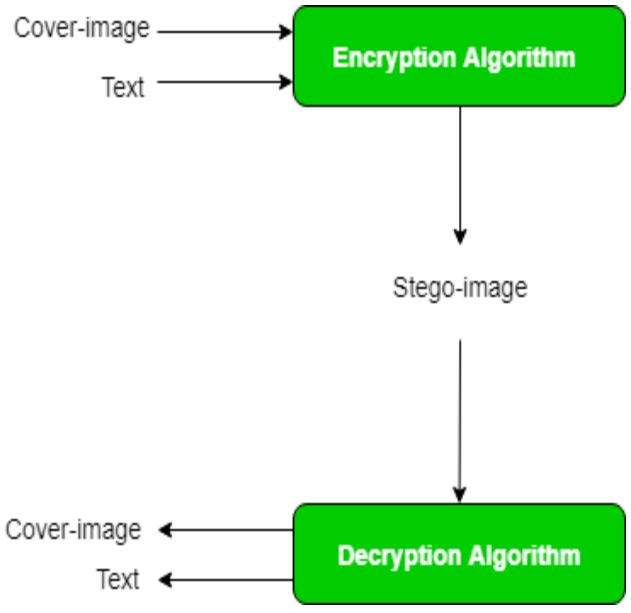
• Confidentiality: The primary aim of cryptography is to ensure that only the owner of the cipher-key reads the code.
Data Integrity: This is an activity that has the right to change a database that belongs to a particular group or entity.
• Non-Repudiation: guarantees that both the sender and the recipient of the report accept receipt of the report.
• Access Control: Guarantees that the delivered message can only be opened by those who have the proper authentication.

Steganography

Steganography is one the most popular methods of providing security to the data that is to be transmitted over a medium. Steganography is derived from the Greek word steganographia, which incorporates the words steganós, which means "covered or veiled," and -graphia, which

means "writing. "Therefore, Steganography is the technique in which message is concealed or hidden over another message in order to avoid disruption, modification and disclosure etc. This technique focuses on hiding the important data unlike other methods that focuses on manipulating the data using a key, making the data unreadable. Steganography differs from cryptography within the sense that it maintains the existence of data secret whereas cryptography maintains contents of information secret. Steganography has various forms, that are text steganography, image steganography, etc.

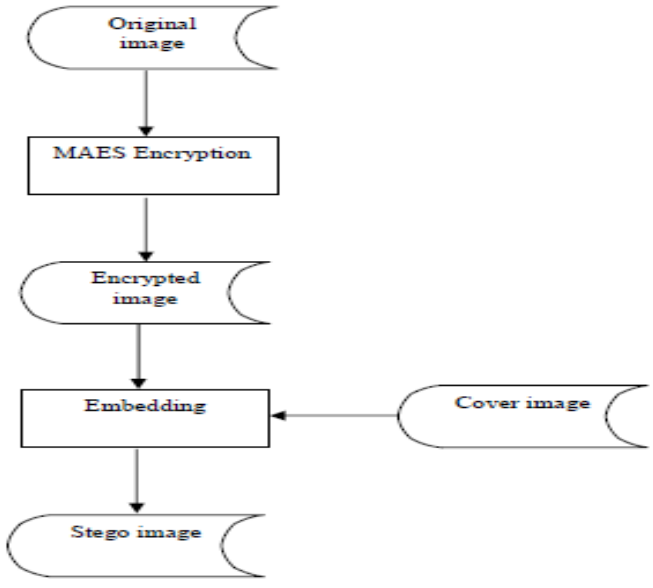
Image steganography is the process of hiding message within the image file. The image used for this purpose is called cover-image and the resultant image obtained is called stego-image. The process of hiding message within a cover is called Embedding and the process of reveling of concealed message from stego-key is called Extracting. There are number of algorithm available for image steganography, one of the most popular algorithms is LSB. In this algorithm least significant bit of each pixel is manipulated and hides the message within the image without disturbing the image. Thus, our secret message goes unnoticed if third party intercepts the message. Therefore, steganography is one of great methods that ensure secure and reliable communication.



V. COMBINING CRYPTOGRAPHY AND STEAGANOGRAPHY:

It is desirable to protect information in order to ensure its confidentiality, integrity, and availability. Cryptography, the art and science of securing data, is one of the most important branches of information security. The original data is translated into cypher data that can be transmitted over an insecure channel using cryptography. Encryption is the process of encrypting data [3].

We have seen above that cryptography and steganography both are at their finest approaches from security point of view. And can be considered for providing a secure and reliable communication. What if we combine these two approaches? we will be able to get considerably a high security. This can be achieved by first encrypting the message that is to be sent using any cryptography algorithm say, blowfish algorithm. This encrypted message is to be embedded on a cover-image. Embedding can be done using any algorithm say, LSB. Now the obtained stego-image is ready to be sent to the receiver and receiver will extract the hidden message and decrypt it using the key. Thus, we can enhance the security using this approach by combining both cryptography and steganography.



V. LSB Algorithm

How LSB technique works?

Each pixel has three values: Red, Green, and Blue, which range from 0 to 255, or 8-bit values. To illustrate how this strategy operates, assume you want to cover the word "hello" in a 4x4 image with the following pixel values:

[(225, 12, 99), (155, 2, 50), (99, 51, 15), (15, 55, 22),(155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66),(219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)]

We will translate the hidden message into decimal values and then into binary using the ASCII Table: 0110100 0110101. Now, one by one, we iterate over the pixel values, translating them to binary and replacing each least significant bit with the message bits in sequence. (e.g 225 is 11100001, we replace the last bit, the bit in the right (1) with the first data bit (0) and so on).This will only modify the pixel values by +1 or -1 which is not noticeable at all. The resulting pixel values after performing LSBS is as shown below:

[(224, 13, 99),(154, 3, 50),(98, 50, 15),(15, 54, 23),(154, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190)]

Algotrithm

1. Take string to be Encrypt.
2. Calculate key for encryption
   a. Use SecretKeySpec.
   b. SecretKeySpec's constructor take user define bytes array to generate Key
3. Create Cipher's object basis on key.
4. It encrypts string data and Encodes using Base64Encoder.
5. And return encrypted message.

VI. BLOWFISH ALGORITHM

Cryptography algorithms are crucial in the field of information security. Symmetric and asymmetric key cryptography are the two categories in which these cryptographic algorithms are classified. . The key will play a critical role in the encryption and decryption of data in these types of encryption methods. The use of a weak key in the algorithm allows data to be easily decrypted. The algorithm's strength is determined by the key's strength; the weaker the key, the weaker the algorithm, and vice versa. Asymmetric algorithms work in a similar manner. The way block cypher algorithms work is that they work with data in the form of groups or blocks. The Data Encryption Standard (DES), the Advanced Encryption Standard (AES), and Blowfish are all examples of Symmetric Key Encryption. In the case of asymmetric key encryption, we have two kinds of keys: private keys and public keys [4].

The public key is used during the encryption process, and the private key is used during the decryption process. Digital Signatures are an example of asymmetric cryptography. The public key is accessible to the general public, while the private key is only accessible to the user. The Blowfish algorithm will be the focus of this paper, and it is one of the most widely used encryption algorithms in the public domain.

Bruce Schneider conceived it in 1993, and it has since been regarded as a simple replacement for existing encryption algorithms. Blowfish is a symmetric key block cypher that employs a 64-bit block size and a key that is variable in length. The encryption key that we use in Blowfish will range from 32 bits to 448 bits in length. There are some variations of the Blowfish algorithm.

Blowfish is one of the most advanced block cyphers ever devised. Patents and copyrights do not apply to the Blowfish algorithm. There has yet to be a successful attack on this algorithm, but it does have a problem with weak keys [5].

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 or 14
Blowfish	32-448 bit .	64 bits	16

VII. DESCRIPTION OF ALGORITHM

The symmetric block cypher algorithm Blowfish encrypts 64-bit blocks of data at a time. It is based on the Feistel network, and the algorithm's operation is split into two components.

A. Key-expansion

In this section, we'll break down the key, which has a maximum length of 448 bits, into multiple subkey arrays, totaling 4168 bytes.

B. Data – encryption

We'll iterate the network 16 times during the data encryption process. There is a key-dependent permutation as well as a key- and data-dependent substitution in each round. The algorithms use XORs or additions on 32-bit words as their operations. We also need to produce four indexed array data lookup tables for each round in this process [6].

Key Generation:

• Blowfish makes extensive use of sub keys. These keys are generated before any data encryption or decryption takes place.

• The p-array consists of 18, 32-bit sub keys: P1,P2,.....,P18

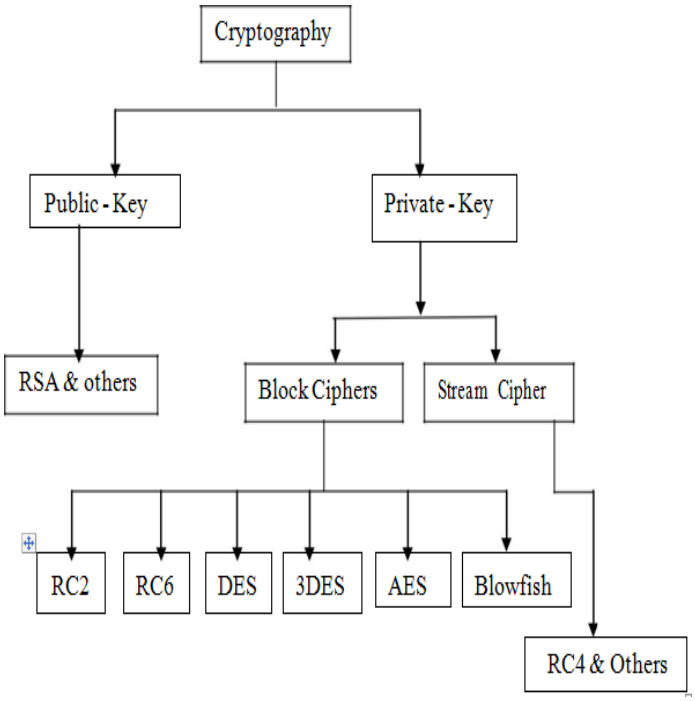
• Four 32-bit S-Boxes consists of 256 entries

each: S1,0, S1,1,.....S1,255

S2,0, S2,1,.....S2,255

S3,0, S3,1,.....S3,255

S4,0, S4,1,.....S4,255



Steps to Generate Sub Keys:

1) With a fixed string, initialise the P-array first, then the four S-boxes in that order. The hexadecimal digits of pi are also included in this string (less the initial 3).

2) XOR P1 with the first 32 bits of the key, XOR P2 with the second 32 bits of the key, and so on until all of the key's bits have been used (possibly up to P14). The process is repeated until all of the bits in the P-key sequence have been XORed. (Every short key has at least one longer key equivalent; for example, if A is a 64-bit key, AA, AAA, and so on are comparable keys.)

CONCLUSIONS

The combination of image compression based on wavelet transform, cryptography based on symmetric key, and steganography based on LSB is introduced in this paper as a novel image security approach. The proposed technique's main concern is the security of the confidential image, with stego image quality being a secondary concern.

This paper introduces a novel image security approach that combines image compression based on wavelet transform, cryptography based on symmetric key, and steganography based on LSB. The security of the confidential image is the primary concern of the proposed approach, with stego image quality being a secondary concern.

REFERENCES

[1] Menezes, Oorschot, Vanstone, and Menezes, "Handbook of Applied Cryptography", CRC Press, Boca Raton, FL, 1997.

[2] B Li, J He, J Huang and YQ Shi., "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2011.

[3] R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Page(s): 1188 – 1193, India 2013.

[4]R.P Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Page(s): 1197 – 1200 India 2013,

[5] Shubhi Mittal; Shivika Arora; Rachna Jain "PData security using RSA encryption combined with image steganography" 1st India International Conference on Information Processing (IICIP), Page(s):1-5, India-2016.

[6] S. Laskar, and K. Hemachandran, "High Capacity Data Hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol. 4, No. 6, pp. 57-68, December 2012