A NOVEL APPROACH FOR DATA TRANSFER WITH ENHANCED SECURITY MERGING ENCRYPTION AND STEGANOGRAPHY

Anju Thomas

Abstract— **Designing a secret key algorithm needs high level security against all kinds of unauthorized attacks like active and passive attacks. An Algorithm is considered computationally secure if it cannot be broken with standard resources, either current or future. This paper has introduced a new block cipher algorithm named Enhanced Multiple Operator Delimiter Based Data Encryption Standard along with LSB steganography. Enhanced Multiple Operator Delimiter Based Data Encryption Standard is one of the best performing partial symmetric key algorithm among the data algorithms like DES, Triple-DES, AES (Rijndael). The algorithm is specially designed to produce different cipher texts by applying same key on same plain text.**

Apart from cryptography, stegonagraphy is the additional method leading to better security of messages which goes hand by hand with cryptography, that's why revel of such a message not easy. This paper introduces an LSB steganography along with the encryption methodology which will play a significant role in the world of symmetric key cryptographic algorithm. The security is ensured by encryption and steganography.

Index Terms— **Block cipher, transposition, Substitution, Encryption, Decryption, Modified Secure Code Sequence, Steganography.**

I. INTRODUCTION

1.1 Cryptography

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Encryption is a method of transforming original data, called plaintext or cleartext, into a form that appears to be random and unreadable, which is called cipher text. Most encryption methods use a secret value called a key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text. The algorithm, the set of mathematical rules, dictates how enciphering and deciphering take place.

Enhanced Multiple Operator Delimiter Based Data Encryption Standard is basically a secret key algorithm which uses a 32-bit key and also multiple binary operators and some delimiters, which are chosen randomly from predefined stacks along with a code sequence. The algorithm produces different cipher texts by applying same key on same plain text. Hence it is not fully dependent on the key and code can not be deciphered by applying all possible combinations of keys.

It has already been proved that although cryptography is a measure concern as an information security vehicle but if we merge steganography with a symmetric encryption technique like Enhanced Multiple Operator Delimiter Based Data Encryption Standard, which will be beneficial in the aspect of security world.

1.2 Image Steganography

A) Basic Terminologies

a) Cover Image: It is defined as original image into which the required information is embedded. We may also call it carrier image.

b) Stego Image: It is an unified image obtained by combination of the cover image with payload.

B) Least Significant Bit based Image Steganography

Least Significant Bit (LSB) insertion is a common, simple approach for embedding information in a cover image. Proposed scheme is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image . The secret message may be hidden by altering least significant bit in a certain layer.

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a

Manuscript received Dec 07, 2014
Anju Thomas, Asst Professor,Nitte Meenakshi Institute of Technology, Bangalore, India

pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference
This paper proposes a new idea of data security by applying Enhanced Multiple Operator Delimiter Based Data Encryption Standard on a text or image file, then hiding it using LSB Steganography.

II. PROPOSED METHODOLOGY

The proposed system uses the following methodology for secured transferring of messages. Firstly, both sender and receiver clients have to agree upon a common key value to be stored in the server having central database. Note that the 32 bit key is used for encryption and decryption.

At the sender side,

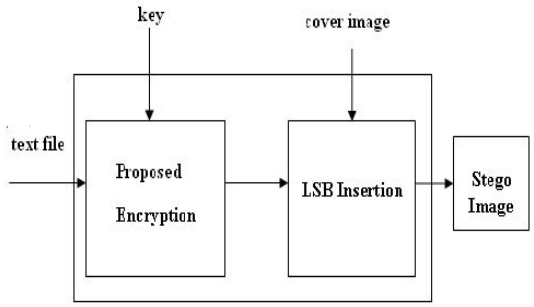

Fig. 1 Proposed Encryption and LSB Insertion

Encryption Procedure of Proposed System

In this algorithm, we have taken two predefined stacks along with a logic based lookup table concept. The first stack consists of different combinations of strings of operators and another stack consists of combinations of several delimiters, which are chosen randomly on the basis of a predefined method which makes the code sequence more secure.
The steps in the algorithm are given below:

1. Text file content is read and position of characters is changed by using Transposition approach.
2. The text received after transposition is then subjected to substitution.
3. Binary shift operations are then applied to substituted text.
4. Now, each character from the modified text file is read and their ASCII value is determined.
5. Binary equivalent of ASCII value is calculated in 32-bit format and stored as a binary string.
6. Next step involves performing a set of mathematical operations, using operators from the operator string, which is stored in operator stack, over the bits, using the secret key.
7. The secrecy of operators used is maintained by encoding the operators from the look-up table.
8. A suitable mathematical operation is performed with randomly generated number, depending on the nature of the key.
9. The corresponding character of the generated random number is added to code sequence.
10. A secured code sequence is obtained by applying any suitable encryption methodology.
11. From the other predefined stack, a random delimiter is chosen and added at the end of the modified secure code sequence.
12. Continue steps (iv) to (xi) for the next characters of the file until end of file is reached.

LSB insertion

The modified secure code sequence generated during encryption now undergoes LSB insertion, which uses a LSB Embedding algorithm.
The LSB Embedding algorithm operates over cover image and the cipher text to produce a stego image. Here, binary equivalent of the ciphertext (to be hidden) is distributed among the LSB's of each pixel of the cover image.

Steps

1. Each character of ciphertext is read and binary equivalent is determined.
2. The cover image is converted into byte stream.
3. Hide each bit of ciphertext in the LSBs of each byte of a cover image. (Cover image is 24-bit image, ie we can store 3 bits in each pixel.)
4. Repeat the above steps for every character in the cipher text.

This results in a stegoimage which is transferred to the receiver.

At the receiver end,

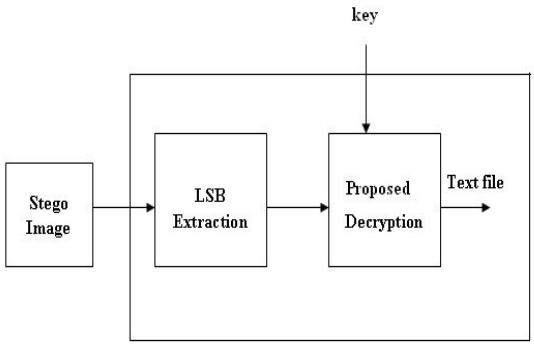

Fig. 2. Proposed Decryption and LSB Extraction

LSB Extraction:

The LSB Extracting algorithm operates over stego image and the modified secure code sequence is extracted. A sequential LSB reading, starting from the first image pixel of the stego image, will extract the secret message.
Decryption Procedure:

Steps:

1. The first character from cipher text is read and then its corresponding ASCII value is calculated.
2. The key is examined and the character before the delimiter in the modified secure code sequence is verified.
3. Similar mathematical operations are performed on this character depending upon the nature of the key.
4. The modified secure code sequence is decoded and inverse operation for each and every character is performed.
5. The inverse of the corresponding binary shift operation is applied.
6. Then the reverse substitution method is performed along with the reverse transposition.
7. Repeat the step (i) to (vi) till the end.

III. CRYPTO ANALYSIS

Modern high quality data encryption methods have several flaws and are subjected to extensive attacks by expert cryptanalyst. This process is called "cryptanalysis", which is a science of reading encrypted traffic without prior knowledge of the key.

To demonstrate the efficiency of proposed methodology, consider the following example. For decryption of the word "CALIFORNIA", the key value and four operators used in encryption algorithm are known.

To demonstrate the efficiency of proposed encryption methodology,let's consider the following example:

C	01000011	3
A	01000001	2
L	01001100	3
I	01001001	3
F	01000110	3
O	01001111	5
R	01010010	3
N	01001110	4
I	01001001	3
A	01000001	2

Fig. 3. Cryptanalysis

Thus, the possible number of attempts to break this word based on four operators is

(4)^3 * (4)^2 *(4)^3 *(4)^3 *(4)^3 * (4)^5 *(4)^3 *(4)^4 *(4)^3 *(4)^2 = (4)^31

On the basis of numbers of one's available in the bits position in the last octet of the binary string is **(4)^31**, possible numbers of combinations of modified secure code sequence string. The transposition of characters also gives **10!** number of combinations.

So, total number of combinations required to decipher the text "CALIFORNIA" is

- **(4)^31 +10! =4611686018431016704 combinations**
- **((4) ^31 +10!) / (2.4*(10)^9) = 1921535841 seconds [Implemented on 2.4 GHz machine]**
- **533759.95 hours**
- **22240 days**
- **60.93 years**

The cryptanalysis of cipher text requires 60.93 years.

If we merge steganography along with the proposed encryption methodology, the security can be enhanced further, as there are two levels of security that has been applied to the message.

CONCLUSION

With the rapid growing of internet and networks applications, data security becomes more important than ever before. Cryptography is a method for secure communication. An Algorithm is an effective method to express finite list of well-defined instructions for calculating a function. Designing a secret key algorithm needs high-level security against all kinds of unauthorized attacks like active and passive attacks.

This paper introduces steganography along with a suitable encryption methodology which will play a significant role in the world of security. The system is indented to provide a complete solution for transferring messages, ensuring security and preserving bandwidth. The implementation is done in java out of which the best possible outcome is obtained.

EXPERIMENTAL RESULTS

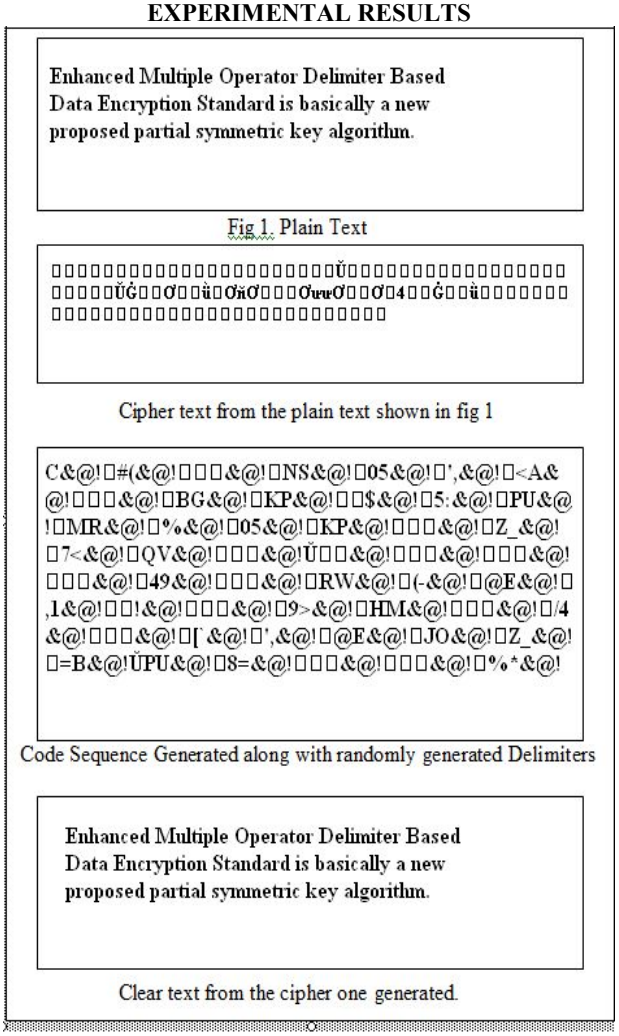

Fig 4. Proposed Encryption and Decryption when applied to Plaintext

Fig 5. Modified secure code sequence with cover image

Fig 6. Stego Image

PSNR VALUE: 65.4902DB

REFERENCES

[1] X-MODDES (eXtended Multi Operator Delimiter based Data Encryption Standard) 2010 Second International Conference on Future Networks

[2] Exploring Steganography: Seeing the Unseen ,Neil F. Johnson ,Sushil Jajodia George Mason University

[3] An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard Dhanraj, C. Nandini, and Mohd. Tajuddin.

[4] Multi Operator Delimiter based Data Encryption Standard (MODDES). ICCNT 2009

[5] A comparative study of performance based crypto analysis features for standard Data Encryption Algorithms with (MODDES),ICCNT 2009

[6] Twenty Second National Radio Science Conference (NRSC 2005), RDEA Algorithm.

[7] Daemen, Jjmen, V.: "AES Proposal: Rijndael", Banksys/Katholieke, R Universiteit Leuven, Belgium, AES submission, June 1998

[8] W.Stallings "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007

[9] Computer Networks by Andrew S. Tanenbaum, Fourth Edition, Prentice hall, 2004