BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN 2348-0513
Vol. 2, Issue 11, Nov 2014, 25-32

MESSAGE SECURITY USING CRYPTOGRAPHY AND LSB ALGORITHM OF STEGANOGRAPHY

RAHUL YADAV

Department of Computer Science, SRM University, NCR Campus, Ghaziabad, Uttar Pradesh, India

ABSTRACT

In this paper, a new approach of information security is discussed. In which, Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography, AES algorithm is being used to encrypt a message, and in Steganography we are using LSB (Least significant Bit) method to hide the message in an image object. The proposed system is experimented on various scenarios in order to evaluate its performance. In all the cases, proposed system exhibits satisfactory results.

KEYWORDS: Cryptography**,** Steganography**,** Least Significant Bit, Advance Encryption Standard, Cipher Text, Plain Text, Stego Image, Cover Image

INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security.

Presently we have very secure methods for both cryptography and Steganography – AES algorithm is a very secure technique for cryptography and the Steganography methods, which use Least significant bit, are highly secured. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography.

LITRATURE SURVEY

Dipti Kapoor Sarmah (Department of Computer Engineering), Maharashtra Academy of Engineering, Pune, INDIA and NEHA BAJPAI (Department of Information Technology), Center of Development of advance computing, Noida, INDIA proposed a paper that was on combined approach of steganography and cryptography but they used FREQUENCY DOMAIN method for steganography. Bret Dunbar proposed a paper for various steganographic techniques and explained how messages can be hidden in text and other object.

After reviewing all papers we have come to this conclusion that very little work has been reported in field of making secure communication between two parties. This extensive review has helped us greatly in identifying our problem for proposed project work, which has been discussed in coming chapters of this project report.

Cryptography

Cryptography concerns with keeping communication private. It scrambles (distorts) a message or plain text into cipher text, so it cannot be understood. This process is called Encryption and back again convert it into a plain text at receiver hand, the reverse process is called Decryption.

NOTATION

Notation for relating plaintext, ciphertext, and key

C=Ek(P),

Where, C is cipher

P is plaintext,

K is key.

Means that the encryption of the plaintext P using key K, gives the cipher text C.

Similarly, P = DK(C) represents of decryption of C to get the plaintext again.

So, DK **(Ek (P)) = P**

Steganography

Steganography hides the existence of a message (information). So it cannot be seen easily. Data can be hidden in a popular object that will not attract any attention like images, audio or video objects which can be represented in binary, and at the receiver hand this hidden information can be extracted, from the image or any other object in which information is hidden.

There are two main approaches to hide the data in these objects, these are:-

- LSB (Least Significant Bit)
- DCT (Discrete Cosine Transform)

OBJECTIVE

The objective of the proposed information security approachis:-

Combine both techniques i.e. CRYPTOGRAPHY and STEGANOGRAPHY and an extra security module to get a very highly secure system for data hiding . So that if any intruder extracted the data, it will be encrypted.

PROBLEM DESCRIPTION

Existing Problem (Techniques)

Till now, the combined approach of cryptography and steganography has been already implemented but this combine approach is quite hard to implement and expensive. Because in this existing technique DCT (Discrete Cosine Transform) method is used for steganography which is hard to execute and expensive.

There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements for cryptography, including Authentication,

Privacy/confidentiality, and Integrity Non-repudiation. Steganography is the other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images, audio, video, text, or some other digitally representative code.

Proposed Technique

AES algorithm for Cryptography

This standard specifies the Rijndael algorithm, asymmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the Constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the Advanced

Encryption Standard (AES) the only length allowed is 128.

Advantages of Using AES Algorithm

- Very Secure.
- Reasonable Cost.
- Main Characteristics:
- Flexibility, II. Simplicity

LSB Algorithm for Steganography

The embedding process consists of choosing a cover image and performing the substitution operation LSB. One can also change more than one bit of the cover image for example, by storing two message bits in the two least significant bits of one cover element.

In the extraction process, the LSB of the selected stego images are extracted and used to reconstruct the secret message.

METHODOLOGY

In our combined approach, we are going to use LSB algorithm of steganography. Again a question occurs that **Why LSB instead of DCT to Hide the Information**?

There are several advantages of using LSB as a steganographic method**.** LSB Embedding has the advantage that it is simple to implementin comparision to DCT. It also allows for a relatively high payload, carrying one bit of the secret message per byte of pixel data. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

Least Significant Bit (LSB)-Based Substitution

240(Information/Message) can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

240: 011110000 (in binary)

Result

(00100110 11101001 11001001)

(00100111 11001001 11101000)

(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed. Result contains information (240), in the pixels of the image.

Cryptography Method-Advanced Encryption Standard (AES)

AES is a simple design, a high speed algorithm, with low memory costs. AES is a symmetric block cipher.

- The same key is used to encrypt and decrypt the message.
- The plain text and the cipher text are the same size.
- Adopted by National Institute of Standards and Technology (NIST) on May 26, 2002.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with, each stage of decryption is inverse of encryption stages.

The Four Stages are as Follows

- Substitute bytes
- Shift rows
- Mix Columns
- Add Round Key
- The tenth round simply leaves out the Mix Columns stage.
- The first nine rounds of the decryption algorithm consist of the following:
- Inverse Shift rows
  - Inverse Substitute bytes
  - Inverse Add Round Key
  - Inverse Mix Columns
- Again, the tenth round simply leaves out the Inverse Mix Columns stage.

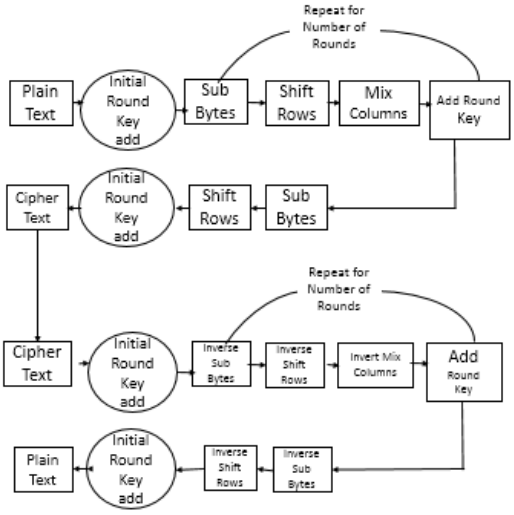

Figure 1: DFD Diagrams of LSB

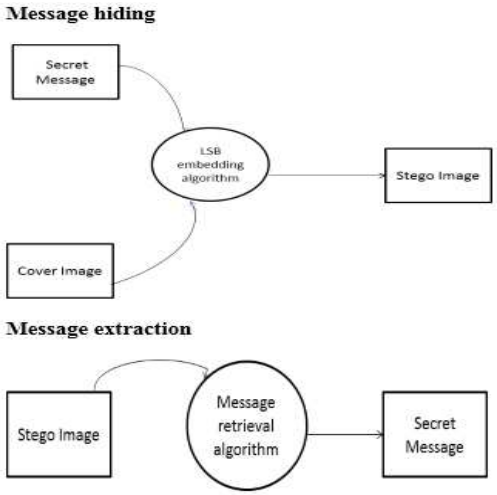

Figure 2: DFD Diagrams of LSB

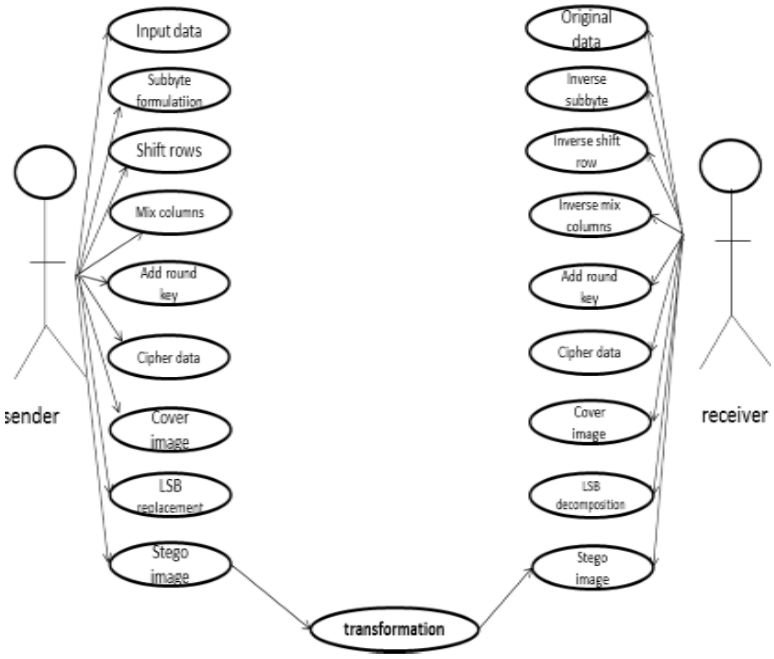

Figure 3: User System Interaction

SCREENSHOTS

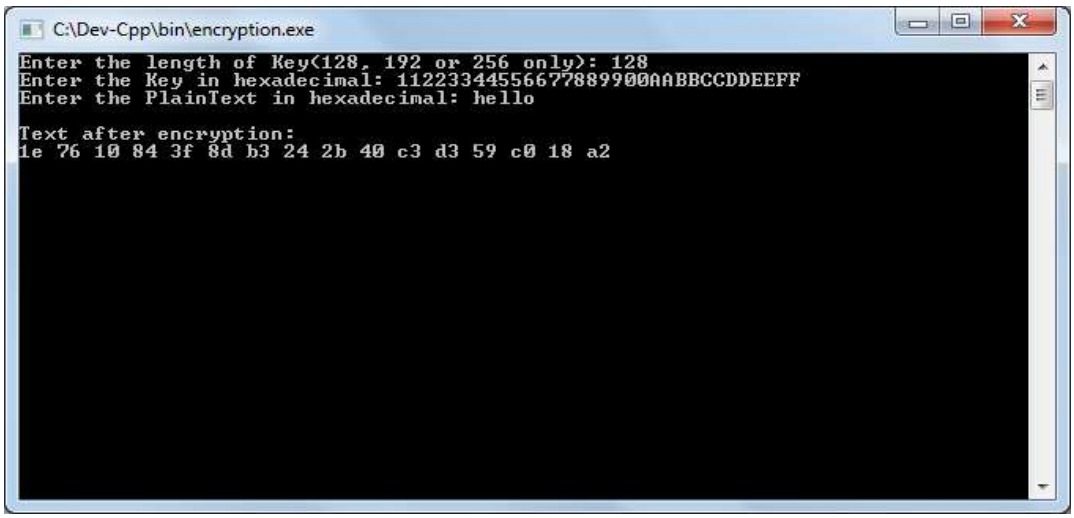

Figure 4: Encryption of Information/Message

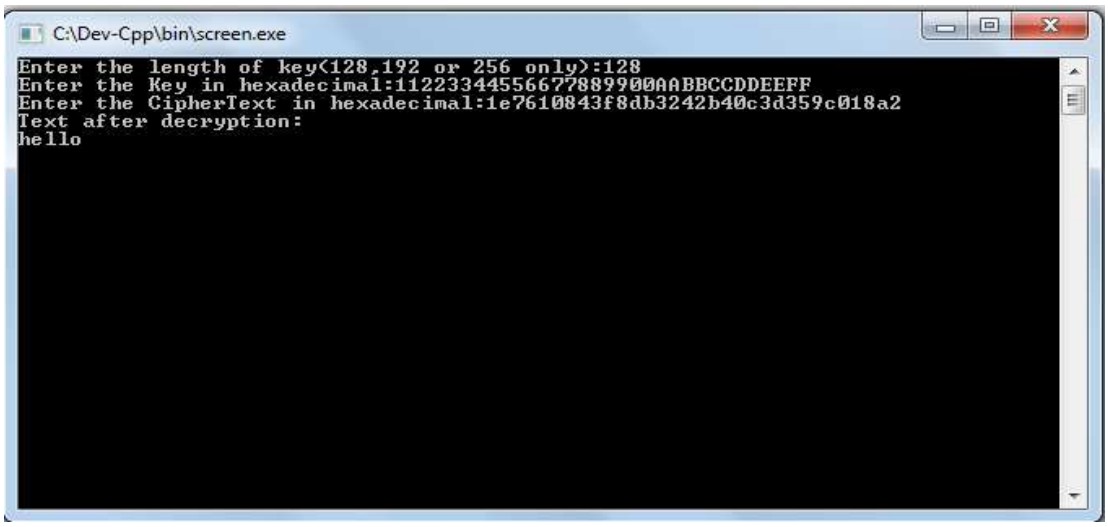

Figure 5: Decryption of Information/Message

CONCLUSIONS

In this project we have presented a new system for thecombination of cryptography and Steganography using LSB algorithm, and an extra security module.

Steganography, especially combined with cryptography, isa powerful tool which enables people to communicate withoutpossible eavesdroppers even knowing there is a form ofcommunication in the first place.

The main advantage of this Crypto/Stegno System is thatthe method used for encryption, AES, is very secure and the LSB Steganography techniques are very hardto detect.

Future Work

The methods used in the science of steganography and cryptography have advanced a lot over The past centuries, especially with the rise of the computer era. Although the techniques are still not used very often, the possibilities are endless. Currently we are using LSB algorithm for steganography and AES for cryptography, in future we can combine cryptography and steganography, by using there other secure algorithms like ECC (Eliptic curve cryptography).

REFERENCES

1. Dipti Kapoor Sarmah, Neha Bajpai: Proposed System for Data hiding Using Cryptography And Steganographic DCT technique.
2. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134.
3. Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series
4. D. R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210
5. Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY
6. Chandramouli, R., Kharrazi, M. &Memon, N., "Image Steganography andsteganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
7. Jessica Fridrich, MiroslovGoljan, and Rui Du, "Detecting Lsb Steganography in color and Grey-scale images", Magazine of IEEE Multimedia, special issue on Multimedia and Security, pp. 22-28, october-December 2001.
8. J. R. Krenn, "Steganography and Steganolysis", January 2004.
9. Hsien – Wen Tseng and Chin- Chen Chang, "High Capacity Data Hiding in JPEG and VQ". Journal of Internet Technology Volume 5(2004).
10. N. F. Johnson and S. Katzenbeisser, A survey of steganograpic techniques, in S. Katzenbiesser and F. Peticolas(Eds.): Information hiding, pp.43-78. Artech House, Norwood, MA, 2000.
11. Chan, C. K and cheng. L. M. 2003. Hiding data in image by simple LSB substitution. Pattern Recognition Letters, 25: 1431-1437.