A Combination Of Plain Text And Cipher Text Based Steganography Through Advanced Encryption Standard

Karthikeyan B, Kattari Sai Krishna, Dinesh G Chandrasekaran, R. Seethalakshmi

`

Abstract: ***Steganography is the way of hiding a secret data inside a trivial data and the extraction of it at its other end. The main aim of steganography is to conceal the presence of a message from unauthorized users. Many techniques are used to hide data in various formats in steganography. One of the methods is to use the Least Significant Bit. This paper is based on the concept of steganography and presents an idea to conceal the information into a color image (eg.JPEG, BMP) using last two significant bits of each pixel. Data is first encrypted by Advanced Encryption Standard (AES) and then inserted into each pixel. Secrecy of the information is increased by encrypting the information and then embedding it into the image using steganography.***

Index Terms: Advanced Encryption Standard, Mean Square Error, Peak Signal to Noise Ratio, Plaintext and Cipher text.

I. INTRODUCTION

Steganography is the art of a hiding important message into ordinary message so that the existence of the important message is undetectable. The main aim of steganography is to transmit the message without any detection by the casual eye. In fact, there should not be any suspicion by the unauthorized user's weather a hidden message is present in the message received by them. This one of the most popular and significant methods to encode images. Least Significant Bit (LSB) method is used by the programs [6-10] for encoding the information into the least significant bit of each and every byte present in the image. By following the above method, the value that each pixel holds is modified negligibly, which will not make any significant changes in the image. This methodology of writing information in some material and afterwards it is covered with wax, on bald head tattooing messages then it is covered by growing hair was used by Greeks. During the World War II inks which are invisible used to write text message within the text of normal message. In World War II Germans used the microdots technology. The technology that is used by microdots is to reduce the picture of hidden message to size of a period [1].

In order to secure information a symmetric block cipher called Advanced Encryption Standard (AES) is used and it is mainly used to encrypt secret data across various fields by implementing it in both hardware and software. It is mainly used to encrypt and decrypt sensitive information. The process of converting sensitive data into unintelligible data to form cipher text is called Encryption and the process of converting cipher text into original data to form plaintext is called Decryption. The data is divided into blocks of 128 bits for encrypting and decrypting data by cryptographic keys of various length such as 128, 192 and 256 bits by the AES algorithm [11]. The main advantage of image steganography is that it is less suspicious to human eyes. Steganography is simple to implement and many techniques uses this method. After applying AES algorithm on the data it can be safely embedded into an image by slightly changing the color values of the pixels in the image, for instance, the modified bits are transmitted into the image and it is highly unlikely to detect the image weather it is changed or not.

II. METHODOLOGY

The main aim is to improve the security during data transfer from the sender to the intended receiver. By applying both steganography and cryptography techniques security can be provided to data during transmission [2]. The method of embedding plaintext into a cover object like image is called Steganography [3]. Human visual perception should not be able to detect the inserted plaintext in the cover object.

Cryptography is a way of encrypting and decrypting the data. The data is encrypted which sender will send to the receiving party and the data is decrypted on the other side [4-5]. To improve the security of data during transmission, we herein use AES encryption to convert the plain text into cipher text and then embedding it into a cover object to obtain a stego object instead of sending plain text directly into the image. The corresponding stego object will be transmitted to the other end. The recipient acquires the information from the stego object. In this method cryptography provides additional security to the data to be transmitted.

III. RESULT DESCRIPTION

The proposed work delineate about the conversion of alternating plaintext into a cipher text using double Advanced Encryption Standard (AES) and inserting plaintext, cipher text into an image using steganography technique.

Revised Manuscript Received on May 25, 2019

Karthikeyan B, School of Computing, SASTRA Deemed to be University, Thanjavur, India.

Kattari Sai Krishna, School of Computing, SASTRA Deemed to be University, Thanjavur, India.

Dinesh G Chandrasekaran, School of Computing, SASTRA Deemed to be University, Thanjavur, India.

*__R. Seethalakshmi,__ Department of Mathematics, SASTRA Deemed to be University, Thanjavur, India. – Corresponding Author

Figure a and b brief about the encoding process of both the alternating plain and cipher text in an image using last two bit steganography.

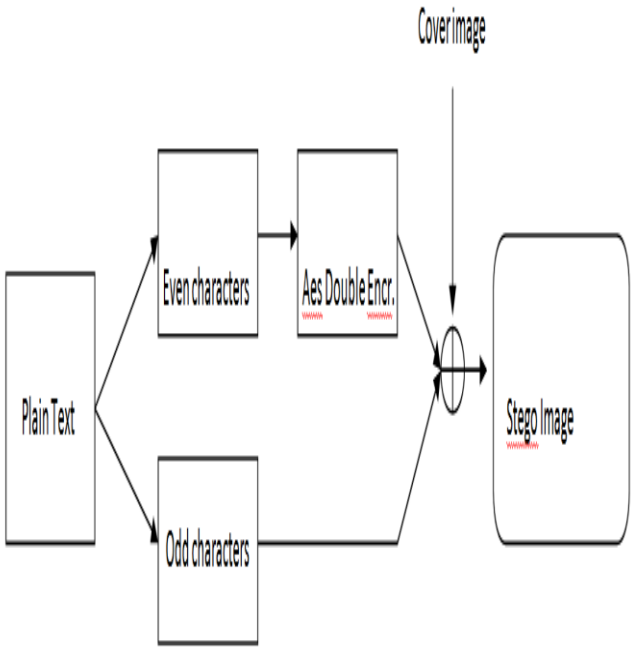

Figure a) Encryption and Embedding flow chart

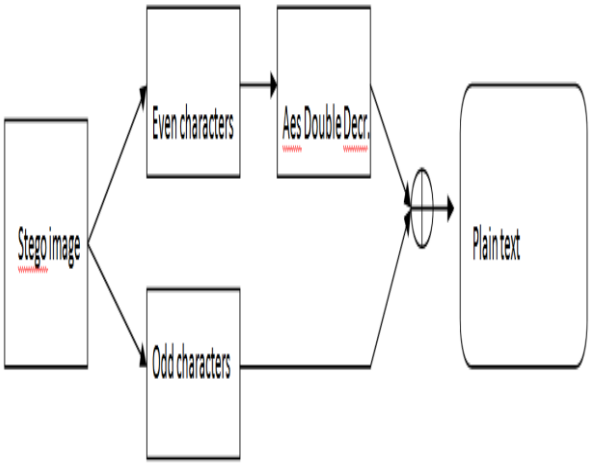

Figure b) Extraction and Decryption flowchart

Let the plaintext be of variable size. Initially take first 16 characters placed in the even positions and pass it to the 16 bit AES for encryption. Again send the encrypted text into the AES encryption algorithm to convert the cipher text into its second form of cipher text. Here the characters undergo double encryption. Unlike even positioned characters, the odd positioned character does not undergo AES encryption. This is shown in Figure c.

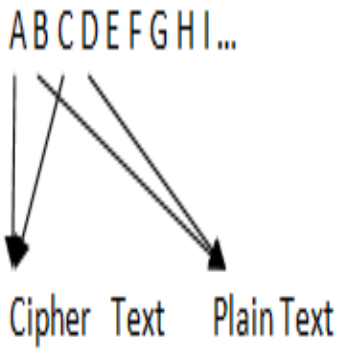

Figure c) Sample Input

A. Embedding the characters

Alternatively store the plain text and cipher text in a file until all the characters are placed. Now take each character from the file and convert them into an 8 bit binary number. Divide the 8 bit binary number into four 2 bit binary numbers. Then take four pixels from the image and replace its corresponding last 2 bits of each pixel with the value of 2 bit binary number which is obtained from the divided 8 bit binary number of the character. Similarly embed all the characters into the image. Thus a stego object is obtained.

B. Extraction and Decryption

Initially take first 16 characters placed in the even positions of the stego image and pass it to the 16 bit AES for decryption. Again send the decrypt the text using AES decryption algorithm to convert the cipher text into its original character. Here the characters undergo double decryption. Unlike even positioned characters, the odd positioned characters do not undergo AES decryption. Now alternatively place the decrypted text and the plain text in a new file to get the original text. The MSE and PSNR value is being calculated for a given image using the formulae as follows:

Given a noise-free $m \times n$ image I and its noisy approximation K, MSE is defined as

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The value of PSNR (in dB) is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

Here, MAX_I refers to the maximum possible pixel value of the image. If the pixels are represented as 8 bits per sample, this value is 255.The MSE and PSNR values for sample images are given in the table I.

Table I) Performance comparison

S. No	Image Name	Row	Col -umn	Depth	Text Size	MSE	PSNR
1	Image1	768	1024	3	32	0.00005	90.92
2	Image1	768	1024	3	96	0.00015	86.19
3	Image1	768	1024	3	192	0.00023	84.35
4	Image2	458	367	3	32	0.00003	93.40
5	Image2	458	367	3	96	0.00032	83.06
6	Image2	458	367	3	192	0.00077	79.22

IV. CONCLUSION

Overall, this describes about the way in which the plain text is transmitted between one authorized user and the other. Authorized user from one side encrypts the alternating characters of the plaintext into cipher text using AES standard encryption. Security is enhanced by embedding cipher text into the image. After transmitting the stego-image to the intended authorized user at the other end, the plaintext is recovered using decryption and AES standard.

ACKNOWLEDGEMENT

Authors would like to convey their sincere thanks to SASTRA Deemed to be University for providing excellent infrastructure facility.

REFERENCES

1. D. Kahn, "The Codebreakers, The Story of Secret Writing", Macmillan, New York, 1967.
2. G. Manikandan, M. Kamarasan and N. Sairam, "A New Approach for Secure Data Transfer based on Wavelet Transform", International Journal of Network Security, 15 (2) , 88-94, 2013.
3. G. Manikandan, N. Sairam, M. Kamarasan, "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme", Research Journal of Applied Sciences, Engineering and Technology, 4 (6), 608-614, 2012.
4. Moon SK, Raut RD, "Analysis of secured video steganography using computer forensics technique for enhance data security", IEEE Second International Conference Image Information Processing, 660–665, 2013.
5. N. Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography", IEEE Security and Privacy, 1(3), 32-44, 2003.
6. Nithin Kumar SSV, Charan GS, Karthikeyan B, Vaithiyanathan V, Rajasekhar Reddy M, "A hybrid approach for data hiding through chaos theory and reversible integer mapping", International Conference on Computational Intelligence, Cyber Security and Computational Models, ICC3 2015; Coimbatore; India, Volume 412, 2016, Pages 483-492.
7. Charan GS, NithinKumar SSV, Vaithiyanathan V, Divya Lakshmi, Karthikeyan B "A novel LSB based image steganography with multi-level encryption", ICIIECS 2014-2015, IEEE International Conference on Innovations in Information, Embedded and Communication Systems, 12 August 2015, Article number 7192867.
8. Sriram S, Karthikeyan B, Vaithiyanathan V, Raj MMA, "An approach of cryptography and steganography using rotor cipher for secure transmission", 2015 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015, 17 March 2016, Article number 7435669.
9. Karthikeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M, "An improved steganographic technique using LSB replacement on a scanned path image", International Journal of Network Security, 16 (1), 14-18, 2014.
10. B Karthikeyan., Shaik Zunaid Sameer., P Srinath., Anishin Raj M M., V.Vaithiyanathan., "A Novel Stretching Approach For Multiple Image Steganography Using Bit Stuffing", International conference on Communication & Security, 2017.
11. William Stallings, Cryptography and Network Security Principles and Practice, Sixth Edition, 2014.

AUTHORS PROFILE

Karthikeyan B completed his Ph.D in Computer Science & Engineering from SASTRA Deemed to be University, Thanjavur in 2015. He has published more than 40research papers in SCOPUS indexed journals and conferences. His area of interest is Image Compression, Steganography and Machine learning.

Kattari Sai Krishna has completed my B.Tech in Information Technology at SASTRA University in 2018. Due to the technological advancements in every industry huge amounts of data is collected and transferred among authorized users so I believe that confidentiality of data is very important. My interest towards data security motivated me to do research in the areas of steganography and cryptography. I was department topper in the courses Artificial Intelligence and expert systems , Signals and systems during my under-graduation. I was overall department 2nd in my fifth semester and 3rd in my sixth semester. I have done my internship at HP Enterprise in Big data Analytics. Currently , I am working at TATA ELXSI a product design company as embedded product design engineer.

Dinesh G Chandrasekaran completed B.Tech in Information Technology from SASTRA University at Thanjavur. He is very curious in learning about data security/protection and especially exploring new ideas in the fields like Steganography and Cryptography

R. Seethalakshmi obtained her Master's degrees M.Sc., from Annamalai University and M.Phil., from Alagappa University, India. She completed her Ph.D. in the year 2017 from SASTRA Deemed to be University and working as a Assistant Professor in the same institution. Her research interests are Mathematical modelling, and differential equations.