Symmetric Image Steganography

Dr. Parul Agarwal
(Assistant Professor)
FET, Jamia Hamdard University
Hamdard Nagar, New Delhi, Delhi 110062
pagarwal@jamiahamdard.ac.in

Saud Khan
FET, Jamia Hamdard University
Hamdard Nagar, New Delhi, Delhi 110062
Saudkhan27@gmail.com

***Abstract*— Security is playing an imperative and crucial role in the field of system correspondence framework and Internet. Data security has turned into the zone of worry as a consequence of boundless utilization of correspondence medium over the web. This paper concentrates on the information security approach when consolidated with encryption and steganographic methods for secret correspondence by concealing it inside the interactive media records. The high results are accomplished by giving the security to information before transmitting it over the web. Steganography is a standout amongst the most intense strategies to disguise the presence of concealed secret information inside a data file such as Image. The Least Significant Bit (LSB) is one of the primary techniques in spatial area image steganography. In this paper, we proposed a combinative process of AES cryptographic encryption algorithm and image steganography with LSB substitution method to increase the security.**

Keywords-Cryptography, Steganography, AES (Advanced Encryption Standard), LSB (Least Significant Bit).

I. INTRODUCTION

One reason that intruders can be fruitful is that the majority of the data they get from a framework is in a structure that they can read and appreciate. Intruders may uncover the data to others, alter it to distort an individual or association, or use it to dispatch an assault. One solution for this issue is to utilize steganography. Steganography and Cryptography play an important role in computer security applications. Steganography is a method of concealing data in advanced media. As opposed to cryptography, it is not to keep others from knowing the concealed data however it is to keep others from imagining that the data even exists. There are a few strategies to disguise data inside spread picture. The spatial area methods control the spread picture pixel bit qualities to install the secret information. The secret bits are composed straightforwardly to the spread image pixel bytes. Therefore, the spatial area systems are basic and simple to actualize. The Least Significant Bit (LSB) is one of the principle techniques in spatial area image steganography. [1, 3]

In the way of cryptography, an AES (Advanced Encryption Standard) is a symmetric block cipher algorithm used to encrypt the information to make it as secret information before embedding it inside the cover image. Cryptography is an art of encrypting the data by making it in a non-readable form to prevent information from unauthorized user or attacker. [2, 4]

OVERVIEW OF STEGANOGRAPHY

Steganography is the art and science of conveying in a way which conceals the presence of the correspondence. Steganography assumes an imperative part in data security. It is the craft of undetectable correspondence by hiding data inside other data. The term steganography is gotten from Greek and truly signifies "secured making". A Steganography structure involves of three components: cover image (which shrouds the secret message), the secret message what's more, the stegano-image (which is the spread item with message installed inside it). A computerized picture is portrayed utilizing a 2-D grid of the shading guts at every network point (i.e. pixel). Normally dark pictures utilize 8 bits, while shaded uses 24 bits to portray the shading model, for example, RGB model. The Steganography framework which utilizes a picture as the spread, there are a few methods to hide data inside spread picture. The spatial space strategies control the spread picture pixel bit qualities to insert the secret data. The secret bits are composed specifically to the spread picture pixel bytes. Thus, the spatial space strategies are basic and simple to actualize. The Least Significant Bit (LSB) is one of the primary strategies in spatial area picture Steganography. The LSB is the most minimal critical piece in the byte estimation of the picture pixel. The LSB based image steganography implants the secret at all critical bits of pixel estimations of the spread picture. While cryptography results in making the information human mixed up structure called as figure in this way cryptography is scrambling of messages. Though the steganography results in abuse of human mindfulness so it stays in secret and undetected or in place. It is conceivable to utilize all document medium, advanced information, or records as a spread medium in steganography. By and large steganography procedure is connected where the cryptography is insufficient. The objective of Steganography is to abstain from attracting suspicion to the presence of a shrouded message. These days' images are the most well known spread item utilized for steganography where an adjusted image with slight varieties in its hues will be unclear from the first image by an individual, and consequently the importance of Image Steganography. In this work, images are utilized as a spread article to conceal the secret data. [6]

II. PROPOSED WORK

A. *Steganography Model*

This is a combinative process of cryptographic and steganographic technique to increase the security. The steganography model consists Cover image, Secret message (encrypted via AES), and Stego-Object. Cover is otherwise called spread article, in which the image is installed and serves to conceal the encrypted message. First, message is encrypted by AES (Advanced Encryption Standard) algorithm and then the encrypted message will embed inside the image with LSB substitution method to make the Stego-Object which contains the secret information. This process provides the higher security so none can be able to reveal the secret information.

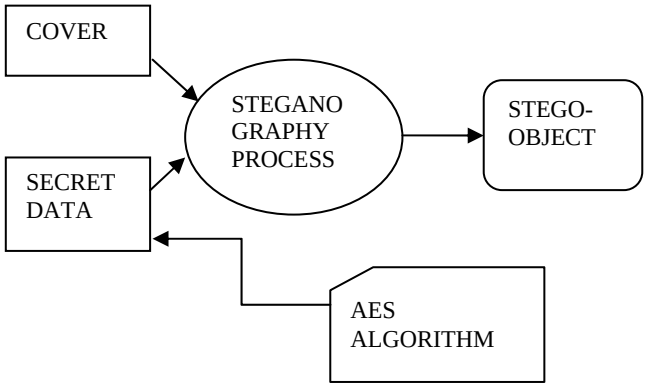

FIG 2.1: Combinative Process of Cryptography and Steganography.

B. *AES (Advanced Encryption Standard)Algorithm*

- AES is a block cipher with a block length of 128 bits.
- AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits.
- Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
- Except for the last round in each case, all other rounds are identical. [10, 12]
- Above AES encryption algorithm is used to encrypt the data and then encrypted information is embedding into secret cover frame by using LSB approach.

C. *Embedding Process*

LSB is straightforward and most normally utilized picture steganography calculation. LSB is essentially taken after insertion process in which last piece is basically supplanted by the bit of mystery message. At to begin with, unique picture called spread picture (I) is changed over into 8-bit stream in any case, on the off chance that we are utilizing a 24-bit image then it can likewise be separated into 3 piece of 8-bit of red, green and blue shading segment. At that point LSB or last piece of every 8-bit square is supplanted with the bit of secret message/image successively or arbitrarily utilizing a pseudo-irregular generator with the assistance of Stego-key.

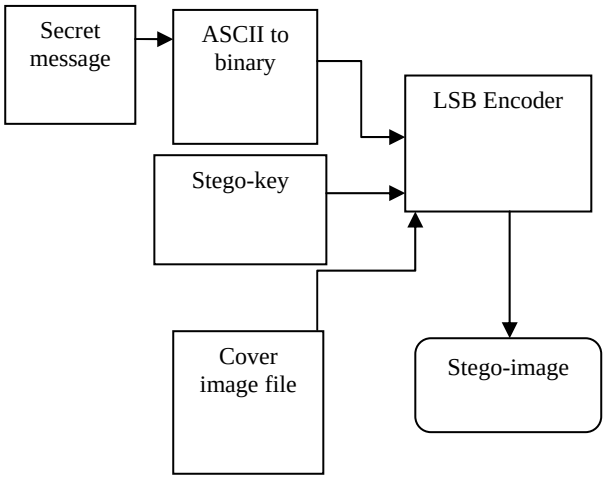

FIG 2.3: Embedding Process

D. *Extraction Process*

The Stego-Object can be removed at purported collector's side by performing decoding of Stego-Object and after that by extracting the Cover Image. The resultant information is the encoded secret information which is again unscrambled to get unique data. Thus the proposed framework gives the most secure methodology utilizing two layer of encryption the first is performed on the secret information itself and another on the Image file.

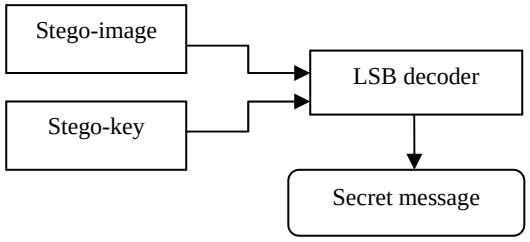

FIG 2.2: Extraction Process

E. *Advantages of Using AES (Advanced Encryption Standard) Algorithm*

- ✓ AES is more secure and it is less susceptible to cryptanalysis than other encryption algorithm.
- ✓ AES is faster in both hardware and software.
- ✓ AES supports larger key sizes.
- ✓ AES is required by the latest U.S. and international standards.
- ✓ NSA has also declared that AES algorithm is secured for classified data.

F. Steganography vs Cryptogrphy

Table 2.5: Comparisons between Steganography and Cryptography

Method	**Steganography**	**Cryptography**
Carrier	Any digital media	Normally message based, with a few augmentations to image files
Secret data	Payload and no progressions to the structures	Plain text and changes the structure
Key	Discretionary	Necessary
Input files	At least two unless in self-installing	One
Detection	Blind	Blind
Authentication	Full recovery of information	Full recovery of information
Objective	Secret communication	Data protection
Result	Stego-record	Cipher text
Concern	Limit	Robustness
Type of attacks	Steganalysis	Cryptanalysis
Visibility	Never	Always
Fails when	It is identified	De-ciphered
Relation to cover	Not as a matter of course identified with the spread. The message is more critical than the spread.	N/A
Flexibility	All suitable cover	N/A
History	Exceptionally antiquated aside from it computerized variant	Modern era

[13]

III. ANALYSIS VIA MATLAB

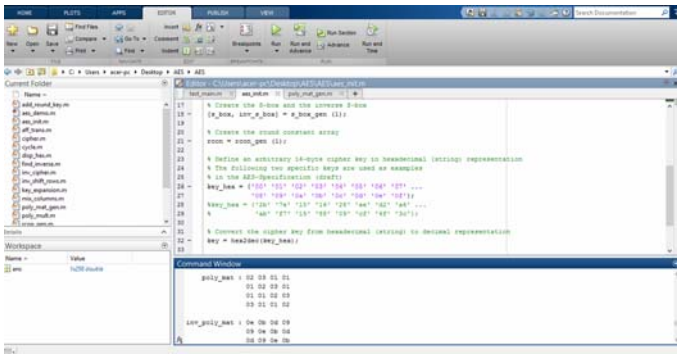

FIG 3: (a) AES Algorithm Flow

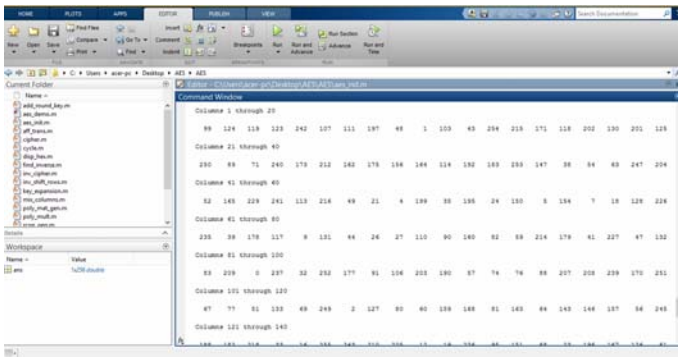

FIG: 3 (b) AES Algorithm Flow

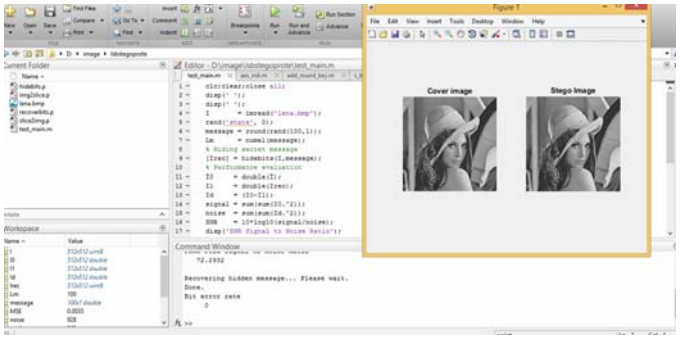

FIG: 3 (c) Cover Image Generation (contains hidden information)

IV. FLOWCHART

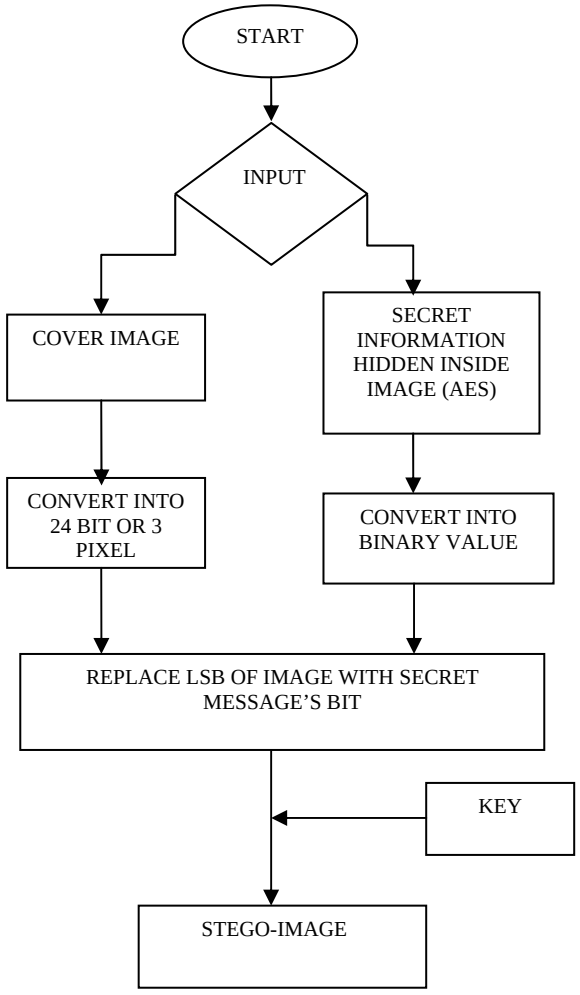

FIG 4: Process Flow Chart

Above flow chart of proposed model is showing the flow of work in which information (input) is send to AES algorithm to encrypt it first, and then it converts into binary value. So it can be embed inside the cover image with the help of LSB method to increase the security in the communication system. Therefore none intruders can access the secret information. Thus, this combinative process provides the higher security.

CONCLUSION

In this paper we displayed a few methods for concealing the mystery information inside the Image file. The proposed framework for information concealing uses AES for encryption. It results in more secure strategy for information hiding. We can reason that the proposed framework is more powerful for secret correspondence over the system channel.

ACKNOWLEDGMENT

We are thankful to the Professors at Jamia Hamdard University for their valuable suggestions.

REFERENCES

[1] K.Steffy Jenifer, G.Yogaraj, K.Rajalakshmi, "LSB Approach for Video Steganography to Embed Images," International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1), 2014, 319-322.

[2] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography," International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[3] Mamta Juneja, Parvinder Singh Sandhu, "Information Hiding using Improved LSB Steganography and Feature Detection Technique," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[4] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for data hiding using Cryptography and Steganography," Proc.International Journal of Computer Applications, Vol 9, Isuue2, 2010.

[5] H.Al-Barhmtoshy, E.Osman and M.Ezzat, "A Novel Security Model Combining Cryptography and Steganography", 2004.

[6] Champakamala .B.S, Padmini.K, Radhika .D. K, "Least Significant Bit algorithm for image steganography," International Journal of Advanced Computer Technology (IJACT), Volume 2, Issue 4, August 25,2014 ISSN: 2319-7900.

[7] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M, "Image Steganography Techniques: An Over-view," International Journal of computer science and security, vol (6), Issue (3), 2012.

[8] Vijay kumar sharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimize technique," Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.

[9] Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar, **"**Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques,**"** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[10] Atul Kahte, "Cryptography and Network Security," Tata Mcgraw Hill, 2007.

[11] Shasi Mehlrotra seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms For Data Communication," IJCST Vol. 2, Issue 2, June 2011.

[12] William Stallings, "Cryptography and Network Security Principles and Practices," Prentice Hall, November 16, 2005.

[13] Sandeep Kumar, Ms Vineeta Bassi, "Image Steganography using Improved LSB and EXOR Encryption Algorithm," July 2014.

AUTHORS PROFILE

Authors Profile

Dr. Parul Agarwal holds a Ph.D. Degree in Computer Science. Currently she is an assistant professor in FET, Jamia Hamdard University, New Delhi. She has about 14 years of experience in teaching at University level. She has specialization in Fuzzy Data Mining, and Soft Computing. She has several published papers in Indexed, reputed International Journals. Also she had reviewed several papers which were published in International Conferences, and Journals.

Saud Khan currently pursuing M.tech in Information Security and Cyber Forensics in FET, Jamia Hamdard University, New Delhi. He had done his B.tech in Computer Science from FET, Manav Rachna International University, Faridabad.