Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Novel Security Scheme for Image Steganography using Cryptography Technique

Lokesh Kumar
IMSEC, Ghaziabad (India)
lokeshk_gautam@yahoo.com

Abstract: - In today's information age, information sharing and transfer has increased exponentially. The information vulnerable to unauthorised access and interception, while in storage or transmission. Cryptography and Steganography are the two major techniques for secret communication. The contents of secret message are scrambled in cryptography, where as in steganography the secret message is embedded into the cover medium. This paper presents a new generalized model by combining cryptographic and steganographic Technique. These two techniques encrypt the data as well as hide the encrypted data in another medium so the fact that a message being sent is concealed. In cryptography we are using advanced encryption standard (AES) algorithm to encrypt secret message and then alteration component method is used to hide encrypted message. By using these two techniques the security of secret data increases to two tier and a high quality of stego image is obtained.

Keywords: Steganography techniques, Cryptography techniques, Information Hiding, Information Security, Image hiding, Advance encryption standard (AES)

1. Introduction:

Classic methods of securing communication mainly base on cryptography, which encrypts plain text to generate cipher text. However, the transmission of cipher text may easily arouse attackers' suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to make up for the shortcomings of cryptographic techniques, steganography has been developed as a new covert communication means in recent years. It transfers message secretly by embedding it into a cover medium with the use of information hiding techniques.

Cryptography and Steganography are two important branches of information security. Cryptography provides encryption techniques for a secure communication. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [1], [2]. Steganography is the art and science of hiding communication [3]. Steganography involves hiding information so it appears that no information is hidden at all.

Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography, in contrast attempts to prevent an unintended recipient from suspecting that the data is there. [4].Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable.

This paper organized in Sections. Firstly I describe the introduction of Steganography and Cryptography Techniques under the heads of Introduction in Section-I. Subsequently I have gone through the literature review and give overview of AES. All this we have mentioned under heads of Backgrounds in Section-II. In Section-III, the proposed architecture and mechanism described in detail. Finally, this paper concluded and mentions its further enhancements under future scope in Section – IV and Section-V respectively. All used references used during writing of this paper are mention in Section –VI under head of references.

2. Background

Compared to other types of steganography, image steganography has attracted extensive research as well

as popular usability in recent years. This is due to the fact that huge amounts of data can be hidden without perceptible impact to the carriers and possibly because of the popularity of electronic images that have become widely available. With this in mind, I describe steganography techniques and tools that use image files in more details. I present a set of criteria to appraise them. Due to limited space, we include a subset of the tools that we have studied and compared.
An early work on the image steganography is Least Significant Bit technique (LSB) [5, 8, 10]. This technique is simple in both the embedding and de-embedding (extracting messages) processes, but suffers several disadvantages. Fridrich et al. [14] point out that recent advances in steganalysis have shown that LSB does not guarantee detectability, evidenced by the fact that they can be successfully attacked using statistical [15], or even visual attacks [13]. In addition, it is extremely vulnerable. For example, re-saving in a BMP image can destroy the hidden information [5]. Further this technique is not appropriate for JPEG and GIF format.
Transform domain steganographic methods hide data in the coefficients of the represented domain [6, 12]. After mapping the signals to another domain such as discrete Fourier transform, cosine transform, Hartley transform, and wavelet
transforms, the obtained coefficients are altered or replaced [17]. The methods are more robust than spatial domain embedding techniques while maintaining good image quality. They are also independent to various image file formats either lossy or lossless image formats; however, have lower capacity. Examples include F5 [20], OutGuess [7] and StegHide [9].

Advanced Encryption Standard (AES)

Advanced Encryption Standard is the Rijndael algorithm by two researchers Dr. Joan Daemon and Dr. Vincent Rijmen from Belgium [16], [18]. Unlike its predecessor, DES, AES does not use a Feistel network [11]. The AES algorithm is a symmetric key block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used to both encrypt and decrypt a message. Also, the cipher text produced by the AES algorithm is the same size as the plain text message. Most of the operations in the AES algorithm take place on bytes of data or on words of data 4 bytes long, which are represented in the field GF (28), called the Galois Field. AES is based on a design principle known as a Substitution permutation network. AES operates on a 4×4 matrix of bytes, termed the *state*. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. The AES algorithm loops through certain sections N_r times.
It is fast in both software and hardware.
AES Algorithm have following steps.
1) Key Expansion—Round keys are derived from the cipher key using Rijndael's key schedule.
2) Initial Round
a) Add Round Key—each byte of the state is combined with the round key using bitwise XOR.
3) Rounds
a) Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
b) Shift Rows—A transposition step where each row of the state is shifted cyclically a certain number of steps.
c) Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
d) Add Round Key
4) Final Round (no Mix Columns)
a) Sub Bytes
b) Shift Rows
c) Add Round Key

Advantages of using AES algorithm
1) Very Secure.
2) Reasonable Cost.
3) Main Characteristics
i) Flexibility, ii) Simplicity

3. Proposed Technique:

3.1 Proposed Message Embedding Procedure:

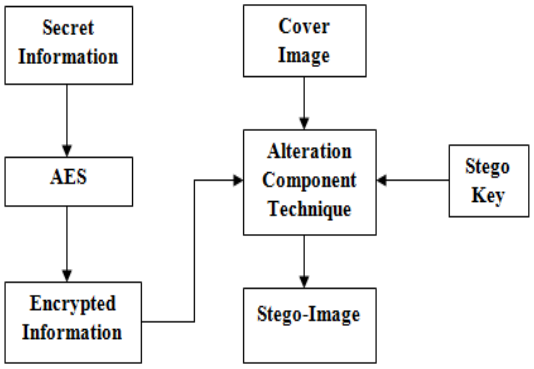

Fig 1: Sender Prospect

Figure-1 shows the sender's prospect of Proposed Technique in which the secret information is encrypted by using advance encrypted standard (AES) encryption algorithm. Then encrypted message is embedded into cover image by using Alteration component technique. Image containing the secret data is called stego image. Next phase is to select the stego key for encoding. In Embedding process data is hidden by using Alteration component technique in which pixels have been replaced by key and secret message. Firstly key is converted into binary form and its binary form is filled in the first component of first

pixels. After then, secret message is converted into binary form and its binary form is filled in first component of next pixels.

Embedding Algorithm

Step (a): Extract all the pixels in the given image and store it in the array called Pixel-Array.
Step (b): Extract all the characters in the given text file and store it in the array called Character- Array.
Step (c): Extract all the characters from the Stego key and store it in the array called Key - Array.
Step (d): Choose first pixel and pick characters from Key- Array and place it in first component of pixel. If there are more characters in Key- Array, then place rest in the first component of next pixels, otherwise follow Step (e).
Step (e): Place some terminating symbol to indicate end of the key. '0' has been used as a terminating symbol in this algorithm.
Step (f): Place characters of Character- Array in each first component (blue channel) of next pixels by replacing it.
Step (g): Repeat step (f) till all the characters has been embedded.
Step (h): Again place some terminating symbol to indicate end of data.
Step (i): Obtained image will hide all the characters that we input.

3.2 Proposed Message Extraction Procedure:

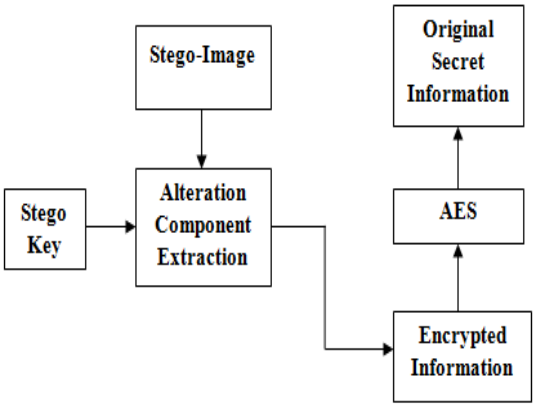

Fig 2: Receiver Prospect

Figure-2 shows the receiver's prospect of Proposed Technique in which the sender sends a stego-image to the receiver or legitimate user. The legitimate user having the stego key to extract secret data from stego image. The legitimate user must have the same key with which the image is embedded. On Stego image Extracting process is applied by using Alteration component technique. After data extraction I get the secret message which is in encrypted form. Advanced encryption standard (AES) decryption algorithm is used to decrypt message. Finally we get the Secret Data which is embedded.

Extraction Algorithm

Step (a): Consider three arrays. Let they be Character-Array, Key-Array and Pixel-Array.
Step (b): Extract all the pixels in the given image and store it in the array called Pixel-Array.
Step (c): Now, start scanning pixels from first pixel and extract key characters from first (blue) component of the pixels and place it in Key-Array. Follow Step 3 till we get terminating symbol, otherwise follow step (d).
Step (d): If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program by displaying message —Key is not matching.
Step (e): If the key is valid, then again start scanning next pixels and extract secret message characters from first (blue) component of next pixels and place it in Character Array. Follow Step (e) till we get terminating symbol, otherwise follow step 6.
Step (f): Extract secret message from Character-Array.

4. Conclusion

Cryptography and steganography are two major branches of data security. In this proposed system cryptographic and steganographic security is combined to give two tier security to secret data. In proposed scheme secret message is encrypted before hiding it into the cover image which gives high security to secret data. Advanced encryption standard (AES) is used to encrypt secret Message and Alteration component technique is used to hide encrypted secret message into cover image. Since the resulting perceptual quality of the mixed images is good, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication.

5. Future Aspects

In the future work, there is a planning to design a sophisticated software based on this technique which will targeted to use in highly secure multimedia data transmission applications.

REFERENCES

[1] Menezes, Alfred , Paul C van Oorschot ,Scott A. Vanstone, " Handbook of Applied Cryptography. CRC Press", October 1996 , ISBN 0-8493-8523-7.
[2] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.
[3] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy Mag.", 2003, vol. 1, no. 3, pp. 32–44,.
[4] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the

second international workshop on information hiding, vol. 1525 of lecture notes in computer science,Springer, 1998. Pp. 32-47.

[5] Johnson, N.F. and S. Jajodia. "Exploring Steganography: Seeing the Unseen." IEEE Computer Mag., February 1998.

[6] N. F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26–34, 1998.

[7] N. Provos, OutGuess, http://www.outguess.org/, 2006.

[8] Kessler, G. "An Overview of Steganography for the Computer Forensics Examiner ", Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004

[9] S. Hetzl, StegHide, http://steghide.sourceforge.net, 2003.

[10] Bennett, K. "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text" Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.

[11] Data Encryption Standard (DES)'.National Bureau of Standards (US).Federal Information Processing Standards Publication National Technical Information Service. Springfield VA. April 1997.

[12] N. F. Johnson and S. C. Katzenbeisser, "A survey of steganographic techniques," Information Hiding: Techniques for Steganography and Digital Watermarking, Chapter 3, MA, 1999, pp. 43–78.

[13] Westfield, A., and A. Pfitzmann. "Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and Stools - and Some Lessons Learned," Lecture Notes in Computer Science, 1768: 61-75 (2000).

[14] Fridrich ,J, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," IEEE Multimedia Special Issue on Security, pp. 22–28, October- November 2001.

[15] Avcibas, I. , N. Memon, and B. sankur, "Steganalysis using image quality metrics." Security and Watermarking of Multimedia Contents, San Jose, Ca., February 2001.

[16] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." in Springer, 2002, ISBN 3-540-42580-2.

[17] C. B. Smith and S. S. Agaian, "On noise, steganography, and the active warden," Multimedia Forensics and Security, Chapter VIII, Information Science Reference, PA, 2008, pp. 139-162.

[18] Christof Paar, Jan Pelzl, "The Advanced Encryption Standard" Textbook for Students and Practitioners.

[19] A. Westfeld, "F5–A steganographic algorithm high capacity despite better steganalysis," Proceedings of the Fourth International Workshop on Information Hiding, Lecture Notes in Computer Science, vol. 2137, pp. 289–302, 2001.

