ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (264-268), Month: April - June 2015, Available at: www.researchpublish.com

AAKRITI[ed]: An Image and Data Encryption-Decryption Tool

[1]Diwesh Dutt, [2]Vishakha Hegde, [3]Prof. P.T Borse

[1, 2, 3] Computer Engineering, Dr. D.Y Patil School of Engineering, Pune, India

Abstract: **With immense use of the internet in today's highly technological age, data security has gained tremendous importance. Securing sensitive information from unauthorised users and attacks has resulted in a number of data security measures like cryptography and steganography being implemented on a large scale. Steganography is a method of embedding sensitive data in an image normally called a cover-image to generate a stego-image. It becomes difficult to detect the data hidden in a stego-image unless the attacker is aware of the existence of the data. In recent years many steganography techniques have been proposed and implemented. This paper gives a brief overview of some of the works related to steganography. This paper also introduces a technique of steganography using hybrid cryptography and Bit Plane Complexity Segmentation (BPCS) method.**

Keywords: **Steganography, image security, data hiding, hybrid cryptography, encryption, decryption**

I. INTRODUCTION

The word "steganography" was derived from the Greek words Steganós (Covered), and Graptos (Writing) which translates into "covered writing" [1]. Steganography hides sensitive data or message from potential attackers by concealing its existence. This is achieved by embedding the data in another medium like an image file, audio file, video file etc. which is known as the carrier file. Normally, digital images are used as carrier files.

Steganography differs from cryptography in the sense that cryptography makes a message unreadable while steganography hides the very existence of the message. Cryptography can be detected and the message can be deciphered if the attacker has access to the corresponding key for decryption. Steganography, on the other hand, is difficult to detect as the data is hidden within the carrier medium. Watermarking is used to hide details of the concerned image. Watermarking is usually used for copyright purposes while steganography is just used to hide data from intruders.

The general working of steganography is shown in Fig.1. It consists of a carrier file(CF) which can be an image, video or audio file, a Secret message (SM) which has to be embedded, a Stego-Key (SK) which is mainly used to make sure that only an authorised person having the decoding key can extract the message. A suitable Steganography algorithm embeds the secret message into the cover image in such a way that no visible changes occur in the carrier file. Finally the output obtained is known as the stego-object which basically is the secret message embedded within the carrier file.

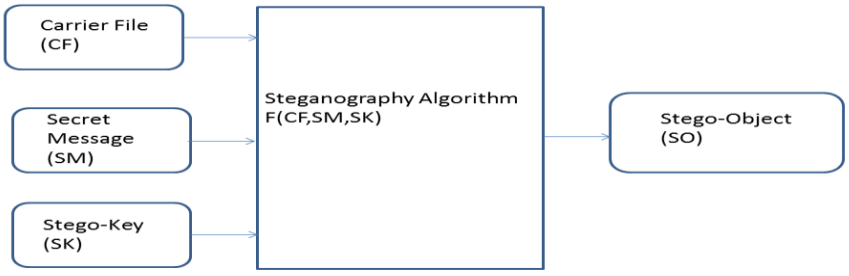

Fig.1 A general steganography model showing the steps of embedding confidential data into a carrier file.

1.1. NECESSARY CHARACTERISTICS OF A STEGANOGRAPHY SYSTEM

A good steganography technique has to possess the following three major characteristics:

1.1.1. Imperceptibility: The carrier file should be embedded in such a way that the stego-object should not be suspected of hiding any data [2].

1.1.2. Robustness: It refers to the resistance of the image to any kind of transformation [3].

1.1.3. Capacity: Capacity refers to the extent up to which data can be embedded in a cover image without degrading image quality [2].

2. RELATED WORK

Mehdi Hussain and Mureed Hussain [1] have given an overview of steganography by describing the different types and techniques of implementing steganography. After critically analysing different embedding techniques they realised that the quality of the cover image deteriorates as the amount of hidden data increases beyond a certain limit using LSB techniques.

Hussein Al-Bahadili [4] has described a secure BPIS (Block Permutation Image Steganography) algorithm which combines permutation and steganography to give a reliable steganography technique. The algorithm works by converting the message to be embedded into its binary form. It then divides this binary sequence into blocks and then permutes each block randomly using a key. These permuted blocks are then concatenated and this binary sequence is embedded into an image in bmp format using the LSB technique. This technique is secure as the message can not be deciphered unless the permutation is known. More work has to be done to check the effect of permutation size on the performance of the algorithm.

Ketki Thakre and Nehal Chitaliya [5] have proposed a four bit LSB technique to embed data in two cover images. The cover can be an image, audio or video. The data to be hidden is embedded in its binary form in two cover images. This provides double protection. A two level security can be obtained along with better imperceptibility and high payload capacity.

Vijay Kumar Sharma and Vishal Shrivastava [6] have proposed an algorithm based on logical operation for 8-bit or 24-bit image. This algorithm replaces nLSB of cover image from a byte with the nMSB of secret image. Experimental analysis show that the stego-image is almost indistinguishable from original image.

Rosziati Ibrahim and Teoh Suk Kuan [7] have proposed a 2 layer security steganography algorithm. In this method the text file to be embedded is first converted to a zip file to maximize data storage inside the image and then converted into binary codes. Each last two bits are encoded into each image pixel. This minimises distortion.

Babita and Ayushi [8] have described a steganography algorithm that uses encryption and a user-defined key. The user first enters a key between 0-255. This key is XOR-ed with the message to be hidden to produce a cipher text. This cipher text is hidden in an RGB image by moving from left to right along the columns till end of image is reached. After embedding the RGB image is saved as a bmp image so that lossy compression does not occur.

Sandeep Singh and Aman Singh [9] have proposed a combined technique of steganography and cryptography to ensure higher level of data security. In this, the message is first encrypted using DES algorithm. The keys used for DES are then encrypted using RSA algorithm. LSB substitution technique is then used to embed this encrypted message. This technique is more secure and brute force attack is almost impossible.

3. PROPOSED SYSTEM

In the proposed system, we have used hybrid cryptography and steganography to provide a higher level of security for the embedded data. This system provides a mechanism for encrypting the cover image as well as the message to be embedded. RSA and AES algorithms are used for encryption and Bit Plane Complexity Segmentation is used for embedding.

3.1 Overview Of Hybrid Cryptography And Bpcs Algorithm:

Encryption algorithms can be broadly classified into Symmetric key and Asymmetric key algorithms. In symmetric key algorithms a single key is used for encryption and decryption. A symmetric key algorithm requires that both the sender and receiver know the secret key. A message can be encrypted and decrypted as long as the secret key is shared between

the sender and receiver. AES, DES are common symmetric key algorithms. Asymmetric key algorithms use public and private keys for encryption and decryption. The message is encrypted using a public key which is available to anyone. This message can be decrypted only by using a matching private key which is held by the concerned receiver. RSA is a well-known asymmetric key algorithm. Thus asymmetric key algorithms, unlike symmetric key algorithms, eliminate the need for sharing the key over the network. However, asymmetric key algorithms are slower as they require more processing power to encrypt and decrypt the message.

Hybrid cryptography combines symmetric and asymmetric cryptography to ensure the convenience and efficiency of the two systems respectively. Normally, an asymmetric algorithm is used to encrypt the message. The public key used for this encryption is then encrypted using a symmetric key algorithm. At the receiver's end, the symmetric key, which was encrypted using the public key of the receiver, is decrypted using the private key of the receiver. Thus hybrid cryptography uses the advantages of both symmetric an asymmetric systems to provide higher security.

Traditional steganography techniques work by either replacing least significant bits of an image with the data bits to be embedded or by replacing special parts of the frequency components of the cover image. These techniques cannot be used to embed large amounts of data without deteriorating the image quality. Bit-Plane Complexity Segmentation (BPCS) Steganography is a method of embedding data which makes use of the human visual system's characteristic of not being able to perceive shape information in a complicated binary pattern. The algorithm works by replacing "noise"-like regions in the bit-planes of the cover image with the secret data. This technique can be used to embed a large amount of data without causing visible deterioration of image quality.

3.2 System Description:

In the proposed system RSA and AES algorithms are used for image and data encryption and BPCS is used for data embedding. The sender first selects a cover image and encrypts it. The data to be embedded is also encrypted. At the receiver's end, an encrypted image containing encrypted data is obtained. If the receiver has the image encryption key he can obtain the original cover image. If the receiver has the data hiding key he can extract the hidden data but cannot decrypt the image or extracted data. If he has the data hiding and data encryption key he can extract the hidden data from the cover image and decrypt it but cannot decrypt the image. Only if the receiver has the image encryption key, data hiding key and data encryption key he can obtain original image and data.

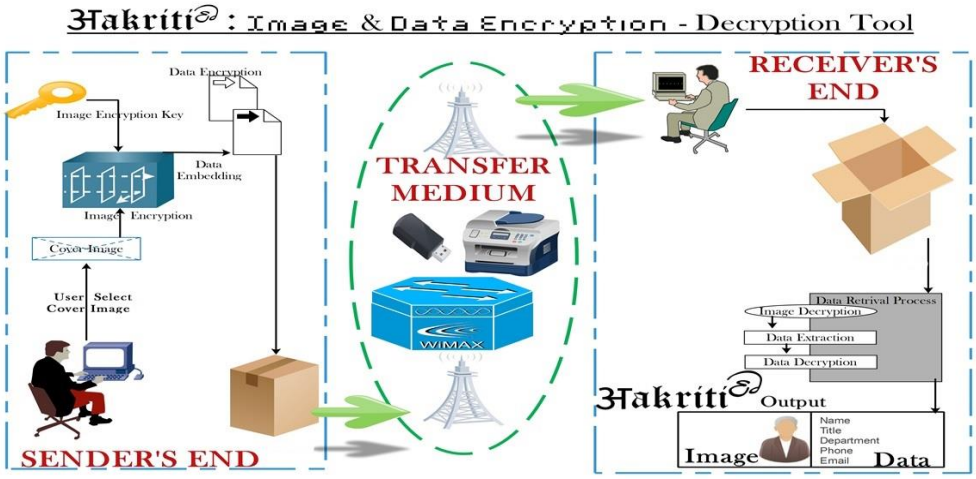

Fig. 2 Aakriti System architecture

3.2.1 Image And Data Encryption:

Hybrid cryptography is used to enhance the security of the image and data. RSA is the asymmetric key algorithm used. RSA uses the receiver's public key for encryption and private key for decryption. The keys are generated using very large prime numbers. AES is the symmetric key algorithm used i.e. it uses the same key for encryption and decryption. AES encrypts data blocks of 128 bits in either 10,12 or 14 rounds with key sizes being 128 bits, 192 bits and 256 bits

respectively. AES is used to encrypt large amounts of data as it's faster than RSA. RSA is better at encrypting a small amount of data.

At the sender's side, AES is used to encrypt the image and data using 128 bit key. The receiver's public key encrypts the symmetric key of AES using RSA algorithm. The encrypted symmetric key and encrypted data are sent to receiver within the encrypted image.

3.2.2 *Embedding Data*:

BPCS algorithm is used for data embedding. BPCS algorithm embeds data in the noisy region of each bit-plane. The cover image is first divided into 24 (8R, 8G, 8B) bit-planes. Each bit-plane is divided into small 8x8 bit blocks. The complexity α of each block is calculated as follows:

$$\alpha = k/M$$

where,
k= no. of pixel borders between black and white pixels
M=total no. of pixel borders
and $0 \leq \alpha \leq 1$.
This technique embeds data in the complex regions of the image. Set the complexity threshold of bit-plane block to *minAlpha*.

The image complexity α is calculated over the whole image and it gives the global complexity of the binary image. If the complexity of the bit-plane block is greater than *minAlpha* then it is used to embed the secret data. Smaller the value of *minAlpha*, larger is the amount of data that can be embedded. A bit-plane that has a smaller complexity value than threshold value is called informative plane. A bit-plane that has a greater complexity value than threshold value is called noisy plane. The secret information is embedded into the bit-plane blocks. In case the bit plane block has a complexity greater than *minAlpha* then the original one can be replaced by the bit-plane block directly. A conjugate processing with the white checkerboard pattern block is taken. The original block is replaced by the new one if the embedded block complexity is less than or equal to *minAlpha.* A record of the conjugate processing blocks is created and embedded into the cover image. The embedding is done in such a way that it does not affect the embedded secret data.

BPCS is used on bit numbers 0, 1, 2 and 3. A modified BPCS method is used for bit numbers 4, 5, 6, and 7. A change in the complexity from the old 8×8 image block to the same block of stego-image gives a new value called *gamma*. α for bit plane numbers 4, 5, 6 and 7 of the image are calculated. If value of α is more than *minAlpha* the bit pattern to be embedded from secret information is created. α of this bit pattern is recalculated. The complex conjugate of stego image is taken if α is less than *minAlpha*. *gamma* value is obtained by calculating change in bit pattern of modified blocks of image. Embed the secret data in the 8×8 blocks if the *gamma* value is smaller than *minGamma.* Avoid the block if the value of *gamma* is greater than *minGamma* and move to next block. Thus BPCS has a large data embedding capacity compared to other methods.

3.2.3 *Extraction Of Data:*

First, the pieces of data having complexity more than *minAlpha* are taken. Secondly, the extra data that was embedded is taken to check the blocks that have taken conjugate processing. For retrieval of data, the blocks are XORed with white chessboard block. Thus, extraction of data is an easy process.

3.2.4 *Image and Data Decryption:*

After receiving the encrypted data and image from the sender, the receiver uses his private key and RSA decryption algorithm to obtain the symmetric key. Using this symmetric key and AES decryption algorithm receiver gets original data and image. Thus with the help of hybrid cryptography only the RSA private key is kept secret.

4. RESULTS AND DISCUSSION

In the proposed system a large amount of data can be embedded using BPCS. Image quality is better. Hybrid cryptography is used for stronger encryption and decryption.

PSNR (peak-signal to-noise ratio) is used to measure image quality. Signal is the original image and noise is the error in reconstruction.

$$PSNR = 10 \times \log_{10}(max_1^{\ 2}/MSE)_{db}$$

$$= 20 \times \log_{10}(max_1^{\ 2}/\sqrt{MSE})_{db}$$

Here, max_i = 255 for a grayscale image.Mean squared error (MSE) is the difference between original and the reconstructed image pixels. It is defined as:

$$MSE = (1/MN) \times \sum_{M}^{i=1} \sum_{N}^{j=1} (|C_1(i,j) - S_1(i,j)|)$$

Here, M = no. of horizontal pixels, N= no. of vertical pixels, C = cover image, and S = stego image. A greater PSNR value and lower MSE is better for image quality.

Fig.3. (a) original image, (b) encrypted image, (c) encrypted and embedded image, (d) decrypted image

5. CONCLUSION AND FUTURE SCOPE

A technique of hybrid cryptography and BPCS steganography was proposed. BPCS enables a larger amount of data to be embedded within an image. The deterioration in image quality is not visible to the human eye. Hybrid cryptography improves security by using the advantages of both RSA and AES algorithms.

The user can thus embed large amounts of data as the system provides a high degree of security and embedding capacity. This technique can be worked upon and improved by using video or audio files as a cover medium.

REFERENCES

[1] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal Of Advanced Science and Technology, Vol. 54, May 2013

[2] C.P.Sumathi, T.Santanam and G.Umamaheswari," A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013

[3] http://en.wikipedia.org/wiki/Digital_watermarking

[4] Hussein Al-Bahadili," A Secure Block Permutation Image Steganography Algorithm", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, September 2013

[5] Ketki Thakre, Nehal Chitaliya," Dual Image Steganography for Communicating High Security Information", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-3 July 2014

[6] Vijay Kumar Sharma and Vishal Shrivastava," A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1

[7] Rosziati Ibrahim and Teoh Suk Kuan," Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108, Published: February 25, 2011.

[8] Babita and Mrs. Ayushi," Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique", International Journal of Computer Science & Engineering Technology (IJCSET)

[9] Sandeep Singh, Aman Singh," An Information Security Technique Using DES-RSA Hybrid and LSB", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)