International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

New robust LSB steganographic technique for increased security

Dipalee Borse

Dr. D. Y. Patil ACS college,Pimpri,Pune -411018
dipa.borse@gmail.com

Abstract: Steganography is fetching attraction because of rapid growth & use of internet as a communication medium. A steganography is a technique of invisible or secret communication. In steganography the secret message can be hidden into a cover media so that no one can realize its subsistence except the sender & receiver. This paper discussed a technique based cryptography applied on numerical values of secret data & coversthe encrypted data into other media, here it is image.So after steganalysis there is less chance of an attacker being able to recover data as the encryption applied on numerical values of data and not the text values itself. This method provides high security.

Keywords: Steganography, Cryptography, Steganalysis, LSB, Spatial domain, PVD, encryption.

1. INTRODUCTION:

With exponential growth and use of internet as a way of communication for exchanging information the information security has become a major issue. To thwart the exploitation, devastation, or malicious modification of the secret information the information hiding technique is used. There are three techniques to hide data are Cryptography, Steganography, Watermarking.

Digital watermarking

Itis hiding information in a carrier like image. A Watermark may contain the copyright information to retain the authenticity & integrity of information. Digital watermark remains constant even through recording, manipulation, compression & de compression, etc.; without affecting the quality of content. The applications of watermark, is to read barcodes on products etc.

Cryptography:

The term cryptography came from Greekword *kryptós* means "hidden, secret"; and *graphein*, means "writing". It is techniques for secure communication in the presence of third parties. In cryptography the original text (plain text) is encrypted and converted into cipher text. The method used to recover original text from the cipher text is Cryptanalysis or decryption.

The types of cryptographic algorithms are:

- Secret key cryptography: It uses a single key for encryption and decryption.
- Public key cryptography: It uses one key for encryption and other key for decryption.
- Hash function:

Steganography:

The term steganography came from Greek words “Steganos” & “*graphein*” which together means “Concealed writing”. Steganography is a science of masking a secret data within another message, image,audio, video or protocol, etc., which results is stego_media so that presence of hidden message is indiscernible and one cannot notice the subsistence of private information. The method used to recover the original message from the Stego_media is called Steganalysis.

Terms used in steganography are:

Secret message: The message is to be hidden into other media.
Cover_media: It is the digital media which will cover the secret message. In this paper we are using binary image.
Stego_media: It is the combination of secret message and the cover_media.

In encryption the structure or sequence of data is altered and looks suspicious which attracts the attention of invaders. This leads to certain actions in order to decrypt it and get secret data.In steganography it hides the existence of any data. So it provides better security.

The niche of steganography is not to replace cryptography but to provide supplement to it. Rather together both can provide two level of security.The proposed algorithm in this paper is also the combination of cryptography & steganography.

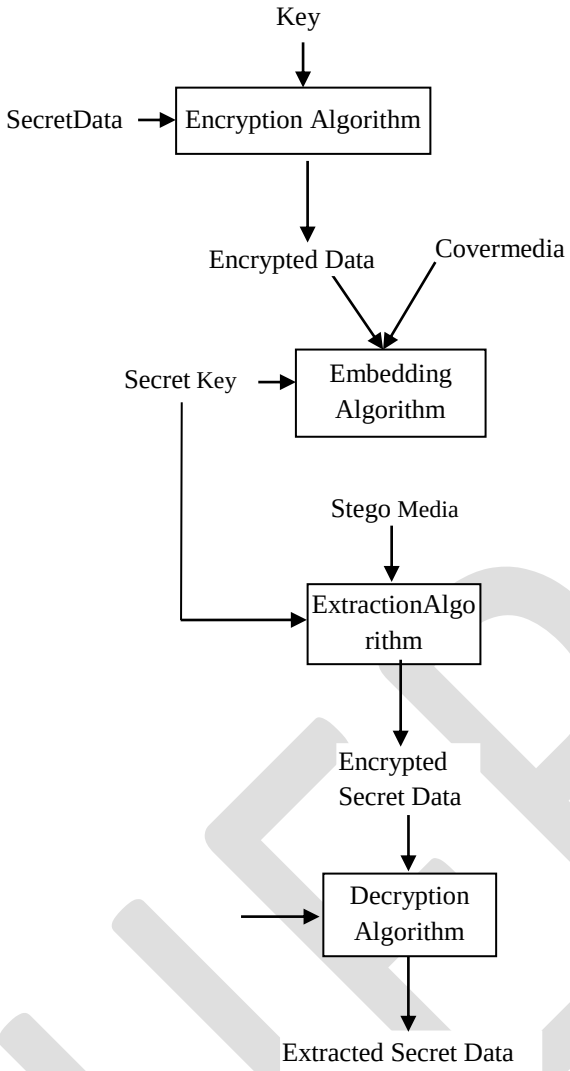
2. LITERATURE SURVEY:

- Ankita Agarwal [1]hasproposed a method with combination of cryptography & steganography. Before hiding a data it encrypted first using simplified data encryption standard(S-DES) .After encryption that scrambled secret message is covered in an image by using alteration component technique. This technique provides two tier security.
- Anil Kumar *et.al.* [2] have proposed an algorithm based on RSA algorithm & Hash-LSB algorithm. Author used RSA algorithm for encryption & Hash LSB method for hiding the encrypted data which is better than RSA-LSB technique. This algorithm gives better image quality gives high PSNR & MSE values because of less variation in image pixels and more security as encryption cannot be break without key as it is probably known to sender & receiver.
- R. Ibrahim *et. al.* [3]have proposed a new algorithm to hide the data Bitmap image. In this algorithm first the secret message is to be transferred into the text file, then zip that text file, Converting the zip file & secret key into binary codes. Encode binary codes using LSB replacement mechanism. It will generate good quality of stego_image as the image distortion cannot be seen by naked eyes. Also the secret message cannot be detected easily by steganalysis. As BMP image is a bigger in size, So it can store large amount of data. Zip technique diminishes the total size of file and improves the security of file.
- Vikas Tyagi [4] has proposed a combination of cryptography and steganography technique to secure the secret data. First the secret information to be scrambled & then that data can be embedded into a cover image. This algorithm gives double layer of security as the original information cannot be extracted even after getting the data from stego-image which is actually an encrypted data. So it is secure & easy to implement practically
- S.K. Bandyopadhyay *et. al*. [5] The authors have proposed alternative method for steganography using reference image for 4 bit images. The binary numbers of the data is stored in an 4 bit gray scale image and the occurrence and x, y coordinates are stored in the different data file. So for steganalysis both stego-image and data file must be available. With one of them one cannot determine the secret message. As a result this approach is more secure and time complexity of algorithm is simple and proportional to o(n).
- Amanpreet Kaur, *et. al* [6]has proposed 'First component alteration technique'. Each image have an array of pixels & each pixel is a combination of Red, Green, Blue values. In 'First component alteration technique' the bits of first component (i.e. blue) of pixels of image can be substituted with bits of each character in secret data . As the visual perception of blue in R, G, B is low, and on changing it slightly will not disturb the color intensity of image. So it diminishes the picture distortion and it is unnoticeable by human eyes. Also gives increased PSNR than Pixel-Value Differencing (PVD) scheme, LSB3 etc. This scheme can integrate more secret data with improved image quality.
- V. K. Sharma *et.al* [7]have proposed improved LSB substitution mechanism to hide image in image which minimizes the revealing possibility. This approach is hiding the secret image into cover image using logic gates, which improves/increase PSNR of stego-image than First component alteration technique'. This method can be used for 24 bit color & 8 bit gray scale image by adding conversion algorithm of color image into gray scale image. Also the number of steps are less which reduces the complexity of algorithm. The limitation of this algorithm is; As the number bits increases the PSNR values will be decreased i.e. the quality of stego-image will be reduced.
- Al-Shatnawi [8],The author has proposed a new method to hide secret message by finding the same or identical bits between cover image & secret message. Also set the locations of hidden data bits to a binary file which can be helpful at the time of retrieval of secret message. By this technique the maximum bits in image remain unchanged so the quality of image will never be degraded.
- Dr. T. Ch. M. Rao et. al. in [9] This algorithm proposed an improved data hiding technique continuing the research in [8]. This algorithm does the searching of identical bits from cover image & the secret text. The 8 bit of secret character is divided into 3 segments such as (3bits; 3bit; 2 bits) so that the first 3bits can be matched & stored in 8 bits of Red, another 3 bits in green & remaining 2 bits in blue in a RGB pixel of cover image. & all non-identical bits can be stored in least significant bits of pixel. This algorithm is highly efficient and gives better resolution than existing models.

3. PROPOSED METHOD:

In the proposed method the encryption of ASCII values of secret data before embedding is introduced.Encryption can be done by manipulating these values and that will result new data set of ASCIIs. This data set is converted into binary format after that traditional least significant bit technique is applied to hide those data bits into cover_image. It gives us combination of encrypted

data and cover_image into a stego_image or stego_gramme. In this paper the cover image used is binary image.While steganalysis the data extracted by someone will be encrypted data. The data looks suspicious but it is very hard get original data by applying cryptanalysis as the numbers are manipulated not the characters, which improves the security of data. The following Figure1 &algorithmshows procedure of embedding the secret data



Algorithm:

Inputs: Cover_image, Text file.

Output: Stego_image

Step 1: Input Text to be hidden

Step 2: Input cover_image (binary image)

Step 3: Convert the secret text to ASCII values

Step 4: Encrypt ASCII values using symmetric key encryption

Step 5: Embed the encrypted data into cover_image

Step 6: That will generate stego_image

Figure 1: Procedure of proposed method

4. EXPERIMENTAL RESULTS:

The traditional LSB methods are easy to crack by the attackers by using Steganalysis. So in the proposed algorithm, encryption technique is used before LSB embedding which provides greater security because the encryption is done on ascii values of data. This proposed method is applied on binary images. This method also gives good image quality.The proposed method gives higher security for the secret data to be hidden in the cover_image. The results of algorithm are as shown in the Figure 2 &Figure 3

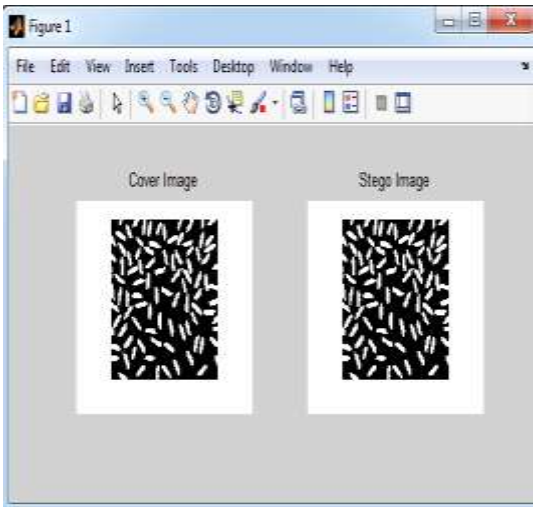


Figure 2:
Image Name: ipexrice_05.png
PSNR: 52.8957
MSE: 0. 3338

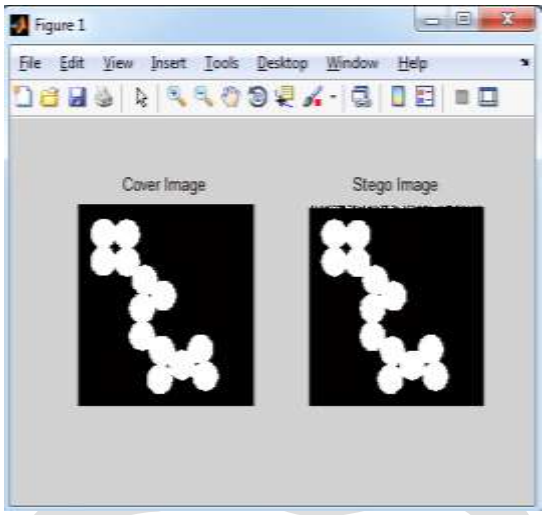


Figure 3:
Image Name:circles.png
PSNR: 49.2268
MSE: 0.7770

5. Conclusions:

Cryptography & Steganography are two major and ancient data security techniques.But only cryptographic or only steganographic techniques may lack in security sometimes. So in this proposed scheme cryptographic & steganographic LSB technique are combined to get greater data security. As the encryption is done on the numerical values that is ascii values of data which is ultimately the binary encryption which is hardly attracted and revealed by eavesdropper. That scrambled data is then concealed by the other image by using LSB technique which is easy to implement. As a result it provides two tier higher security. Also It provide good PNSR & better quality stego_image. In this paper the algorithm is applied on binary images only. Finally we conclude that proposed approach gives higher security with good image quality.

REFERENCES:

[1] Ankita Agarwal, "Security enhancement scheme for image steganography using S-DES technique" , International journal of Advanced Research in computer science & software engineering, ISSN : 2277 128X, Volume 2, April 2012

[2] Anil Kumar, Rohini Sharma, " A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International journal of Advanced Research in computer science & software engineering, ISSN : 2277 128X, Volume 3, April 2013

[3] R. Ibrahim and Teoh Suk Kuan, "Steganography algorithm to hide secret message inside an Image", Computer application and technology, February 2011.`

[4] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar., " Image Steganography using Least significant bit with cryptography", Journal of Global Research in Computer Science, ISSN – 2229-371X, Vol, No. 3, 2012 .

[5] S.K. Bandyopadhyay and I. K. Maitra, "An Alternative approach of steganography using reference image", International journal of advancements in Technology, ISSN 0976-4860, (June 2010).

[6] Amanpreet Kaur, , Renu Dhir, and Geeta Sikka, "A New Image Steganography Based On First Component Alteration Technique", International Journal of Computer Science and Information Security, ISSN 1947-5500. Vol. 6, No. 3, 2009.

[7] V. K. Sharma and V Shrivastava, "A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize detection", Journal of Theoretical and Applied Information Technology , ISSN: 1992-8645. Vol. 36 No.1, 2012.

[8] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality",Applied Mathematical Sciences, Vol. 6, 2012, no. 79.

[9] Dr. T.Ch.Malleswara Rao et. al.," A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality", Int. Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 3, Issue 6, 2013,

[10] N.F. Johnson and S. Jajdodia," Exploring steganography: Seeing the Unseen", IEEE computer, pp 26-34, 1998.

[11] Krati vyas, B.L.Pal, "A proposed method in image steganography to improve image quality with LSB technique", *International Journal of Advanced Research in Computer and Communication Engineering*, ISSN (Print) : 2319-5940, Vol. 3, January 2014.

[12] Dipalee Borse, Shobhana Patil, "Review and Analysis of Multifarious SpatialDomain Steganography Techniques", *International journal of engineering research and technology*, ISSN: 2278-0181, Vol 4, January 2015