International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 4, April 2015, PP 28-33
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Secure Data Hiding

Himanshu Chhabra
B.E Student/Dept. of Computer Engineering
Shah & Anchor Kutchhi Engineering College
Mumbai University
Mumbai, India
himanshu.chhabra9304@gmail.com

Dhiraj Thakur
B.E Student/Dept. of Computer Engineering
Shah & Anchor Kutchhi Engineering College
Mumbai University
Mumbai, India
dhiraj_thakur37@yahoo.in

Riddhi Thacker
B.E Student/Dept. of Computer Engineering
Shah & Anchor Kutchhi Engineering College
Mumbai University
Mumbai, India
riddhi_thacker@yahoo.com

Rupali Kale
Asst. Prof./Dept. of Computer Engineering
Shah & Anchor Kutchhi Engineering College
Mumbai University
Mumbai, India
kalerupalis@gmail.com

Abstract: *Steganography is an ability of concealing information inside the cover in such a way it looks like simple cover. The goal is data hiding without much deteriorating the quality of the picture under consideration and successfully retrieve the data when needed. This approach focuses first on encrypting the secret data and then hiding the existence of the cipher so that any attacker would never know that a secret message is being passed over the insecure channel. This hiding is done using steganographic technique using image as a cover media. In this method, secret data is initially encrypted using Advance Encryption Standard (AES) and steganography scheme is used for hiding the cipher text into a grey cover image. The encryption key is sent securely through the exposed insecure channel using Diffie-Hellman Key Exchange Protocol. On reception of the stego-image, it undergoes extraction process. The extraction model is actually the reverse of the embedding model. The stego-image is resulable.*

Keywords: *Steganography AES, Cover Image, Stego-Image, Key Exchange Protocol.*

1. INTRODUCTION

Data hiding [1] using image steganography is the process to hide secret data into a selected cover media. The proposed technique has been applied to various test images and gives a Peak Signal to Noise Ratio above 49 dB and the stego image was successfully reused to hide new secret data [1, 2].Generally the types of media used as cover are text, images, videos etc [6]. The technique used is lossless and the image under consideration is reusable. To increase the security the message is first encrypted using Advance Encryption Standard technique. The encrypted data is then embedded into the cover image. The key used in AES [9] technique will be shared between the sender and the receiver using Diffie Hellman Key Exchange Protocol. The system block diagram is as shown below:

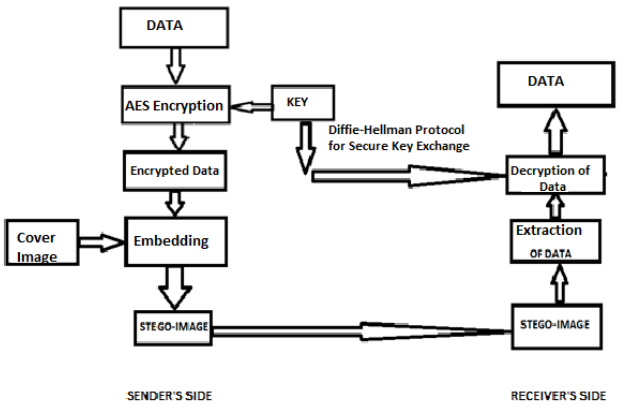


Figure.1 *Block Diagram of the System*

2. METHODS

The cipher text obtained using AES is embedded inside the cover image. For example, the "Dice" image is used as cover media.

2.1 Embedding Process

The steps involved are as follows:

1) Find the Peak point (PP) and the Zero point (ZP) in the cover image [1, 2]. Peak point is the intensity value in the image for which maximum number of pixels occurs and Zero point is the intensity value in the image for which minimum number of pixels occur. In the Dice image, the pixel value 0 occurs 1963 times which is the peak point and the pixel value 173 occurs 9 times which is the zero point.1963 (bits) is also the embedding capacity. Following is the algorithm for finding the peak and zero point:
    - Read the pixels of the cover image.
    - Count the occurrences of each pixel value.
    - Find the pixel with the maximum and minimum occurrences which will be the peak and zero point respectively.
2) Convert the secret data into binary form in 8 bit format.
3) Scan the cover image once in a sequential order. If PP > ZP, then shift each pixel value in the range, (ZP+1, PP−1), to the left-hand side by decreasing the pixel value by one unit. If PP < ZP, then shift each pixel value in the range, (PP + 1, ZP – 1), to the right-hand side by increasing the pixel value by one unit [2]. For example, in Fig. 2, PP < ZP since 0 < 173, each pixel value in the range, (1, 172), are increased by one.
4) Scan the whole image once again in the same sequential order to embed the data. While scanning, when the pixel with the peak point value is encountered and the bit to embed is "1", then shift the pixel value from PP to ZP by one [2] which can either be PP+1 if PP<ZP or PP-1 if PP>ZP, the pixel value does not change if the bit to embed is "0". The resultant image is the Stego-Image

(a) (b)

Figure.2 *Dice Image (a) original image (b) stego image (PSNR:49.706dB) (Size:256*256)*

2.2 PEAK VALUE INSERTION

After embedding the secret data into the cover image there is a possibility that the peak value may change. The peak value is required for extracting the secret data from the stego-image. This arises the need of storing the peak value into the stego-image. The last pixel of the cover image is reserved for storing the peak value, hence the data bit cannot be embedded at this pixel position.

2.3 DE-EMBEDDING PROCESS

To obtain the secret data from the cover image de-embedding process is used. The following algorithm is used to perform de-embedding:

1) Obtain the peak point from the last pixel position of the stego-image.
2) Scan the stego-image in the same sequential order that was used in the data embedding process, at the same time, a bit "1" is extracted if the pixel value is PP+1 and a bit "0" is extracted if the pixel value is PP [2], for PP<ZP
3) Similarly, a bit "1" is extracted if the pixel value is PP-1 and a "0" is extracted if the pixel value is PP for PP>ZP
4) Once the binary stream is obtained it is converted into its text equivalent and the cipher text received undergoes decryption which yields the secret message.

3. RESULTS AND DISCUSSION

3.1 PSNR of the Stego-Image Versus the Original Image

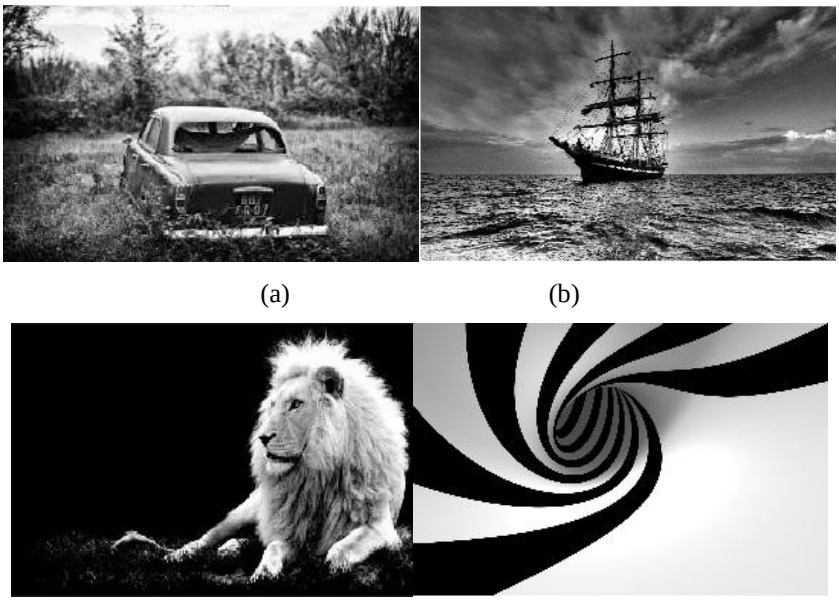
3.1.1 TABLE

Test results of 5 test cases are as follows

Table.1*Test Cases*

IMAGE	PSNR OF STEGO IMAGE(dB)
Car	50.247
Dice	49.706
Ship	49.451
Lion	55.987
Spiral	59.927

3.1.2 FIGURE



(a) (b)

(c) (d)

Figure. 3 *Test Images (a) Car (b) Ship (c) Lion (d) Spiral*

3.2 Result Analysis

The secret message is successfully embedded into the grey scale cover image. The Stego image has PSNR value above 49 dB and has no visible physical changes and the secret message is obtained successfully.

The results of the following Case is:

1. Consider a Secret Message “Hello Everyone!!!” and the Encryption Key chosen is 20.
2. The Cover Image Selected is

The Peak point and the Zero point of the selected cover image is as follows

- Peak Point: 0 and number of pixels: 1963

- Zero Point: 173 and number of pixels: 9
- Thus, capacity for embedding data is 1963 bits.

3. Encryption of the input secret text is performed using the secret key, and the cipher is obtained
    - Input text: Hello Everyone!!!
    - Encrypted Text : DRkP6sd9ckQ6g7WLrdO9SLF/kUrjn6zuGdifGsQu3s0=
4. The Cipher text thus obtained is converted to Bit Stream, the length of the Stream can be computed as Bit-Stream Length=8*number of characters in the encrypted text.For the current scenario Bit-Stream Length=8*44=352 bits.
5. The Bit-Stream obtained is embedded inside the cover image and following Stego-Image is obtained.

Peak Signal to Noise ratio (PSNR): 49.671

6. The Stego Image is sent to the Receiver, the image can withstand zip and email compressions. Thus it can be zipped and sent using email to the intended recipient. If the maximum capacity of the cover image is reached, user can make use of same cover image and same encryption key for embedding the remaining message and can zip the obtained Stego images into a file/folder and send at once.
7. The Received Stego image undergoes the extraction process and the Bit-Steam is extracted and the stream is converted back into its character equivalent and the Cipher text is obtained
    - Cipher Text:DRkP6sd9ckQ6g7WLrdO9SLF/kUrjn6zuGdifGsQu3s0=
8. The Decryption Key entered by the user must match with the Encryption Key if it does decryption of the cipher text takes place and the secret message is obtained, else the decryption doesn't take place.
    - Secret Message: Hello Everyone!!!
9. The Stego Image can be used again as a cover image and new message can be embedded into it, which means the image is Reusable.
10. Computation time for embedding and de-embedding are as follows for current scenario
    - Embedding Time: 4 seconds, the time is inclusive of encrypting the secret text, its conversion into binary form, reading pixels of the cover image, processing it and forming the Stego image
    - De-Embedding Time: 4 seconds, the time is inclusive of reading the Stego image, extracting bits, conversion to character form and decryption.
    - The time varies depending upon the cover image and input text and computing efficiency of device.
11. The encryption of the secret text adds to the security and robustness.

3.3 Further Enhancement

The embedding capacity can be increased by selecting multiple pair of peak and zero points [1]. The embedding procedure remains the same with following changes:

1) As a record of occurrences of each pixel value is maintained, consider for a three level embedding process a pair of three PP and ZP such that they do not overlap are selected from the record.

2) If pp1,pp2,pp3 are three peak points and zp1,zp2,zp3 are three zero points such that pp1<pp2<pp3 and zp3<zp2<zp1 then the recommended order of using the pairs will be [pp1,zp1] , [pp2,zp2] , [pp3,zp3], there are no restrictions on zero points, they can form a pair with any peak point p1, p2 or p3 but the order of using them must include p1 first followed by p2 and then p3.This is necessary to avoid loss of data

3) For the first iteration it is as explained before, for remaining iterations concatenate the bit stream of the secret data of the previous iteration with eight "0" followed by the PP of the next iteration in its binary 8 bit equivalent form where the eight "0" separates the secret data from the PP of the next iteration.

4) During the extraction process the eight bits followed by the eight "0" at the end of the extracted bit streams will be used as the peak value (PP) for the next iteration.

The above procedure is continued until the extracted bit stream does not contain a stream of eight "0" at the end.

4. CONCLUSION

The algorithm used can successfully embed as well as extract the secret text from the cover image. The experiments with the test image show that the algorithm yields images with PSNR not less than 48db.The Algorithm used is easy to implement, has uniformity and execution time is short and is simple. The Stego image is reusable. This technique is useful in various domains like military where confidentiality and Secrecy are very important. The procedure used yields file having png format which is a lossless format thereby avoiding loss of data. The stego images can withstand zip image compression. Additionally encryption of the secret text adds up to the security. Its overall performance is good.

REFERENCES

[1]. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding" in IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006.

[2]. Y.-C. Li, C.-M. Yeh and C.-C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility" in Digital Signal Processing, vol. 20, no. 4, pp. 1116–1128, 2010.

[3]. J.Anita Christaline, D. Vaishali , "Image Steganographic Techniques With Improved Embedding Capacity and Robustness" in IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 IEEE MIT, Anna University, Chennai, 978-1-4577-0590-8/11, June 3-5, 2011.

[4]. Jagbir Singh, Savina Bansal and R.K. Bansal, "Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013.

[5]. Y.Yu Tsai, D.S. Tsai and C.L. Liu, "Reversible data hiding scheme based on neighbouring pixel differences", Elsevier Journal of Digital Signal Processing, 2012.

[6]. T. Morkel, J.H.P. Eloff and M.S. Olivier, "An overview of image steganography", in Proc. Of 5th Annual Information Security South Africa Conference (ISSA), 2005.

[7]. Rajkumar Ramaswamy, Vasuki Arumugam, "Lossless Data Hiding based on Histogram Modification" in The International Arab Journal Of Information Technology, Volume 9, No. 5, September 2012.

[8]. A.Cheddad, Joan Condell, K. Curran and P. McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume 90, pp. 727-752, 2010.

[9]. William Stallings, "Cryptography and Network Security" 5/e, Chapter 5 –"Advanced Encryption Standard".

AUTHORS' BIOGRAPHY

Himanshu Chhabra is currently pursuing B.E, Final Year in the Department of Computer Engineering from Shah and Anchor Kutchhi Engineering College, Mumbai, India.

Dhiraj Thakur is currently pursuing B.E, Final Year in the Department of Computer Engineering from Shah and Anchor Kutchhi Engineering College, Mumbai, India.

Riddhi Thacker is currently pursuing B.E, Final Year in the Department of Computer Engineering from Shah and Anchor Kutchhi Engineering College, Mumbai, India.

Rupali Kale is currently working as Asst. Professor in the Department of Computer Engineering from Shah and Anchor Kutchhi Engineering College, Mumbai, India. She completed her B.tech from Usha Mittal Institute of technology for women,SNDT University, in 2004. She completed her ME from PIIT Panvel, Mumbai University, in 2014.