Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Private key Steganography using DCT

Jagroop kaur*

Dept of Computer Science & Engg.

Guru Nanak Dev University

Amritsar, India

Abstract-Steganography is the art and science of invisible communication. This paper proposed a technique implement steganogaraphy with private key to hide the data into an image. In this technique it encrypt message using secret private-key then embedded the data in image. Decryption is done only by giving the correct private key. Each selected pixel will be used to hide data by using LSB method.

Keywords: private key, decryption, steganography

1. Introduction

Security of information is one of the most important factors of information technology and communication. Cryptography is a technique for securing the confidentiality of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Sometimes it is not sufficient to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is ideal and can be compromised. Once the presence of hidden information is exposed or even supposed, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

2. Literature Survey

Dragan [1] has provided an general idea of some steganographic methods using DCT transform, LSB technique and one-time pad keys**.** This method uses the security of one-time pad technique and the simplicity of LSB combined with DCT technique. They also tested this method using steganalysis tests and steganographic tools. The DCT transform assures robustness to JPEG compression attacks.

Kumar et al.[2] have proposed a new steganography method called JMQT based on modified quantization table. This steganography method is compared with steganography method JPEG-Jsteg**.** Two parameters namely Capacity and Stego-size has been compared. More data can be embedding using this method as compared to JPEG-JSteg. So JMQT provides better capacity and JPEG-Jsteg provides better stego-size.

Huayong et al.[3] have reviewed steganography and steganalysis based on digital image. Concept and principle of steganography and steganalysis are illustrated. Spatial domain and transform domain embedding methods are generalized. And the recent advances in steganalysis are recapitulated. Then the performance specification of image steganography is discussed. Finally some new trend and problems faced are also discussed like notion of security and capacity for steganography needsto be investigated deeply.

JIANG et al.[4] have presented forward steganographic method based on the JPEG digital images. Instead of dividing cover-image into 8×8 blocks, non-overlapping blocks of 16×16 pixels is used. With their proposed quantization table , the DCT coefficients are quantized and embedded the secret messages.The experiment results show that their method has the larger steganography capacity and better stego-image quality than the other methods

Kumar et al.[5] have proposed Coherent Steganographic Technique using Segmentation and Discrete Cosine Transform (CSSDCT). The cover image is divided into 8*8 blocks and DCT is applied on each block. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing techniques. In future the technique can be verified for robustness.

Marwaha et al.[6] have proposed an advanced system of encrypting data that combines the features of cryptography, steganography along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems.

Almohammad A. et al.[7] evaluates the performance and efficiency of using optimized quantization tables instead of default JPEG tables within JPEG steganography. They found that using optimized tables significantly improves the quality of stego-images. Experimental results show that the proposed approach can provide a higher information-hiding capacity than the other methods tested.

3. Problem Definition:

This dissertation proposed a new Private-key based steganography. As shown in literature survey private key based steganography is neglected by many researchers so far. So this dissertation focuses on a providing a new algorithm which will use the feature of steganography and also implement private key to improve the security over the existing techniques.As proposed algorithm also come up with some potential overheads so overheads are also evaluated in this research work. Different image parameters are also calculated to evaluate the performance of the proposed algorithm.

4. Methodology

In order to provide high security, here we elaborate the steganographic system using DCT with private key. Private key is secret key used for encoding /decoding known only to the parties that exchange secret messages. First message is embedded in image using encoding algorithm and then extracted using decoding algorithm.

Encoding Algorithm:

1.Take an jpeg image which can be RGB Or gray.
2.Apply DCT on image which is to transform the signal or image from the spatial domain to the frequency domain.
3. Encode message that is in ASCII format to the LSB with private key.
4. Save image as .bmp which is stego image.

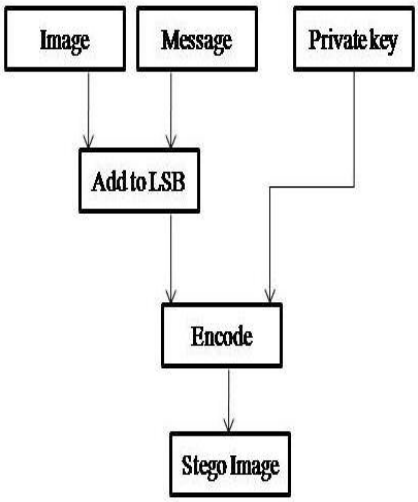

Fig 1: Encoding process

Decoding algorithm:

1.Stego image is given.
2.Apply private key to decode message from stego image.
3.Apply IDCT on image.bmp.
4.Extract message from stego image.

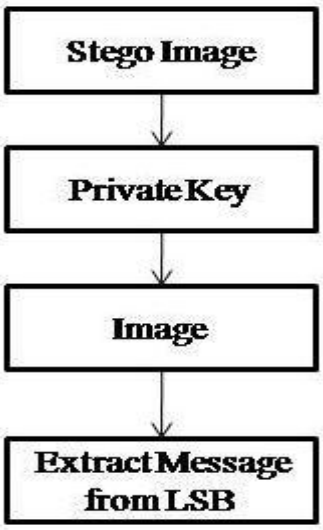

Fig 2: Decoding process

5. Performance Metrices

For performance analysis, Cover Image (CI) and Payload (PL) of any size and formats are considered. Different evaluation parameters are considered for performance analysis.

a)Peak signal to noise ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e. it measures the percentage of the stegano data to the image Percentage. The PSNR is most commonly used to measure the quality of reconstruction in an image; by comparing the stego image with the original image.

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

b)Mean Square Error (MSE): It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

where

f represents the matrix data of our original image

g represents the matrix data of our degraded image in question

m represents the numbers of rows of pixels of the images and i represents the index of that row

n represents the no. of columns of pixels of the image and j represents the index of that column

$\mathbf{MAX_f}$ is the maximum signal value that exists in our original "known to be good" image.

c) Maxmium difference: The maxmium difference between original image and stego image.

d) Minimum difference: The minimum difference between original image and stego image.

e) Average difference: The average difference between original image and stego image.

f) Normalized absolute error: Normalize absolute error is used to express the inaccuracy in a measurement.

6. Results

The method used in this experiment were coded in Matlab 7.10.0(R2010a). The results were derived using an RGB image of size 65.7 KB After embedding message in image we get stego image of size 97 KB.The original image and stego image were given below respectively. The results were derived by using functions that were evaluated or difference between original image and stego image given below in table.

Fig 3: Original Image

Fig 4: Stego Image

Table 1: Evaluated parameters

MSE	556.4095
PSNR	20.6769
MAX DIFF	1
NAE	8.9316e-006
AVG DIFF	6.9152e-004
MIN DIFF	-1

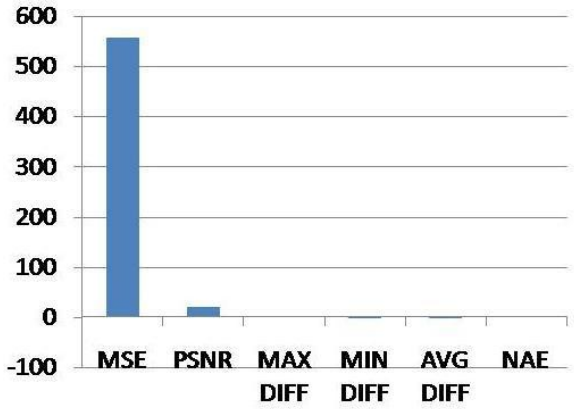

Chart: histogram of parameters

7. Comparison

As steganography system can be used with both public and private key .We are doing comparison between them:

Table 2: Comparison of public/ private key

Public key	Private key
Uses public key and private key both..	Uses single key i.e private key.
A public key for encryption and private key for decryption.	Same private key for encryption and decryption
No need of agreement of two parties.	Both parties must agree to use the same private key.
Public key used for encryption does not need to remain secure.	It is much faster than public key , is easier to implement, and requires less processing power.

8. Conclusion

Steganography is the art and science of invisible communication. It is a technique which keeps the existence of the message secret. Private key steganography is much faster than public key steganography, is easier to implement,generally require less processing power.Comparison of public and private key steganography is done in this research work.Both public and private key steganography system are secured and having its own advantages and disadvantages but it has been found that in certain critical cases private key provide better results.

References

1. Drăgan A.F." Another Steganographic LSB-based Function"Communications (COMM), 2012 9th International Conference Page(s): 311 – 314,IEEE 2012.
2. Kumar A. and Sachdeva S." Colour Image Steganography Based on Modified Quantization Table" Second International Conference on Advanced Computing & Communication Technologies, Page(s): 309 – 313, IEEE 2012.
3. Huayong G., Mingsheng H. and Qian W." Steganography and Steganalysis Based on Digital Image" 4th International Congress on Image and Signal Processing,Vol 1, Page(s): 252 -255, IEEE 2011
4. JIANG C.L, PANG Y.L and Zhu Y." A Steganographic Method based on the JPEG Digital images" Computer Research and Development (ICCRD),3rd International Conference, Volume: 3 , Page(s): 35 – 38,IEEE 2011
5. Kumar K.B.S,Raja K.B., Chhotaray R.K.and Pattnaik S." Coherent Steganography using Segmentation and DCT" Computational Intelligence and Computing Research (ICCIC),IEEE International Conference Page(s): 1 – 6 , 2010
6. Marwaha P. and Marwaha P." VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES" Second International conference on Computing, Communication and Networking Technologies, Page(s): 1 - 6 , IEEE 2010
7. Almohammad A., Ghinea G. and Hierons R. M. "JPEG steganography: a performance evaluation of quantization tables", IEEE International Conference on advanced information networking and applications AINA '09, Bradford, pp. 471-478, IEEE May 2009.

