Review and Analysis of Multifarious Spatial Domain Steganography Techniques

Dipalee Borse
Department of computer science
Dr.D.Y. Patil ACS college,
Pimpri - 411018

Shobhana Patil
Department of computer science
Dr. D.Y. Patil ACS college,
Pimpri - 411018

***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 which results in the stego_media, so that no one can realize its subsistence except the sender & receiver. There are various medium used as a cover such as image, audio, video, protocol, DNA etc. But image is mostly used as a cover media. There are several type and techniques of steganography, each having its own confines and rewards. In this paper we have explicated & analyzed the different spatial domain steganography techniques.**

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

I. INTRODUCTION

The use of internet as a communication media is increasing exponentially day by day.

Information hiding techniques can be used to preclude the malicious modification, use or obliteration of the secret data. Information Security is process of keeping information secure, protecting its accessibility, integrity, and secrecy. There are several data hiding mechanisms like Steganography, Cryptography, and watermarking.

Steganography is process of the hiding of a secret data within another media such as image, so that the presence of the hidden message is indiscernible. Steganalysis is reveals the secret data form stego media. Cryptography referred to as *encryption*, which is the process of converting ordinary information (plaintext) into unintelligible text (cipher text). Decryption is a process of altering inarticulate cipher text back to plaintext. Watermarking is a hiding data in a carrier media like image. A Watermark may contain the copyright information to preserve the authenticity & integrity of information. Digital watermark remains constant even through recording, manipulation, compression & de compression, etc.; without affecting the quality of content.

Steganography hide the subsistence of secret data so there is less chance of being cracked as compared to cryptography as in cryptography it encrypt the data and modify its structure which become suspicious to the attackers and they may apply decryption algorithms to access the secret data. Steganography's niche in security is to supplement cryptography, not replace it rather it can be better together.

II. OVERVIEW OF STEGANOGRAPHY

The word *steganography* chains the ancient greekwords *steganos* means "protected", and *graphie* means "writing". The first recorded use of the term was in 1499 by Johannes Trithemius. In ancient times, various entities were used as a cover for the secret message are invisible inks, wax tablets, shaved head of a trusted slave, etc. In digital steganography digital images, video, audio, DNA, Protocol, etc., are used as a cover media to hide the secret information Figure below shows the general process of steganography:

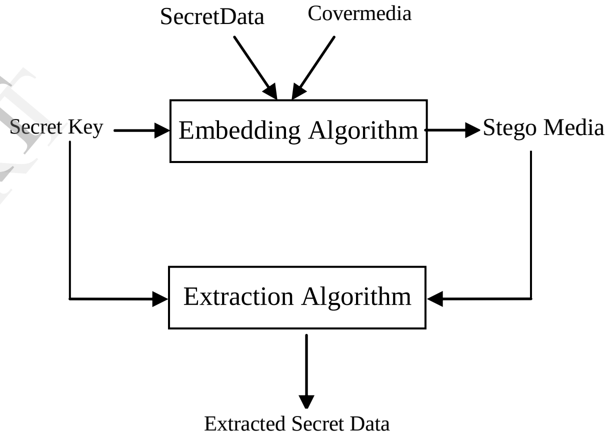

Figure 1: Process of steganography

Steganography can be categorized as image steganography, audio steganography, video steganography etc.

Image Steganographic Techniques

Image steganography techniques can be divided into following domains.

A. Substitution or Spatial Domain
B. Transform Domain
C. Statistical
D. Distortion
E. Cover Generation

Spatial Domain Methods: Spatial steganography directly alter bits in the image pixel values in hiding data. Least significant bit (LSB) steganography is the simplest techniques to hides a secret message in the LSBs of pixel values very less perceptible misrepresentations. Changes in the value of the LSB are indiscernible for human eyes.

Transform Domain Technique: Various transformations are used on the image to hide information in it. The process of embedding data in the frequency domain of a signal is sturdier than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques is advantageous than spatial domain as they hide information in those areas of the image which are not affected in compression, cropping, or other image processing techniques. Transform domain techniques may outrun lossless and lossy format conversions

Distortion Techniques: Decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a stego object is created by applying a sequence of modifications to the cover image.

Statistical Techniques: These are also called as model based technique be interpreted by humans. This technique is vulnerable to rotating, cropping, scaling attacks and also all the watermarking attacks.

Cover Generation Techniques: In this technique, digital cover is generated only for the purpose of being a cover for secret communication .Regular expressions and mimic functions are used to generate a cover.

III. LITERATURE REVIEW

A. R. Ibrahim and Teoh Suk Kuan. [1]

The authors have proposed a new algorithm to hide the data Bitmap image. This algorithm used zipping technique. First the secret message is to be transferred into the text file, then convert that text file into zip file, Altering the zip file & secret key into binary codes. Encode binary codes using LSB replacement mechanism. It will generate better quality of stego_image as the image distortion cannot be seen by naked eyes. Also the secret message cannot be spotted easily by steganalysis. As BMP image is a bigger in size, So it can store large amount of data. Zip technique minimizes the total size of file & improves the security of file.

B. S.K. Bandyopadhyay and I. K. Maitra[2]

The authors have proposed alternative method for steganography using reference image for 4 bit images. The binary numbers of the data is stored in a 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).

C. Amanpreet Kaur, Renu Dhir, and Geeta Sikka,[3]

The scheme 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 affect the color intensity of image. So it reduces 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.

D. V. K. Sharma and V Shrivastava[4]

This proposed improved LSB substitution mechanism to hide image in image which minimizes the detection 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 numbers 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.

E. Al-Shatnawi [5]

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. It is different from [3], as here the author uses color image and [3] uses 4-bit binary images as a cover.

F. *Dr. T.Ch.Malleswara Rao, Koyi lakshmi prasad[6*

This algorithm proposed an improved data hiding technique continuing the research in [5]. 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.

G. Vikas Tyagi [7]

This scheme has proposed a combination of cryptography and steganography technique to secure the secret data. First the secret information to be encrypted & 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

H. Ankita Agarwal [8]

This author has proposed 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 securities.

I. *Anil kumar, Rohini Sharma[9]*

Author has 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.

J. Da-Chun Wu, Wen-Hsiang Tsai [10]

Authors have proposed Pixel value differencing (PVD) method for embedding secret messages into a 256 gray-valued cover image. In PVD, the number of bits to be embedded in an image changes in consecutive pixel. It can store large amount of data, without losing properties of an image. PVD method is based on storing the information in the edges of an image as it cannot be noticed by naked eyes.Absolute Range of gray values (0, 255) is divided into smaller ranges and each range defined by lower and upper boundary. An absolute difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. Width of the range is calculated .The range near to 0 represents smooth area with small width and the ranges near to 255 represent contrast area with larger width.Embedding process take place in both pixels in the block which will generate new gray scale values for these pixels. Then, the difference value is replaced by a new value to embed the value of the secret message. This proposed scheme can hide more data with superior quality of stego -image.

Butcolor pixel-components may exceed the range 0~255 in the stego image when applying PVD method.

K. K. Mandal and Debashis[11]

Authors have proposed a steganographic approach on color images, using PVD. They have removed drawback of [10] here. It will provide more security with better stego image quality than [10] method. First embed bits in 1st pixel block (two consecutive non-overlapping pixels) of the red component matrix, then in 1st block of green component matrix and lastly in blue, then again 2nd block of red matrix and so on. In the proposed method we have used the original PVD method to embed secret data. If pixel value surpasses the range, then check the bit-stream to be hidden. If MSB of the selected bit stream is 1 then we embeds one less number of bits, where MSB position is discarded from it; otherwise the bit number of hidden data depends on width of range. If the pixel value exceeds range again, then embed the value at one pixel, rather than both pixels of the pixel block, which will not exceed the range after embedding; where the other pixel is kept unchanged.

L. Dinesh D. Patil & S. M. Bansode.[12]

A novel stegnographic approach using four and eight pixel-value differencing is proposed.
In the proposed system blocks of 2 (PVD), 4 and 8 pixels size are used to embed data in images. The data hiding procedure is independent in each block.
The paper proposed modified approach termed as Block based PVD extends from 2-pixel block to 4 and 8-pixel block differencing where large amount of information can be embedded. It improves security of the data to be hidden with increasing embedding capacity. The proposed technique obtained better visibility with better PSNR ratio.

M. Hsien-Wen Tseng1 and Hui-Shih Leng.[13]

This proposed technique design a new quantization range table based on the perfect square number. For each pixel value choose the nearest perfect square number range as well as width of the range is defined. The width of the range is no longer a power of two, and if the difference value islocated in the first subrange, there is no modification needed.If we choose aproper width for each range and use the proposed methodwe can obtain better image quantity and higher capacity.The theoretical analysis shows the proposedscheme is well defined and has larger capacity and higherPSNR than [10].

IV. COMPARATIVE STUDY:

Terms used:
PSNR: Peak signal to noise ratio
DHC: Data hiding capacity

Ref. No	PSNR	DHC	Security	Description
[1]	High	High	High	Zipped data covered in BMP file
[2]	High	Low	High	Use of reference file requires more size so increase in hidden data the size for 2 files in this algorithm also increases.
[3]	High	High	Low	Change in blue pixel reduces image distortion
[7]	Low	High	High	It is more secure as it uses encryption on secret data.
[8]	Low	Mid	High	This algorithm is a combination of S-DES and LSB technique
[9]	High	High	High	Author used RSA technique in combination with Hash-LSB method
[10]	Low	Mid	low	It's a basic PVD. High security as compared to LSB
[11]	Mid	high	Mid	It removed limitation of [10] So DHC is high than [10]
[12]	High	High	High	In this PVD block of 4 & 8 pixels are used for RGB image

V. CONCLUSION

Information security is becoming a major issue nowadays. That is the reason steganography is fetching attraction of everyone to secure data while communicating. In above paper we have studied and analyzed different spatial domain steganographic methods which have been innovated from last few years. In spatial domain we focused on two major techniques are least significant bit and pixel value differencing technique. Every technique differs from every other technique. Few of them work on better image quality, while others aimed at data hiding capacity or provide more security. All these techniques can be vital for future research in steganography.

REFERENCES:

1. R. Ibrahim and Teoh Suk Kuan, "Steganography algorithm to hide secret message inside an Image", Computer application and technology, February 2011.
2. 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).
3. 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.
4. 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.
5. Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality",Applied Mathematical Sciences, Vol. 6, 2012, no. 79.
6. Dr. T.Ch.Malleswara Rao, Koyi lakshmi prasad," 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,
7. 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 .
8. Ankita agarwal, "Security enhancement scheme for image steganography using S-DES technique", International journal for advanced research in computer science & software engineering, ISSN 2277-128X, Vol. 2, April 2012.
9. Anil kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International journal for advanced research in computer science & software engineering, ISSN 2277-128X, Vol. 3, July 2013.
10. Da-Chun Wu , Wen-Hsiang Tsai ,"A steganographic method for images by pixel-value differencing", Pattern Recognition LettersVolume 24, Issues 9–10, June 2003, Pages 1613–1626.
11. J. K. Mandal and Debashis Das ,"Color Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques, Vol.2, July 2012
12. Dinesh D. Patil & S. M. Bansode, "Secured Information Hiding Using Variable Pixel Block Size of PVD Steganographic Techniques", International Journal on Advanced Computer Theory and Engineering
13. Hsien-Wen Tseng1 and Hui-Shih Leng "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics Volume 2013, Article ID 189706, 8 pages http://dx.doi.org/10.1155/2013/189706
14. N.F. Johnson and S. Jajdodia," Exploring steganography: Seeing the Unseen", IEEE computer, pp. 26-34, 1998.
15. Hedieh Sajedi, "Recent advances in Steganography", www.intechopen.com, ISBN 978-953-51-0840-5
16. H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image steganographic scheme based on pixel value differencing and LSB replacement method", IEEE Proceedings on Vision, Image and Signal processing, Vol. 152, No. 5,pp. 611-615, 2005.)
17. http://www.academia.edu/4849962/Pixel_Value_Differencing_Steganography_Attacks_and_Improvements
18. C.P. Sumathi, T. Santanam and G.Umamaheswari, "A Study of Various Stenographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey, Vol.4, December 2013.
19. Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Computer Security series, Boston, London.
20. Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal processing, volume 90, Issue 3, March2010, pages 727-752.