International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Study of Different Image Steganography Techniques to Transfer Secret Data Securely

Mr. Viral Shah[1], Prof.(Dr.) C.K.Kumbharana[2]
[1]Research Scholar, [2]HOD, Dept.
[*] Dept. Of Computer Science,
[*]Saurashtra University, Rajkot
viral.shah.mca@gmail.com[1], ckkumbharana@yahoo.com[2]
919427731460[1], 919426719388[2]

Abstract- This paper represents an overview of various data hiding and security techniques for survey point of view. The word steganography comes from the Greek words steganos (secret or covere) and graphy(drawing or writing) and this means, literally, covered writing. Steganography is the science of embedding the data secretly inside other medium files in a way; it hides the existence of the secret data at all. It can be applied to image, text, audio and video file types with various extensions. If we talk about image steganography, using various methods like RGB colour model, LSB embedding, spatial domain etc. In RGB colour model we can increases efficiency of hiding data within image. In this method we can use new LSB embedding in coloured images in which instead of embedding data into its' LSB, we used image pixels for embedding data [1].
Keywords : Cryptography, Steganography, LSB, MSB, PSNR, Spatial Domain.

1. INTRODUCTION

Now a day's digitalization is a booming field. Due to advancement in digital communication, sending a secure message through digital medium is a common thing. In this condition sending a secure message where intruders from every nook and corner of the world are present is a challenging task [2].

Party attacks, phishing by intruder like hackers are always active to leak or crake official, personal or legislative information in the form of message using public networks. That's why cyber crime is the biggest issue in this fully connected internetworking world [2]. Information security is the most booming and on demand filed in data communication. There are many security problems exist in communication technology world which are very critical. One of the problems is related to hide information of the message in web. There are two relevant strategies to provide information hiding is Watermarking and Steganography [2]. Both are different from each other in terms of carrying capacity and objective to be achieved. Watermarking has low payload capacity and the main objective is attaching the payload in a carrier in the most robust manner. Whereas, steganography has high payload capacity and the main objective is to make the embedded message as imperceptible as possible [1].

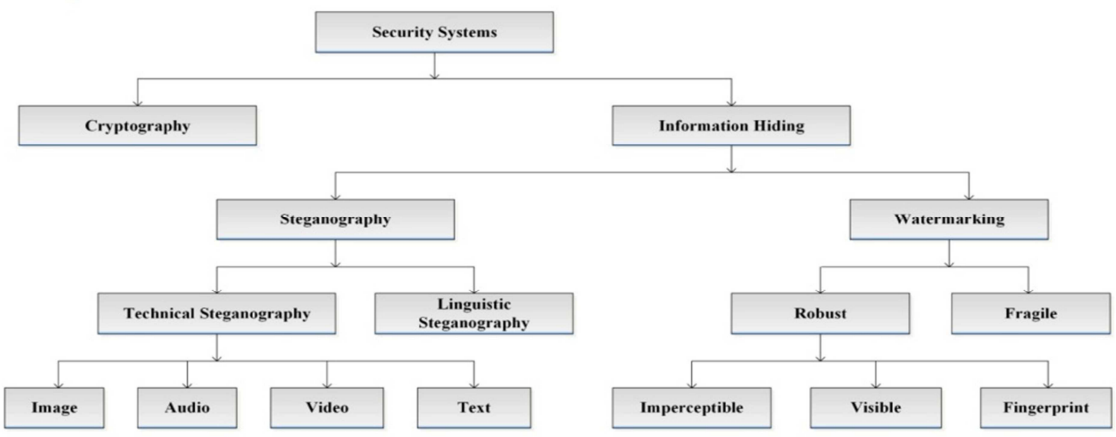

Figure – I Information Hiding Types [3]

2. DIFFERENT STEGANOGRAPHY TECHNIQUES

There are different steganography methods [4], for example, spatial domain Steganography and frequency domain Steganography, A concept of Least Significant Bit manipulation is being utilized as a part of Steganography with spatial domain, which can be enhanced to elegant bit selection criteria, random bit selection, LSB with wet paper coding [5] etc, and concept of frequency domain Steganography consists of Discrete Cosine Transformation (DCT) which may be applied on AC coefficients and DC coefficients, DCT embeds the secrete data into two dimensional signal such as image.

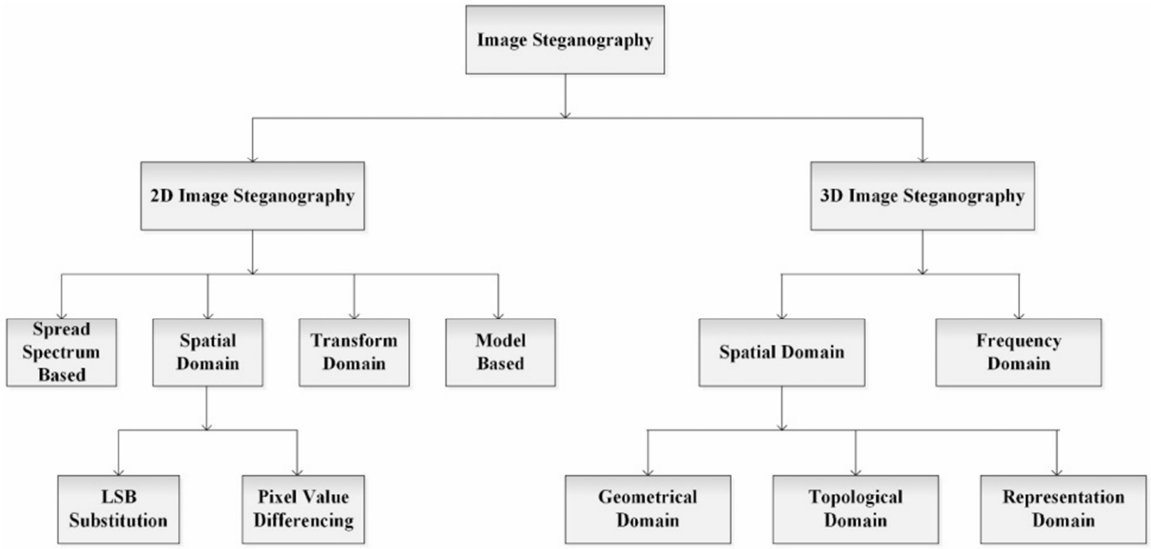

Figure –II Types of Image Steganography[2]

TCP/IP packets may be useful for concealing small amount of bits of secrete data. There are various locations in TCP/IP packets, which are not sometimes in usage in communication, can be used for embedding the secrete bits [5].

It described that watermarking is one of the latest application of Steganography to embed the invisible signal in digital file, for example, sound, video and pictures for copyright control. The digital Steganography is remarkable solution for copy right protection by using the watermarking and embedding authorized information into digital image [5], a digitized hand written signature may also be used to protect the ownership of objective property [5].

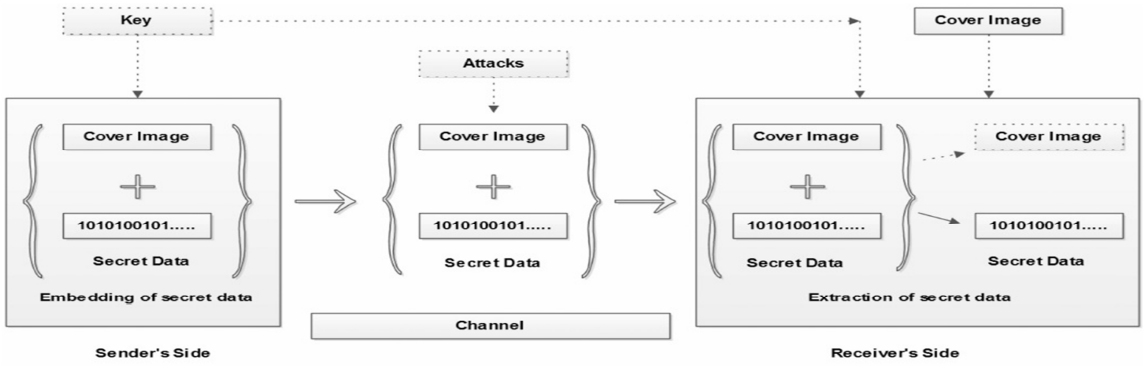

Fig – III Generalised view of Steganographic System[2]

The technique of cover/hiding the secret message is steganography. Steganography techniques comprise of two main phases: embedding and extraction. In embedding phase, the secret message which may be considered as a bit stream is placed inside the cover file. This is done in such a way that the human eye cannot differentiate between the cover image and the stego-image perceptually. In extraction phase, secret message is extracted from the stego media (secret bits imbibed inside cover file) at the destination. In this phase, the secret message bits are extracted from the stego-file with or without keys.

In LSB(Least Significant Bit) method researcher embedded one bit or more from secret message in cover directly. This is way simplicity and easy to detect and extract secret message. To enhancement the security of LSB standard, some researcher using Intermediate Significant Bit and Most Significant Bit (ISB and MSBA). In [6] developed LSB method to increase security by using intermediate significant bit (ISB) to hide secret message in smooth area in image. He is using 2, 3, 4 bit in cover to hide secret message. On other hands [7] proposed techniques to embed to conceal the secret data [8].This however makes the hiding capacity of the carrier image very low[5].

Table 1 : Steganography techniques with brief description[9]

Sr. No.	Image Steganography Technique	Description / Advantages
1	Extension of LSB(Least Significant Bit)	This algorithm is used to store maximize capacity of information bits for .bmp images. Payload Capacity is low.Security is low compare to DCT.
2	DCT(Discrete Cosine Transform)	
3	IWT(IntegerWavelet Transform)	This method can hide multiple secret images and keys in a cover image. It produces image that is Indistinguishable from human eye.
4	Spatial Domain	Based on physical location of pixels in image. It is more robust and secure.
5	Hash LSB	Uses hash function to generate a pattern for hiding data in LSB. Hash-LSB with RSA increases the security of secret message.
6	Selection of l –LSB	Normal MSE and Payload with better PSNR value
7	Selection of 2-LSB	Payload will be increased with increased MSE with decreased PSNR value.
8	Selection of 3-LSB	Payload will be incremented (approx. 3 times of I-LSB) with high increment in MSE with decreased PSNR value.
9	Selection of 4-LSB	Payload will be incremented (approx. 4 times of I-LSB) with very high increment in MSE with decreased PSNR value which in not acceptable in image Steganography.
10	8x8,Block - I LSB	Payload is decreased but low MSE and improved PSNR value.
11	8x8,Block-1 in Frequency domain	Payload is decreased but low MSE and Frequency domain High PSNR value.

REFERENCES

[1] Zaid Y. Al-Omari and Ahmad T. Al-Taani, "Secure LSB Steganography for Colored Images UsingCharacter ColorMapping", DOI:10.1109/IACS.2017.7921954

[2] Ashish Girdhar1 , Vijay Kumar1, "Comprehensive survey of 3D image steganography techniques Comprehensive survey of 3D image steganography techniques",DOI:10.1109/IACS.2017.7921954

[3]Cheddad, A., Condell, J., Curran, K., et al.: 'Digital image steganography: survey and analysis of current methods', Signal Process., 2010, 90, (3), pp.727–752

[4] Binu P K, Sreekutty H L, Sreekutty V S,"Security Plugin for Mozilla which Integrates Cryptography and Steganography Features", DOI: 10.1109/ICCIC.2016.7919538

[5] G.Prashanti, B.V.Jyothirmai, K.Sai Chandana, "Data Confidentiality Using Steganography and Cryptographic Techniques", DOI: 10.1109/ICCPCT.2017.8074276

[6] Stalling, W; "Network Security Essentials (Applications and Standards)"Pearson Education, 2004.

[7] Kahate, A.; "Cryptography and Network Security", 2nd edition, McGraw-Hill, 2009.

[8] Johnson, N.F. and Katzenbeisser, S.C.; "A survey of steganographic Techniques", International Journal of Computer Applications, 2004.

[9] Sanjive Tyagi , Ashendra Sexena2and Sohan Garg, "Secured High Capacity Steganography using Distribution Technique with Validity and Reliability", Conference ID: 39669

[10] Kunal Kumar Mandal, SantanuKoley, SudiptoDhar, "A Mathematical Model for Secret Message Passing UsingSteganography", DOI:10.1109/ICCIC.2016.7919527

[11]Gupta, Shilpa, GeetaGujral, andNehaAggarwal. "Enhanced least significant bit algorithm for image steganography." IJCEM International Journal of Computational Engineering & Management 15, no. 4 (2012): 40-42.

[12]Palwunder Singh, Assistant Professor, GurunanakDev University, Amritsar." A comparative Study of Audio Steganography Techniques". IRJET, Volume-3, Isuue-4, April 2016.

[13] ShengDun Hu, KinTak U, (2011), "A Novel Video Steganography Based on Non-uniform Rectangular P artition", International Conference on Computational Science and Engineering CSE/ISPAN/IUCC 2011 , 978-0-769S-4477-911 1, 2011 IEEE, DOI 10.1 I 09/CSE/I-SPAN/IUCC.20 I 1.24, pp.-S7, The 14th IEEE International.

[14] Anish, K., Arpita, N., Nikhil, H., et al.: 'Intelligence system security based on 3-D image', Adv. Intell. Syst. Comput., 2017, 515, pp. 159–167