Steagnography: An Overview

Sagar R. Deshmukh
Department of Computer Science & Engineering
MGI-COET, Shegaon, India
sagardeshmukh04@gmail.com

Manjusha M. Patil
Department of Electronics & Telecommunication
MGI-COET, Shegaon, India
mmpatil208@gmail.com

Ashwini G. Sharma
Department of Computer Science & Engineering
MGI-COET, Shegaon, India
ashwini.unnatti@gmail.com

Anand G. Sharma
Department of Information Technology
SSGMCE, Shegaon, India
sharmaanand2008@gmail.com

***Abstract*—** Steganography is described as learning to communicate invisible. Steganography often touching way of hiding the existence of the material in a way that keeps it hidden. It remains a secret between two communicating parties. In image steganography, the hiding is achieved by embedding information into the cover image and generating a stego-image. There are species of various steganography techniques and their own limitations. This paper, we review the different security and date of concealment techniques that are used to using steganography such LSB, ISB, MLSB etc.

Keywords- Steganography, Cryptography, LSB, BPCP, PVD, DCT, PSNR

*****

I. INTRODUCTION

Steganography is secretly writing a word. "Steganos" means "cover" and "graphical" "writing" means. Therefore, steganography hide not only data, but also the art of hiding the facts of communication of confidential data. Steganography hides confidential data in another file knows the presence of the message only that, in such a way. In ancient times, hiding it on the back of data wax, table, were protected by rabbits or write stomach on slave skull. But today people all text, images, video, audio and transmit data in the form of medium. Communication of confidential data in a secure manner in order, such as multimedia audio, video, images, objects are used as cover to hide the source data. Steganography is a method of sharing secret information by making it inconspicuous to non-authenticated users. [2] Steganography has been originated from Greek word Steganos and graphics. Steganos means covered or hidden and graphics means writing. Greek People used steganography to convey secret message through different methods [3]. Other method to maintain security of information is Cryptography and Watermarking. Of which former is mainly used for authentication and later is used for hiding message using encryption. A comparison of cryptography, watermarking and steganography has been provided through Table 1. Steganography is mainly used in security applications like covert communication, legal fields and copyright Control. Security systems are mainly focusing on protection of secret information by using encryption or cryptography. Cryptography [4] provides security of information by altering meaning of information through scrambling or encoding by using encryption key. No matter how shatter proofed is our encrypted message, it will always be vulnerable to attack as intruder already knows the existence of secret information. Steganography is better than cryptography as it hides the existence of secret message from intruder. Adding information to a media file by altering its contents in an imperceptible way is known as Watermarking [5]. Watermarking is used for protection of copyright material as it must be robust against any type of attack. Watermarking makes our data protected through hiding data in the form of copyright protection but steganography hides data inside a cover object. In summary we can say that steganography provides us the mixture of cryptography and watermarking by adding imperceptibility. On the basis of type of cover object steganographic has been classified in five forms as shown in Fig 1[7].Text Steganography mainly deals with concealing Text in Text Files and in Binary Files.[8] Text can be scrambled or concealed in any way inside a video. Text steganography has very high capacity to hide text data in Cover Text File. Digital image steganography mainly deals with concealing data inside a cover image [9]. Being very popular in current internet era Digital images are considered to be highly used cover media in steganography [10]. Digital Image can be defined as a collection of pixels. Pixels based on their intensities are selected to hide data. Video can be considered as combination of audio and collection of still images which moves in constant time sequence. Videos are getting popular as a cover

object in steganography due to high embedding payload than a digital image [6] [7] and temporal features of video also provide perpetual redundancy which is not available in digital images .Due to availability of large number of frames secret data can be easily disguised inside a video. Disguising secret information in some network protocols is known as protocol steganography. Noreka et. al. [11] described steganography in application layer TCP/IP protocol. Bartosz et.al [18] had described protocol steganography using relation between two or more protocols.DNA.

Criteria	Cryptography	Steganography	Watermarking
Carrier Object	Text files or image	Any media file	Digital image/Audio
Secret information	Text	Any type of file	watermark
Secret key	Necessary	Optional	optional
Visibility	YES	Never	May or may not be
Objective	Protection	Secret communication	Copyright protection
Security	High	Very High	High
Capacity	High	High	Low

Table 1.1 Comparisons between Cryptography, Steganography and Watermarking[1]

Steganography is getting popular due to high security, high embedding capacity and high embedding efficiency. Andre et.al [12] had described steganography using DNA binary strands.

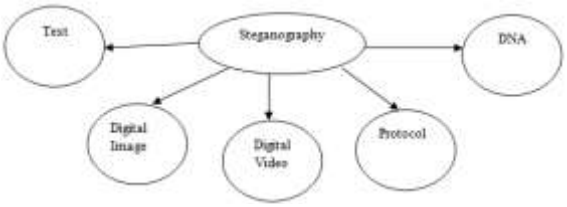

Fig 1.1 Types of Steganography[1]

.

II. A BRIEF HISTORY OF STEGANOGRAPHY

Back to Greece were using steganography first statement. Herodotus wrote a message to wax tablet down Xerses' hostile intentions have had about how the Greek says, and gradual letter to Aeneas because of the Tactician, cover with a secret ink dotting chapter describes a technique. It was the hair that hide pirate legends, one in the head, this map is a secret information, say the practice of tattooing. Kahn ideogram a pay status code embedded in a prearranged move to China says use; A similar idea medieval Europe, where a wood insert a secret message template stressing, seemingly innocuous text had been the most used system led grille.

During WWII grille method was used by spies, or something different. In the same period, a dot the size of the German shrinking it clear, good quality image printed on the microdot technology, developed. There's Margareth Thatcher during the 1980s, and the UK Prime Minister, cabinet documents so angry about the press leak, the word processor that is capable of pursuing, word distance to encode the identity of the author of the program was that the rumors of the unfaithful servant. The "Cold War" during the US and the Soviet Union wanted to hide the enemy's facilities, its sensor. These devices without being spotted, your nations, the data was sent. Today, research is due to both legal and illegal steganography.

Between the first ones there and the source of the message, both to hide or meteor scatter radio spectrum use in order to spread the war telecommunications, is. Industry market, digital communication and storage, the most important issues of digital watermarking technology, so with the advent of a copyright data are being developed to prohibit use of copyright enforcement. Another important use of the patient's record, and photos that match any problems, medical images about the data is embedded. Illegal export of cryptography among individuals not governed by the laws of hard-encrypted data to hide the practice.

Herodotus mentions two examples in our history, can be traced Steganography first recorded use was in 440 BC. [3] Histiaeus, shaving her head, sent Aristagoras his most trusted servant, "Mark" message on his scalp, once sending him on his way, education when his hair had regrown "come Miletus, Aristagoras shave his head, and looked." And Demaratus, who come from an attack sent a warning about writing it directly to help implement a wax tablet wood surface beeswax Greece. Wax surface as writing tablets were in common use, sometimes used for shorthand.

His work in Polygraphiae Johannes Trithemius, so-called, "Ave- Maria-cipher", which developed that can hide information in Latin praise of God. "Share includes Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris" VICIPEDIA secret for example.

III. LITERATURE SURVEY

In 2007 Daniel Socek et.al [13] has proposed an extended version of encryption algorithm of video which is applicable on both lossy and lossless low motion video codec and extension to this encryption algorithm as a new steganography algorithm to disguise a video inside a video with high security and low computational cost. There are two main types of video encoding standards i.e. compressed and uncompressed. Bin Liu et.al [16] has proposed compressed video secure steganography algorithm to achieve high security with robustness against statistical attacks without decompression process. Run level pairs which are formed by quantization of 8X8 discrete cosine transformed (DCT) are selected as positions to embed secret bits. Video steganography is famous due to high spatial and temporal redundancy. This feature can be easily applied to design a steganography algorithm with high security and high embedding efficiency. For example M.Jafar et.al [17] has proposed a compressed video steganography using temporal and spatial features of video signal. The proposed algorithm has constant bit rate, high

imperceptibility and embedded data has been extracted without full decomposition. There are many video steganography schemes proposed on motion vectors as they are used to remove temporal redundancies in video frames. Feng Pan et. al [18] has proposed an enhanced version of motion vector based video steganography algorithm by concealing data in motion vectors of cover media. This algorithm has maintained embedding capacity of 4 bits of secret message per 6 motion vectors i.e. approximately 2/3 of total number of motion vectors and PSNR value of more than 30dB. Due to low computational complexity and high bit rate of watermark channel Least Significant bit (LSB) is high used to embed secret data in steganography algorithm. R.Mritha [14] has proposed a modified least significant algorithm for video steganography with high security. Significant growth of video data over internet had made it a popular choice for steganography. Embedding capacity and embedding efficiency are contrary to each other. Maintaining security along with high embedding capacity in steganography is a difficult task. Ramadhan et.al [15] had proposed high payload and high secure video steganography algorithm with hiding ration of 28.12% and PSNR ranged between 35.58-45.68dBs.To achieve high security BCH(15,11) encoding and segmentation has been applied on secret message before embedding using 2D-DWT domain , two security keys have been used to provide additional security. Ramadhan et.al [20] had also proposed another technique using Wavelet Domain based on the KLT Tracking Algorithm and High security using BCH codes.KLT algorithm has been applied for the detection of facial region of interest in video frames and message has been embedded in RGB pixel values of these pixels using 2D-DWT domain method by generating four sub bands. This proposed algorithm needs some further modification for robustness against some video processing attacks and artificial attacks. RGB pixel's intensity values can be easily used to embed information in LSB of cover video file because modifications made to these pixels are almost invisible to HVS (Human Visual System) [15].LSB substitution being the most simple and less complex method can be easily utilized to embed secret information. A.Swathi et.al [19] has proposed a method of video steganography using selection of embedding location by applying polynomial equations. Speed of data extraction and data embedding depends on the steganography algorithm. M.Ramalingam has proposed an enhanced version of Hidden Markov model to increase the speed of data embedding and extraction process. Hidden Markov models (HMM) are based on markov chains which are considered to be most suitable for increasing the speed of retrieval and extraction process due to no use of memory for states and independence of conditional probabilities of all states on the time in sequence. The HMM performs embedding of secret data by locating colored objects and applying some mathematical tools to model these objects in spatial domain. Any successful steganography technique must consider some factors like imperceptibility, antisteganalysis and payload capacity but some factors contradict to each other, for example increasing payload capacity leads to distortion of imperceptibility and distortion of imperceptibility leads to vulnerability to attacks. Hence any steganography scheme can be considered as optimization problem where steganography technique hides secret message inside the cover video frame. Koushik et.al [21] had proposed an optimized technique for basic video steganography technique using genetic algorithm. Optimizer has been used to optimize a 3-3-2 LSB technique to achieve PSNR between 20 to 40dB and improved image fidelity (IF) as compared to previous existing method.

IV. TYPES OF STEGANOGRAPHY

1. Text Steganography: It masks the information inside the text files. In this method, the secret data is hidden behind each nth letter of each words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method[22].
2. Image Steganography: Masking the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to mask the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital delegation of an image [22].
3. Audio Steganography: It holds the data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum [22].
4. Video Steganography: It is a technique of masking any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in particular images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, video steganography uses AVI formats.
5. Network or Protocol Steganography: It involves hiding the information by catching the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used [22].

V. Steganography Terminology

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

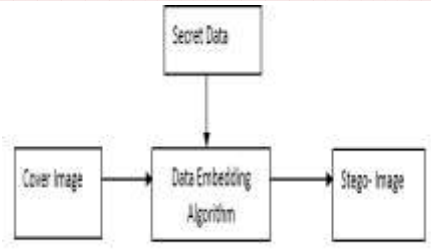

Fig 1 : Steganography Diagram

VI. Steganography Techniques

1. Spatial Domain Methods**:** This method is included directly in the intensity of confidential data pixels. This means, are directly transferred to the mask image pixel data values.

i) less significant bit (LSB)
ii) pixel value differencing (PVD)
iii) method embedding based data (EBE)
iv) random pixels (vairalaisa)
v) mapping pixels hidden corners: class under a different domain techniques data are classified
vi) Labelling or connection method
vii) pixel-based intensity.

i) LSB: This method is commonly used to hide data. Image with a bit of confidential data included in this procedure is done by changing the least significant bit of the pixels. Changes in pixel LSB of the image, because the image is obtained after adding, not taking too much difference between the image is almost identical to the original image. ii) BPCP: the image of this segmentation is used to measure the complexity. Complexity has been used to block out noise. In this method, two pixels are selected for embedding data: this method maps the binary pattern to a secret data block noise III bit scheme) are replaced with PVD. Two pixels of the Payload is determined by checking the difference between two successive pixels and recognize it serves as the basis for what is associated with an edge of the area or smooth.

2. Spread Spectrum Technique: Is used in this technique to spread the concept of spectrum. Confidential data in this method is spread over a wide frequency bandwidth. Each frequency of the signal to noise ratio in the band should be difficult to detect the presence of this data that it is small. Even if part of the data are removed several bands, is still present in the data to recover the other bands would be enough information there. So it is completely destroyed cover .It is difficult to remove without complete data is used in a very strong technique mostly military communications.

3. Statistical Technique: Many technology has been added to replace the cover feature in the message. Deploying the block and then cover embedding a message bits in each block. Cover block is modified, the size of the message only when bits require another amendment.

4. Transform Domain Technique: In this technique; Secret message has been added to cover alternative or frequency domain. This is a more complicated way of hiding a message in an image. Various algorithms and change are used to hide messages in images. Replace domain techniques broadly

i) Specific technique Fourier transformation (DFT)
ii) Specific calculations change technology (disiti)
iii) Specific changes Wavelet Technology (DWT)
iv) Compliance or reversible method (d. CT) are classified embedding
iv) Coefficient bit.

5. Distortion Techniques: In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message [22].

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information whereas watermarks becomes a portion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images [22].

VII. Factors Affecting a Steganographic Method

Success steganographic method can be determined by comparing stego-image as the cover image. There are some factors that determines the efficiency of a professional. These elements:

1) Robustness: Robustness means simple root words withstand or image stego- undergoes transformations, such as Linear and Non-Linear filtering, measure of inner calm or blurring, adding noise venture, rotations and scaling, cropping or decimation, lossy compression.

2) Imperceptibility: The imperceptibility means to blur a steganographic algorithm. For the first requirement, as steganography strength lies in its ability to observe human eye.

3) Payload capacity: It refers to the amount of information secret can be hidden inside the cover comes. Watermarking often embed only a few words Copyright, whereas, steganography sense to discuss a secret and so to finish embedding best.

4) PSNR (Peak signal to noise ratio), reportedly described as the ratio between pleasing as possible, power and standard power corrupting noise that affects the integrity of its

representation. This ratio measures the quality of the original image and extract the compressed. Important high among PSNR represents better extract the compressed image.

5) MSE (I Mean Square error): Called on the average squared difference between the reference image and the image is incorrect. The small MSE, especially transportation image steganography techniques. MSE is computed Pixel-by-Pixel is added to the sides squared differences of all pixels and dividing by the total Pixel count.

6) SNR (signal to noise ratio) is the ratio of signal power and noise power. It compares a step desired signal to the level of background noise.

VIII. Application of Steganography

i)Confidential Communication and Secret Data Storing ii) Protection of Data Alteration iii) Access Control System for Digital Content Distribution iv) E-Commerce v) Media vi) Database Systems. vii) digital watermarking.

IX. CONCLUSION:

By reviewing these PAPERSs, we noticed that many steganography role in 2012 & 2013. Through the years, LSB is the most common way of steganography. Some researchers have used the water system, not just skills, spatial skills, ISB, MSB job and provided a powerful way to secure the virus. Many papers are presented here were taken from the Audit um, AICCSA, Jet, IJCSE, IJCA etc. These papers provide more assistance to the initiator to start their career in this field. This research paper is enough to start their career in this field. The different security and date of concealment techniques are used to using steganography using LSB, ISB, MLSB .In some research, we go up to use foreknowledge projects like steganography other hybrid cryptographic algorithm to enhance information security.

REFERENCES:

[1] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17 www.iosrjournals.org

[2] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn: Information Hiding-A Survey, Proc. IEEE, 1999.

[3] N. Provos and P. Honeyman, Hide and Seek: An introduction to steganography, IEEE Security and Privacy, 1(3), 2003, 32-44.

[4] K.G.Paterson, Cryptography from Painings: A snapshot of Current Research, Information Security Technical Report, 7(3), September 2002, 41-54.

[5] M. Bachrach, F.Y. Shih, Image Steganography and steganalysis, Wiley Interdisciplinary Reviews: Computational Statistics, 3(3), 2011, 251-259.

[6] M. Jafar, K. Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging System and Technology,19, December 2009,306-315.

[7] M.M. Sadek, A.S. Khalifa, G. M. Mostafa, Video Steganography: A Comprehensive Review, Multimedia Tools Applications, 74, March 2014, 7063-7094.

[8] E. Satir, H. Isik, A Compression-based text steganography method, Journal of System and Software, 85(10), Oct 2012, 2385-2394.

[9] A.Cheddad, J.Condell, K.Curran, P. Mckevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727-752.

[10] I.Anastasia, T.Spyros, T.Halkidis, S.George, A novel technique for image steganography based on high payload method and edge detection, Expert System with Application, 39(14), October 2012, 11517-11524.

[11] L. Norka, P. James, Y.Payman, C.Steve, Syntax and Semantics-Preserving Application Layer Protocol Steganography, Information hiding, 3200, 2005, 164-179.

[12] L. Andre, R.Christoph, B. Wolfgang, R. Hlimar, Cryptography with DNA binary strands, Biosystems,57(1),June 2000,13-22.

[13] F. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding – a survey, Proc IEEE, 87(7), 1062-1078.

[14] R.Mritha, Stego Machine- Video Steganography using Modified LSB Algorithm, World Academy of Science, Engineering and Technology,5, Feb 2011.

[15] M. Ramadhan, E. Khaled, A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11), Wireless Telecommunications Symposium (WTS), New York, April 2015, 1-8.

[16] Bin Liu, Y.Chunfang, L. Fenlin, S.Yifeng, Secure Steganography in Compressed Video Bitstreams, Availability, Reliability and Security (ARES), Barcelona, March 2008.

[17] M.Jafar, K.Morteza, An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal, International Journal of Imaging Systems and Technology,19(4), December 2009,306-315.

[18] F.Pan, L. Xiang, X.Y. Yang, Y. Guo, Video Steganography using motion vector and linear block codes, Software Engineering and Service Sciences, Beijing, July 2010, 592-595.

[19] A.Swathi, S.A.Kjilani, Video Steganography by LSB substitution using Different Polynomial Equations, International Journal of Computational Engineering and Research ,2(5),September 2012,1621-1623.

[20] J. U. Duncombe, Infrared navigation—Part I: An assessment of feasibility (Periodical style), IEEE Trans. Electron Devices, 11, Jan. 1959, 34-39.

[21] D. Kousik, K. Jyotsna, D. Paramartha, Optimized Video Steganography using Genetic Algorithm(GA) , International Conference on Computational Engineering and Research, 2(5),September 2012,1621-1623.

[22] International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) "Steganography Techniques –A Review Paper"