International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 3 Issue 12 December 2017

A Survey on various types of Steganography and Its Techniques

Ketki Pande
Research Scholar
Department of CSE, LNCT Bhopal
ketkiupadhyay22@gmail.com

Dr. Vineet Richhariya
Professor & Head
Department of CSE, LNCT Bhopal
vineetrich100@gmail.com

***Abstract*— Imaging is playing a critical role in our life and shaping the world we live in. Ancestors passed on the information about their cultures and their lives by painting the walls of the caves with pictures from their daily lives. Imaging has made a commendable growth specifically in the beginning of the twentieth century. Steganography is about hiding the information whether the hiding thing is an image only. There is the technique of hiding message in different medium is coming from a long traditional time. The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. The amount of information that is generated and stored through the world contributed by all the branch of science put to gather is overwhelming. The information is sorted, categorized while it is stored on the computer. To retrieve the information back, it is needed to be looked back among all the information that lies in the computer.**

Keywords*— *Steganography, LSB Embedding, DCT, PSNR.

I. INTRODUCTION

Steganography is the science of hiding secret messages within an otherwise normal, innocent medium. Steganography has long been in use, even before the invention of the computer. For example, warring nations used invisible ink and microdots to communicate messages covertly. However, computer technology has taken steganography to the next level. Nowadays, messages are typically hidden within digital images, video and audio. This paper focuses on one particular popular technique, Least Significant Bit (LSB) Embedding, using digital images as the medium. The terminology is that a message is hidden within a cover image to produce a stego-image. First, the choice of a good cover image is discussed. Then, variations of LSB Embedding are detailed. Finally, the advantages and disadvantages of LSB Embedding are summarized [1].

.

II. THE BASIC IDEA OF LSB EMBEDDING

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. By using the least significant bits of the pixels' color data to store the hidden message, the image itself will seem unaltered [1].

III. HISTORY OF STEGANOGRAPHY

Steganography is about hiding the information whether the hiding thing is an image only. There is the technique of hiding message in different medium is coming from a long traditional time [1].Throughout history Steganography has been used to secretly communicate information between people. Some examples of use of Steganography of past times are:

1. During World War 2, invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.
3. Another method used in Greece was where someone would peel wax off a tablet that was so steganography is chosen, because this system includes not only imperceptibility but also un-delectability by any steganalysis tool [1].

IV. APPLICATION OF STEGANOGRAPHY

- **Confidential Communication and Secret Data Storing** The various steps are where a communication need to a secret way and also the data storage in a secret medium can be obtained.
- **Protection of Data modification** The data modification and its protection from the intruder is a wide area of Application where the different foe protection is necessary to transmit the message between sources to destination.
- **Access Control System for Digital Content Distribution** Digital medium access control services to process and manipulate digital Content are required application interface with steganography.
- **E-Commerce ex. online shopping** The E-commerce website, shopping sites required to hide product info, such As Price, size and other parameters which represent a product specific to Brand, Size and it price tag associate with its logo.
- **Media ex. Encrypt the disk media** Encrypting disk and medium for the storage usage is being utilize by the Steganography approach which deal here.
- **Database Systems for password storage** A secure password storage system can be a wide application, where theStorage can be performing for password in hidden manner.
- **Digital watermarking** One of the technique to authenticate documents and some other secure process, they make use of stenographic approach.

V. TYPES OF STEGANOGRAPHY

- **Image Steganography**

Taking the cover object as image in steganography is known as image steganography, in this technique pixel intensities are used to hide the information.

- **Network Steganography**

When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc.*, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

- **Video Steganography**

Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.*, 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye [2] [3].

- **Audio Steganography**

When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity.

- **Text Steganography**

General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and etc.is used to achieve information hiding.

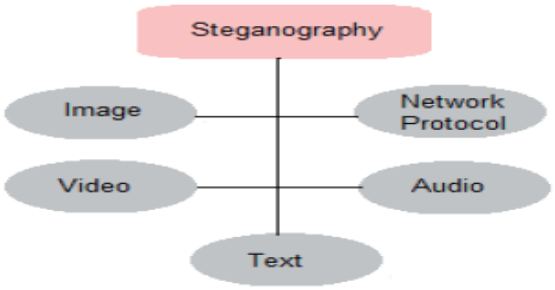

Fig 1: Various formats of Steganography on different Objects.

VI. THE NEED OF IMAGE DATA MANAGEMENT

The amount of information that is generated and stored through the world contributed by all the branch of science put to gather is overwhelming. The information is sorted, categorized while it is stored on the computer. To retrieve the information back, it is needed to be looked back among all the information that lies in the computer. Internet has made it easy to search obvious that search engines offers millions of information related to search topic making it a tedious task to find the right solution from among millions of similar search results. This problem highlights the requirement for better and efficient technology proposition that will facilitate fast and smart search capabilities.

Storing and managing of images can get quite troublesome because of their size. There seems to be an acute requirement for efficient system that can offer smarter ways of cataloguing and indexing when required. The biggest challenge in storing the images is the difficulty in locating the desired image from the large pool of varied collection of images. Searching for images using trivial and primitive methods such as searching by name or description might still be useful while searching for information in small database; this definitely isn't the smartest way while dealing with large database. Much effective retrieval techniques are required when database in question contains enormous amount of

information. This is even more imperative when the database in question contains enormous amount of image data [4].

VII. INFORMATION DECODING FROM THE STEGANOGRAPHY IMAGE

The image data storage is available for the data insertion and hiding into it. Further the reverse functionality is very much required to analyze to revert back the original data from the stenographic image.

In the last one decade there has been flood of information published around computer readable formats. Along the way, much of the information that was available in printed formats such as books, journals and newspapers have been digitalized and made computer readable. Huge archive of videos, audios, images & satellite images, books, journals, newspapers and magazines have become accessible through internet. Internet has played a pivotal role in last one decade to make it possible for humans to have access to huge amount of information. However the biggest challenge for the World Wide Web is accumulation of information at an alarming rate. The more the information gets available about specific topic, the more it will get difficult to locate accurate and most relevant information. Most of the people searching the internet know what they are looking for, yet not pretty sure where to look for. Search engines impart the ability to locate relevant information [5].

VIII. TERMINOLOGIES OF STEGANOGRAPHY

The basic terminologies used in the steganography systems are: the cover message, secret message, the secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually used to embed the secret information in the cover message [6][5].

IX. PICKING A GOOD MEDIUM

As important as the stenographic technique is, equally important is the choice of the cover image. In LSB Embedding, a poor choice of cover image can lead to a stego-image that is easily differentiable from the original.

Current image formats can be divided into two broad categories, lossy and lossless (Johnson & Jojodia, 1998). Lossy images are those formats, which loses some of the image's data when stored. An example would be JPEG. The plus side of lossy images, in particular JPEG, is that it achieves extremely high compression, while maintaining fairly good quality. However, due to the very nature of lossy formats, it is not suitable for LSB Embedding. Since LSB Embedding spreads the hidden message throughout the image's data, the loss of the image's data by compression would lead to the loss of parts of the hidden message. On the other hand, lossless images are suitable for LSB Embedding, since the integrity of the image data is preserved. However, they do not have the high compression ratio that lossy formats do. Not all lossless images are good candidates as a cover image. 24-bit bitmaps, as well as gray scale images and other color images with small variations in its palette are good candidates as cover images. The reasons will be detailed in the respective sections below.

1. THE SIMPLE CASE – 24-BIT BITMAPS

Perhaps the simplest implementation of LSB Embedding is that using 24-bit bitmaps. According to the Worldwide Center for the Study of Leif Computer Science Team (2001), the structure of a 24-bit bitmap is a bitmap header, followed by the pixels' data. Each pixel is represented by three bytes, representing the red, green and blue color values for that pixel. The higher the number, the more intense that color is for that pixel. For example, if the data for a pixel p_a were FF FF FF_{16}, that pixel would contain the most of all three primary colors and thus be white. LSB uses the fact that changing the LSB of these bytes would produce only a minute, insignificant change to the color value (Johnson & Jojodia, 1998). For example, changing the color values for $p_a$to FE FE FE_{16} would make the color darker by a factor of 1/256. This change would be imperceptible to the human eye. The idea then is to simply encode one bit of the hidden message in the LSB of each byte of pixel data. Thus, we can embed <number of bytes per pixel> * <number of pixels in image> bits of secret information in any particular cover image. In the implementation however, one should be aware of a particular detail. In 24-bit bitmaps, the number of bytes per row is always end-padded with zeros to be a multiple of four. Although initially one may think to use these extra bytes to store hide additional information that would be unwise. Since these bytes are supposed to contain zeros, any alteration would be easily detectable. Thus, in order for the image to remain inconspicuous, only the LSBs of the actual pixel data should be altered. Listing 1 and 2 contain an implementation of LSB Embedding using 24-bit bitmaps as described.

X. VISUAL CONTENT LEVELS

Every image naturally possesses some attributes or information that can help in resolving image retrieval issues. The information content derived from the image can classify the image in three levels.

- **Low Level**

This includes visual features such as texture, shapes, colors, motion and spatial information.

- **Middle Level**
  This describes the presence or absence of specific type of arrangements on specific types of objects, scenes and roles.
- **High Level**
  These are impressions specific to images, like emotions and meaning associated with the combination of perceptual features. Some of the common examples include scenes with emotional or religious significance.

XI. PRACTICAL APPLICATION OF LSB

LSB concept has found wide spread usage in many real applications. Most of the field including Medical science, architectural, Criminal all can be seen leveraging the capabilities of LSB image processing and retrieving system. In the field of medical science, LSB is widely used to diagnose by comparing similar past case. This technique is also commonly used n finger print and retina scanning. The web is where LSB is used the most. Common example of applications can be seen using it for retrieving images based on their content [7]. Below are some case scenarios where LSB is used extensively.

- **Crime Prevention**
  Police department maintains a huge archive of evidences from past suspects and criminals. This includes photographs and fingerprints. Whenever there is an incidence of crime happens, the evidences found at the crime scene are compared to the archive database of past evidences and are compared against it. LSB is used to compare the results. Harnessing the capabilities of LSB allows running search on the entire database of to extract closest matching records. Doing the same manually would mean a labor intensive and time consuming job.

- **Medical Diagnosis**
  Modern medical science highly depends on diagnoses made using technologies such as histopathology, computerized tomography and radiology. These technologies not only offer easy solution to diagnose by comparing the results to the old stored archive but also add the new images to the system making the system inadvertently smarter after each test, the medical related identity and security over the image can be embed in the dataset.

- **Home Entertainment**
  People save images taken from the vacation or during festival celebration and videos. LSB method can be used at a smaller level at home to manage images and managing security at image data level. Increasingly many organizations can be spending time and effort in developing simple software for retrieval at affordable price.

XII. MEASUREMENT TRIANGLE OF STEGANOGRAPHY

A. Capacity

Capacity is the maximum amount of secret information can be embedded in a file. Capacity either can be defined as an absolute value in term of number of bits for particular cover or as a relative number regarding necessary bits to save final stego file. Capacity value depends on both embedding function and cover properties. For instance, in LSB technique if the cover is 8-bit gray scale image file for one bit per pixel embedding the capacity would be equal with 12.5% or less because of the cover file header information which is not embeddable. This fact also is notable that not always the secret message is in maximum embeddable size and bit per pixel is just a measurement of capacity for maximum embedding [8]. P is a metric which shows proportion of length of the secret message relative to the maximum length of message can be embedded in cover. P value would be $0 \leq p \leq 1$ and can be calculated by following formula: Not always finding embedding rate is this easy because some stego systems are able to embed into compressed covers and therefore final embedding ratio would be variable. In these kinds of cases it is hard to find particular formula which can accurately define embedding capacity. So another capacity measurement for compressed formats is needed. For instance, F5 is a stenographic algorithm for compressed JPEG format which reduces file size monotonically with the needed size of embedding secret data [9, 10]. In fact it degrades quality of lossy compressed images to make free hole for embedding secret information. A bit per non-zero DCT coefficient (bpc) is a capacity metric for JPEG images. Practical and theoretical studies [11] show that larger secret messages would have more changes on cover and statistically are more detectable than short ones. Therefore embedding rate and capacity are directly related to property of imperceptibility.

B. Imperceptibility

Stego object should not have important perceptual artifact. The higher fidelity of stego object, will give the better imperceptibility. This property would be satisfied if difference of resultant stego file be not distinguishable from original cover for warden.There are various evaluation techniques different steganography types but the main evaluation method is PSNR. Peak Signal to Noise Ratio (PSNR) is a metric to evaluate the ratio between possible maximum signal and influence of modifying noise to fidelity of its representation . This metric can be calculated as follow [11]:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

C. Robustness

Robustness is property of harness of eliminating secret information from stego file. While detection of embedded secret data has much higher importance than its removal, but property of robustness talks about resisting against intentional distortion of communication channel by means of systematic interface or channel noise aiming to ban use of steganography techniques. Robustness metrics of stenographic algorithms are classified in distortion classes like geometric transformations or additive noise. In each one of the classes distortion value can be expressed according generic (like noise source parameters) or specific (like PSNR) measures [11]. Robustness of steganography methods also can be examined through steganalysis attacks. Challenging aim of steganalysis is detection of existence of the secret message in cover file [11]. Today numerous methods exist which can conduct steganalysis to reveal existence of secret information especially when the cover file is digital image.

XIII. LITERATURE SURVEY

[1] In this paper author worked with the encryption and steganography. Thus the author combines the chaotic theory and cryptography to form a valuable technique for information security. In this scheme user uses a hybrid approach using which first chaotic map based encryption has been performed and then the hidden data LSB technique been performed to make the system effective and can be used. In the paper's investigation done on proposed system which implement three nonlinear differential chaos based encryption technique where for the first time 3 differentials chooses is used for position permutation and value transformation technique. In the data hiding phase, data which is in the binary forms embedded into an encrypted image by using a least significant bit algorithm. We tabulate correlation coefficient value both horizontal and vertical position for cipher and original image and compare the performance of our Method with some existing methods. They have performed their scheme in five steps 1. 3D chaos generation, 2.Chaos equalization 3.Row rotation, 4.Column rotation, 5.XOR operation with the image. And finally a data embedding LSB technique is used for the data steganography or hiding in the scheme. Further on data retrieval side data decryption and data extraction process is performed to retrieve original data and image.

In [12] authors proposed an unique technique which enhance the security of the data and protect it from the attacks, for this authors use an inverse coding technique in which encryption and decryption of the data is done independently and a scale text is used to encrypt and decrypt data. For this purpose an 8-bit gray scale image is used as a cover of data and LSB operation is performed on that image to encrypt information, that image is known as stegano-image, quality of stegano image is depends on the quality of the image used as medium. It encrypts the data and transmits it in hidden form.

In [13] authors proposed an AES encryption based LSB embedding technique, in this technique first the plain text convert into cipher text and then embed that cipher text into the image, and transmit that image in hidden form. In this technique a filtering algorithm is used to filtering large data it uses MSB for filtering purpose. Thus in this method AES encryption and steganography algorithms are used which ensures the two layer protection for that data thus it gives a secure way to transmit data inn hidden form.

In [14] in this paper authors proposed a technique which uses AES encryption and data hiding technique with fake data generation. This technique enhance the security of data, first data is convert into cipher text and then LSB hiding technique applied on that data to cover it in image and send that data to receiver end, by the mean of mails or others. At the receivers end only receiver who having decryption key can decrypt image and having hiding key can decrypt text, if any unintended user want to decrypt text that system generate a fake key so it's too hard to guess key. Thus it enhances the security.AES has been adopted by the U.S. government and is now used worldwide.

In [15] authors presented a survey over embedding techniques which used in steganography like edge adaptive image steganography, the amplitude of histogram local extrema etc. but in these technique problems like image distortion occurs to converges these problems authors propose an method which is based on PPM (Pixels Pair matching) which offers a minimum Mean Square Error (MSE) thus in that way this technique optimize the other existing techniques.

In [16] author presented a Steganography technique using LSB, in this technique lossless data hiding technique using LSB is used because LSB does not affect the visual properties of any image where is steganography is an art to hide data during communication it can be done by any medium like text, audio, video, image. In LSB, in a gray scale image change in its LSB affect only by 1 thus it does not affect the visual property of the image and provide a suitable way for hiding data inside image. In steganography if data can be suspected by any steganography software but it will be nearly impossible to detect it until having a valid password. But work for capacity is still required to hide more data inside a image.

In [17] a reversible data hiding technique is presented which resolve the drawback of conventional technique in which data is lost at data extraction but in reversible data hiding technique data recovery approach is used to recover data in this technique a reserving room before encryption RRBE, is used in which a sufficient space on image is reserved before encryption which helps to recover data from that image and provide a lossless framework. Reversible data hiding is a Technique that is mainly used for the authentication of data like images, videos, electronic documents etc.

XIV. CONCLUSION

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message. In this paper provides literature review on digital steganography. As steganography becomes widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. We surveyed various types of steganography. We studied the various techniques, Least Significant Bit (LSB), DCT (Direct Cosine Transform), DWT (Discrete Wavelet Transform) which helps to improve in security.

References

[1] Aparajita, Prof Ajay Rana Assistant Professor, Dept. of MCA, Galgotia Institute of Management and Technology/ UPTU, Greater Noida, Uttar Pradesh, India 1 Program Director, Amity School of Engineering and Technology, Amity University, Uttar Pradesh, India

[2] C.P.Sumathi , T.Santanam and G.Umamaheswari Department of Computer Science, SDNB Vaishnav College For Women, Chennai,India.Department of Computer Science, DG Vaishnav College For Men, Chennai, India.Video steganography A. Munasinghe; Anuja Dharmaratne; Kasun De Zoysa 2013 International Conference on Advances in ICT for Emerging Regions (ICTer) Year: 2013

[3] Video steganography A. Munasinghe; Anuja Dharmaratne; Kasun De Zoysa 2013 International Conference on Advances in ICT for Emerging Regions (ICTer) Year: 2013

[4] Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed and Ki-Hyun Jung Symmetry 2016, 8(6), 41; doi:10.3390/sym8060041

[5] Adnan Gutub , Institution Umm Al-Qura University , Department Department of Computer Engineering

[6] Chi-KwongChanL.M.Cheng, https://doi.org/10.1016/j.patcog.2003.08.007

[7] Masoud Afrakhteh, Jeong-A Lee First published: 12 March 2014DOI: 10.1002/sec.998

[8] François Cayre and Benoît Macq, Senior Member, IEEE, Benchmark Requirements, European Union, EU IST-1999-10 987 CERTIMARK Project, 2000.

[9] François Cayre and Benoît Macq, Senior Member, IEEE, R. Ohbuchi, H. Masuda, and M. Aono, Watermarking three-dimensional polygonal models through geometric and topological modifications, IEEE J. Select. Areas Commun., vol. 16, pp. 551–559, Apr. 1999.

[10] François Cayre and Benoît Macq, Senior Member, IEEE, Watermarking three-dimensional models, in Proc. ACM Multimedia, 1997, pp. 261–272.

[11] François Cayre and Benoît Macq, Senior Member, IEEE, A shape-preserving data embedding algorithm for NURBS curves and surfaces, in Proc. Comput. Graph. Int., June 4–11, 1999

[12] Soumyendu Das Information Security Consultant Kolkata, India, Subhendu Das STQC IT Services, Kolkata, India, Bijoy Bandyopadhyay Institute of Radio physics & Electronics, University of Calcutta, Kolkata, India

[13] Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Institute of Technology,Bangalore, India

[14] Announcing the Advanced encryption standard (AES) (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.

[15] School of Information Science and Technology, Sun Yat-Sen University and Guangdong Key Laboratory of Information Security Technology, Guangzhou, China

[16] Marwa M. Emam Computer Science Department Minia university, Egypt Abdelmgeid A. Aly Computer Science Department Minia university, Egypt Fatma A. Omara Computer Science Department Cairo university, Egypt

[17] Bee Ee Khoo Universiti Sains Malaysia.