A Survey on Image Steganography with its Related Techniques and its types

Yash Kumar Singh[1], Divyanshu Tripathi[2], Rohit Singh[3]
[1, 2, 3] Department of CSE
[1, 2] ITM University, Gwalior, India
[3] Assistant Professor, ITM University, Gwalior, India

Abstract- *Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means "cover writing". Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. In this paper, we define survey on steganography, types on steganography, classification on steganography and techniques of steganography, etc.*

Keywords- Steganography; Techniques; Classification

I. INTRODUCTION

Steganography technique is the art and science to hide information in any digital object like image, audio, video only recipient knows of the existence of the information [1]. Literally meaning of steganography is covered message and includes transmitting secret information through the seemingly innocuous files. Steganography is gaining popularity due to growing necessity for security of data.

The main objective of steganography is to transfer information from sender to receiver securely in a completely untraceable way and to evade depiction suspicion to the transmission of concealed information. The idea of message hiding in any object is not a novelty; this has been used form centuries all over world under different regimes. It is a technique for hiding information so that it does not even seem to exist.

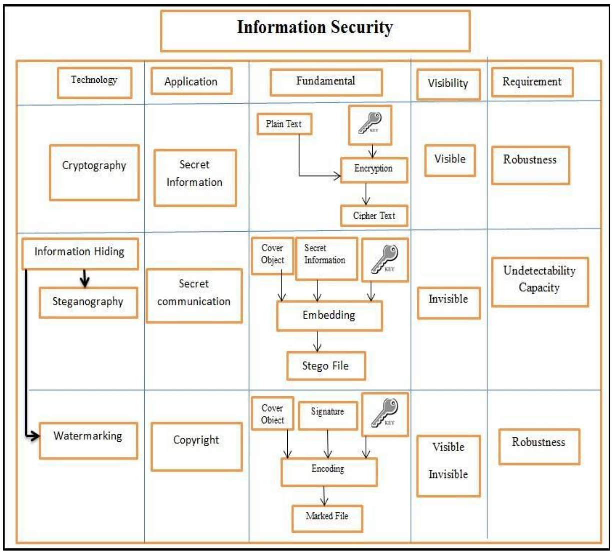

Fig 1: Information security disciplines

Image Steganography is mostly used in modern printers. HP and Xerox brand laser printers use Image Steganography. This printer adds tiny yellow dots to each page. The dots are not easily visible and contain encoded printer serial numbers as well as date and time stamps. The Russian foreign intelligence service uses custom image steganography software for hiding encrypted information inside images for communication with "illegal agents". Image Steganography adds extra layer to security of information by hiding encrypted secret message in image and not affecting quality of image [2].

II. STEGANOGRAPHY TYPES

There are five main categories of file formats that can be used for steganography based on these, the types are:

A. Text Steganography

Hiding information in text is the most important and basic method of steganography. It can be classified in three categories: format based, random & statistical generation and linguistic method [3].

B. Image Steganography

Images are used as the popular cover files for steganography. This technique exploits the weakness of the human visual system (HVS). HVS can't detect the variation in luminance of color vectors expressed in terms of 1s and 0s.

C. Audio Steganography

It takes advantage of the psycho acoustical masking phenomenon of the human auditory system [HAS]. Psycho acoustical or auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal or spectral neighborhood. In audio steganography, secret file is embedded into a digitized audio signal which result slight altering of binary sequences of the cover audio file.

D. Video Steganography

Video files are generally a collection of image and audio, so most of the presented techniques for images and audio can be applied to video files to [16]. The advantages of video are the large amount of data that can be hidden inside and noticeable distortions might go unobserved by humans because of the continuous flow of information.

E. Protocol Steganography

In this technique, the information is embedded within messages and network control protocols used in network transmission. A network packet consists of packet headers, user data and packet trailers. So during some of the layers of the network model, steganography can be used.

III. IMAGE STEGANOGRAPHY CLASSIFICATIONS

Generally image steganography is categorized in following aspects and Table-1 shows the best steganographic measures.

High Capacity: Maximum size of information can be embedded into the image.

Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover the image.

Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and the addition of noise.

Temper Resistance: It should be difficult to alter the message once it has been embedded into stego-image [4].

Computation Complexity: How much more expensive it is computationally for embedding and extracting a hidden message?

Table 1. Image Steganography Algorithm Measures

Measures	Advantage	Disadvantage
High Capacity	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation Complexity	Low	High

TABLE I. COMPARISON OF VARIOUSTECHNIQUES [5]

Parameters	Format exploit	LSB	DCT	DWT	DFT	Adaptive	distributed
Cover Format	Any	Any	JPG	JPG	BMP,TIFF	BMP,TIFF	JPG , BMP,TIFF
Robustness to modification	Good	Bad	Good	Good	Good	Good	Bad
Payload Size	Large	Large	Medium	Small	Small	Tiny	Large
Visual Detection (PSNR)	∞	High	Medium	Low	Low	Low	High
Steganalysis	EXIF	Spectral Analysis	X^2 test	RS Analysis	Unknown	Spectral Analysis	X^2 test

IV. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods:

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories:

i) Least significant bit (LSB)
ii) Pixel value differencing (PVD)
iii) Edges based data embedding method (EBE)
iv) Random pixel embedding method (RPE)
v) Mapping pixel to is hidden data method
vi) Labelling or connectivity method
vii) Pixel intensity based.

I. **LSB:** this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to the original image because the change in the LSB of image pixel does not bring too much differences in the image.

II. **BPCP:** In this segmentation of the image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

III. **PVD:** In this method, two consecutive pixels are selected for embedding the data. The payload is determined by checking the difference between two consecutive pixels and it serves as a basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it's become difficult to detect the presence of data. Even if parts of the data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus, it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3. Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one, otherwise no modification is required.

4. Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding messages in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as

i) Discrete Fourier transform technique (DFT)
ii) Discrete cosine transformation technique (DCT)
iii) Discrete Wavelet transformation technique (DWT)
iv) Lossless or reversible method (DCT)
v) Embedding in coefficient bits

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 the modifications and consequently recover the secret message.

6. Masking and Filtering:

These techniques hide information by marking an image. Steganography only hides the information where as watermarks become a potion 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 gray scale images [6].

V. LITERATURE SURVEY

Sayantari Ghosh et al- (2015) In this paper, the author has proposed a Hilbert curve based technique to embed information in an image using the neuro psychological behavior of human vision system which is robust to different attacks like cropping, scratching, additive noise etc [7].

Princymol Joseph et al- (2015) Strength of a steganographic technique lies in its capacity to keep the message, as secret as possible and also the amount of data that can be hidden, as large as possible. In spite of the fact that numerous approaches already exist in steganography, researches are going on in this field [8].

Avinash Tyagi et al- (2015) A new image steganography technique has been proposed which is based on the pixel value differencing and the pixel value sum of two consecutive pixels of a cover image. This technique is an improvement over the Wu and Tsai's PVD technique that is totally based on pixel value differencing [9].

Yugeshwari Kakde et al- (2015) Working on audio-video steganography, which is the combination of Audio steganography and Image steganography, in this we are using computer forensics technique for authentication purpose. In this paper the author's aim is to hide secret information behind audio and image of video file [10].

Wojciech Mazurczyk et al- (2014) State of the art of steganographic techniques for smartphones, with emphasis on methods developed over the period 2005 to the second quarter of 2014. It showcases the most popular software applications to embed secret data into carriers, as well as possible future directions [11].

Nadeem Akhtar et al - (2014) An improvement in the plain LSB based image steganography is proposed and implemented. The paper proposes the use of bit inversion technique to improve the stegoimage quality. The proposed bit inversion technique provides good improvement to LSB steganography. This technique could be combined with other methods to improve the steganography further [12].

Soon-Nyean Cheong et al- (2014) Validates the user perception and behavioral intention to use NFC ESGP smartphone access control system through an experiment and user evaluation survey. Results indicated that users weigh security as a dominant attribute for their behavioral intention to use NFC ESGP smartphone access control system [13].

Shahrokh Ghaemmaghami et al- (2013) Presented a novel speech steganography method using discrete wavelet transform and sparse decomposition to address the undetectability concern in speech steganography. The proposed speech steganography method exploits the sparse representation to embed secret messages into higher semantic levels of the cover signal, resulting in increased undetectability [14].

Dongming Peng et al- (2013) A novel steganographic attack which can defeat audio steganography algorithms while maintaining an acceptable audio distortion level. The attacking method is based on a proposed transform called discrete spring transform. Similar to the time scale modification, the spring transforms disables the synchronization of the hidden information [15].

Panagiotis Andriotis et al- (2013) A novel approach to the problem of steganography detection with JPEG images by applying a statistical attack. The method is based on the empirical Benford’s Law and, more specifically, on its generalized form. Prove and extend the validity of the logarithmic rule in color images and introduce a blind steganographic method which can flag a file as a suspicious stego-carrier [16].

P. Thiyagarajann et al- (2013) A novel steganography technique that conceals patient information inside a medical image using a dynamic key generated by graph coloring problem. The proposed method ensures reversibility as the original medical image is restored after extracting the embedded data from the stego medical image. Despite the embedding of patient information in the medical image, the visual quality of the image is preserved [17].

Siddharth Singh et al-(2012) Analyzes a technique for steganography named Compress- Encrypt-Stego that pre-processes the text before hiding it behind a cover image. In pre-processing, the text is first compressed and then modified using a key [18].

Harish Kumarl et al-(2012) Presented a Steganography method of embedding text data in an audio file. The basic approach behind this paper is to provide a good, well-organized method for hiding the data and sent to the destination in the safest manner [19].

S. Premkumar et al-(2012) A technique of encode the password of a customer by improved Steganography, most of the steganographic techniques, used either three or four adjacent pixels around a target pixel, whereas the proposed technique is able to utilize at most all eight adjacent neighbors so that imperceptibility value grows bigger and then dividing it into shares [20].

Susmita Mahato et al- (2012) A modified approach for text steganography based on HTML tags and attributes. As HTML is rich in tags and its attributes, easily communicated on the internet, and the source code is rarely checked by anybody it can be used intelligently to perform text steganography. In this approach the relation between two consecutive attributes is considered for hiding secret data [21].

C.L. Philip Chen et al- (2012) Builds up a pattern recognition system to detect anomalies in JPEG images, especially steganographic content. The system consists of feature generation, feature ranking and selection, feature extraction, and pattern classification [22].

G.Karthigai Seivi et al- (2012) Investigate steganography techniques and steganalysis techniques. Here state a set of criteria to analyze and evaluate the strengths and weaknesses of the presented techniques. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses [23].

VI. COMPARISON OF STEGANOGRAPHY TECHNIQUE [24]

Image Steganography technique	Description	Advantage
Integer wavelength transform	Conceal Multiple Secret Images And Keys In A Color Cover Image	Best Of PSNR Value Are Obtained And The Technique Is Simple To Implement

Wavelet transform coefficients	By Retaining The Integrity Of Wavelength Coefficients At High Capacity Embedding , Best Secret – Embedded Image Is Produced That Is Indistinguishable From A Human Eye	Bit Plain Complexity Produces The Best Quality Images
LSB , LZW(Limpel-Ziv-Welch , modified Kekre Algorithm(MKA)	LZW Pre-Processes The Data (Lossless Data Technique), Compression Technique Is Also Used To Increases The Efficiency . The Data Hiding Capacity Is Calculated In Bytes.	High PSNR Value And Low MSE (Mean Square Error) Value Results In To Good Quality Image
DCT, Arnold transform and chaotic sequences	Concept Of Three Keys, One For Scrambling Through Arnold Transform And Two Keys For Generating Chaotic Sequences, Along With The Concept Of DCT And IDCT For Extraction Process. Testing Is Done In The Presence Of JPEG Compression , Low Pass Filtering ,Gaussian Noise Attack And Cropping Operation	Technique Is Very Secure, Provides Multilayer Security And Is Robust. Low Distortion Is Induced In The Cover Image
Spatial domain	Analysis Of Image Steganography Tools Is Performed And Parameters Of Image Are Considered Like Physical Location Of The Pixel, Intensity Value.	Noise Related Parameters Are Obtained Like Size Of Cover Image, Physical Location Of Pixel, Etc. These Parameters Can Produce More Robust And Secure Systems.

VII. CONCLUSION

Now a days, it is very risky to handle the data in internet against intruders. Data is generally in the form of text, audio , video and image. Steganography is one of the best method to share the data secretly and securely. Steganography algorithm can be applied to audio, video and image file. Secret data may in the form of text, image or even in the form of video and audio. Hiding secret information in video file is known as video steganography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature

REFERENCES

[1] Kamred Udham Singh,” A Survey on Audio Steganography Approaches”, International Journal of Computer Applications (0975 – 8887) Volume 95– No. 14, June 2014

[2] Nishant Pattani, Kishan Patel , Nirmal Patel, Kashyap Pandya and Amruta Patel,” Survey on Image Steganography Techniques”, TERNATIONAL JOURNAL FOR RESEARCH IN EMERGING SCIENCE AND TECHNOLOGY, VOLUME-2, ISSUE-1, JANUARY-2015pp: 59- 64.

[3] Hemang A. Prajapati1 and Dr. Nehal G. Chitaliya,” Secured and Robust Dual Image Steganography: A Survey”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January 2015, pp: 30- 37

[4] Mehdi Hussain and Mureed Hussain,” A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp: 113-124

[5] Kalaivanan.S1, Ananth.V2 and Manikandan.T3,” A Survey on Digital Image Steganography”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 4, Issue 1, January-February 2015, pp: 30-33

[6] Z. V. Patel and S. A. Gadhiya,” A Survey Paper on Steganography and Cryptography”, RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ), Volume-2, Issue-5, May-2015.

[7] Sayantari Ghosh and Saumik Bhattacharya “Hilbert Curve Based Steganographic Scheme for Large Data Hiding” 2015 Third International Conference on Image Infonnation Processing.

[8] Princymol Joseph and Vishnukumar S.” A Study on Steganographic Techniques” Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015).

[9] Avinash Tyagi, Ratnakirti Roy and Suvamoy Changder “High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum” 2015 Second International Conference on Advances in Computing and Communication Engineering.

[10] Yugeshwari Kakde, Priyanka Gonnade and Prashant Dahiwale “Audio-Video steganography” 2015 IEEE.

[11] Wojciech Mazurczyk and Luca Caviglione "Steganography in Modern Smartphones and Mitigation Techniques" 2014 IEEE.

[12] Nadeem Akhtar, Shahbaaz Khan, and Pragati Johri "An Improved Inverted LSB Image Steganography" 2014 IEEE.

[13] Soon-Nyean Cheong , Huo-Chong Ling and Pei-Lee Teh b" Secure Encrypted Steganography Graphical Password scheme for NearField Communication smartphone access control system" Expert Systems with Applications 41 (2014) .

[14] Soodeh Ahani, Shahrokh Ghaemmaghami and Z. Jane Wang "A Sparse Representation based Wavelet Domain Speech Steganography Method" 2014. IEEE/ACM.

[15] Qilin Qi, Aaron Sharp, Dongming Peng, Yaoqing Yang and Hamid Sharif "An Active Audio Steganography Attacking Methodusing Discrete Spring Transform" 2013 IEEE.

[16] Panagiotis Andriotis, George Oikonomou, Theo Tryfonas "JPEG steganography detection with Benford's Law" Digital Investigation 9 (2013).

[17] P. Thiyagarajann, G. Aghila "Reversible dynamic secure steganography for medical image using graph coloring" Health Policy and Technology (2013).

[18] Siddharth Singh and Tanveer J. Siddiqui "Robust Image Steganography Technique Based on Redundant Discrete Wavelet Transform" 2012 2nd International Conference.

[19] Harish Kumarl and Anuradha "Enhanced LSB technique for Audio Steganography" 26th_28th July 2012, Coimbatore, India.

[20] Premkumar and A.E.Narayanan2 "New Visual Steganography Scheme for Secure Banking Application" 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].

[21] Susmita Mahato, Dilip Kumar Yadav and Danish Ali Khan "A Modified Approach to Text Steganography using HyperText Markup Language" 2012 Third International Conference on Advanced Computing & Communication Technologies.

[22] C.L. Philip Chen , Mei-Ching Chen , Sos Agaian , Yicong Zhou a,n, Anuradha Roy and Benjamin M. Rodriguez "A pattern recognition system for JPEG steganography detection" Optics Communications 285 (2012).

[23] G.Karthigai Seivi, Leon Mariadhasan and K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].

[24] Latika and Yogita Gulati," A Comparative Study and Literature Review of Image Steganography Techniques", IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015.