Comparative study of image steganography techniques

Himanshu Arora,Cheshta Bansal
Department of Computer Science & Technology
Manav Rachna University, Faridabad, India

Sunny Dagar
Department of Computer Science & Technology
Manav Rachna University, Faridabad, India
dagarsunny08@live.com

***Abstract*—**
This paper tend to review different steganography techniques for suppression of the information. Steganography technique is important as everyone wants to convey their message in such a way that no one could track their information. Steganography is defined as the study of indiscernible communication that usually deals with the ways in which the transmitted data can be preserved from tracking. Another technique is cryptography, which is used for protecting the transmitted information. The encryption methods of cryptography and steganography allows the user to transmit the information which is placed inside a file in plain view. Image steganography is a technique which hides secret information inside an image and conceals the existence of the communication. This will provide more security to the data to be transferred on the network.

Index Terms— **Cryptography, Steganography, Least Significant Bit (LSB), stego image, Discrete Cosine Transform(DCT), and Discrete Wavelet Transform(DWT).**

I. Introduction

In today's scenario,communication is the most basic demand of an invidual around the globe.Individual wants secrecy in the data they transmit around the network.In order to share the information in a secured and effective manner,two techniques are widely used.These techniques are cryptography and steganography.Cryptography is used to encode the text to make it readable.In cryptography technique,the data is transformed in an encrypted form with the help of a key which is known to the sender and receiver only.However,the transmission of the message may be easily arouse the idea of an invidual to track the information out of it and the encrypted data may thus be decoded .In order to overwhelm the weakness of cryptography technique,steganography techniques have been developed.Steganography technique is used to rawhide the data behind some other media content or file.Steganography is the process of suppressing information in various coded media files such as image,audio,text,video.It is a tool which prserves the data and the secret information whose existence can only be detected by the sender and its respective receiver only.Steganography equation is given as:"steg-medium=cover_medium+secret message+stego+key".
covermedium-Original medium which is used as a carrier for hidden information.
Stego medium-After embedding message into cover medium,it is known as stego medium.
Secret message-The data which has to be sent and is kept confidential.
Stego key-which is only know to the sender nd its respective receiver to decode the secret message.

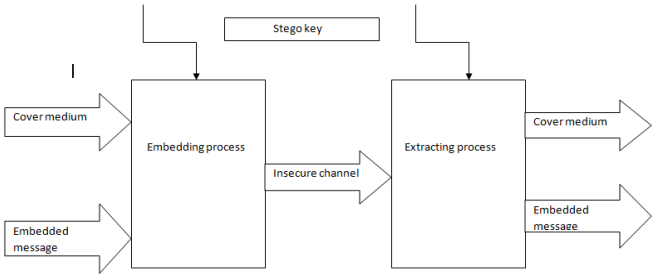

Fig-1

A stego_key is used to regulate the process of data hiding in ought to preserve the information form stealing[1].Nowadays a combination of steagnography and cryptography techniques are used.[2][3]

1.Image steganography:This technique is mostly used nowadays and hence more popular because of the transmission of the information with the help of electronic images with the trending evolution of digital high-end electronic cameras.It helps in hiding the information in the noise that is predicted with the help of electronic images.Almost every kind of information consists of some noise.Noise is the imperfection that come during the conversion of analog images into digitl images.The message is generally hidden by changing the pixels of the image.The message is hidden in the cover image form of image an pixels ,thus giving its name to image steganography[8].At the receiver end the proper techniques are used for decoding the message.The original data to be send is know as the cover image and the data embedded in that image is known as stego image.[9[[10].Various methods included in image steganography are:

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE

1.2.1. Data Embedding:a secret key is required for the retrieval of data that has been embedded inside an image.Without the secret key data can not be retrieved from the image.This is to ensure that data remains integrated and confidential..

1.2.2 Data Extracting : This method is used to extract the data from the message which will require a verification key. To check wether the decodes are done right or not a secret key is also required. If the key matches, the extraction process of zip file is done and then the text file is generated after the extraction following which the secret message is then transferred into the text file which is further compressed into the zip file and finally the zip text file is converted into the binary codes [12].

II.LITERATURE SURVEY

2.Spatial Domain: This technique follows to change only the LSB of the cover image without modifying the whole cover image. It is the simple and basic technique for hiding the information but it is too frail in preserving the information from even small attacks like compression transformations [13].

2.1LSB Substitution:Least Significant Bit substitution is the most commonly used method.It is a basic approach for inserting information in a cover image.The Lsb of one byte in an image is altered into a secret data embedding byte of that image.Using a 24 bit image provides three color bit components which includes red,green,blue each of which stores three bits binary in each pixel.of 800*600 pixel image,total amount of 180,000 bytes of embedded data can be stored.A hidden image with variations in its colors will be indistinguishable from the original image by a human eye.

This technique is suitable for larege images because of the enough space to hide data in it.Usually a 24 bit bitamp as a cover image is used for hiding the message.The secret information is stored in image bits by replacing the actutal bits of the image with the secret information bits and is then stored into specific position of lsb of a cover image.[14]

Lets take an example of hiding data using lsb approach

To hide 01001010 following are the three pixels(8 bytes)

Pixel1

10010101 11000101 10010111

Pixel2

10100100 10110011 10011100

Pixel3

11001011 00001100 10010100

After hiding the data pixels are:

Pixel1

1001010<u>0</u> 1100010<u>0</u> 10010111

Pixel2

10100100 1011001<u>0</u> 1001110<u>1</u>

Pixel3

11001011 0000110<u>1</u> 10010100

In this way the bits get placed in corresponding pixels.Also in lsb the secret key is used to decode the secret message which is confidential and that secret key is known to the sender and receiver only.[15]

PSNR ratio

A peak signal to noise ratio is used to measure the quality of stego images.If a psnr ratio is more that indicates better quality of image and even less distortion.PSNR is defined by the mean square error(MSE) for two a*b monochrome images c and d where one of the image is considered as a noisy approximation of the other.It is defined as

$$PSNR=10log10(max_{i2}/mse)$$
$$=20log10(max_{i2}/sqrt(mse))$$

The mse represents the cumulative speed error between the stego image and the original image and the distortion in the image can be measured by mse.Low value of mse repsents low error.

Max is defined as the maximum possible pixel value of the image.

Transform Domain Technique: This technique despite of its complexity works more efficiently in hiding the information in an image by performing various algorithms and transformations. This technique processes by embedding the data in the frequency domain of the signal respectively which is stronger than the embedding principles operating in the time domain. That is why it is also known as embedding technique and various algorithms have also been suggested for it. Presently the strong steganographic systems operate in the transform domain. Transform Domain Techniques are found to be advantageous over the spatial domain techniques because they hide the information in those areas which are less exposed to compression, cropping and image processing. All the transform dependent techniques are not entirely dependent on the image format as they may outrun lossless and lossy format conversions. These techniques have been broad;lly classified into 2 categories.:

1 Discrete cosine transformation technique (DCT).
2. Discrete Wavelet transformation technique (DWT).

DCT which is a lossy compression technique wherein the cosine cannot be calculated precisely and repeated calculations with the use of limited precision is required. It transforms the hidden picture into a frequency illustration by grouping the pixels into non-overlapping blocks after which pixels blocks are transformed into 64 DCT coefficients each. The converted image is then quantized and modified as a secret message. It then outcomes as in a high degree of compatability,capabilty and controls the compression ratio at same time, At the same time as doing Decompression, the consequent image is going through decoding, de-quantization, inverse DCT and so forth. Then the real valued pixels are obtained which are rounded to the nearest are considered

DWT:domain based embedding method that sincerely operates on DCT or DFT.Embedding is completed by enhancing the least large bits of the selected wavelet coefficients

.FFT area based embedding technique embeds the facts through the fourier transformation mapping but it produces round-off mistakes,that is why the technique is not so useful for hidden communication.
However the sender can not embed an excessive amount of facts and data inside the frequency domain as it causes a distortion in the cover image and hence reduces it quality
They are based on the domain transformation technique of Image steaganography.

Masking and Filtering Techniques:
The techniques of Masking and filtering function in a similar manner by marking an image as the paper watermarks do. It functions in such a way that human visual ability cannot detect the slight changes made in it by embedding the data in more significant areas rather than simply hiding it into the noise level. The message which is hidden is more integral to the cover image. Watermarking technique uses lossy compression as it is better defined and integrated into the image which eliminates the fear of image distortion. Watermaking techniques like visible watermarks are not actual steganography.But it extends the data and becomes an attribute of the cover image. During compression it hides the information in the visible parts of the image which makes this technique sturdier in comparison to LSB replacement. The application of these techniques is limited only to the gray scale images and is only restricted to 24 bits.

III.APPLICATIONS

Most of the more recent programs use steganography like a watermark, to guard a copyright on statistics. Photo collections, bought on CD, often have hidden messages inside the pics which allow detection of unauthorized use. The same technique carried out to DVDs is even more powerful, for the reason that industry builds DVD recorders to hit upon and disallow copying of covered DVDs.
A virtual photograph is a dimensional characteristic, f, that takes an enter spatial coordinates x and y and returns a value f(x,y). Thecost f(x,y) is a gray level of the photograph at that point. the gray degree is also referred to as the intensity. digital snap shots are a discretized partition of the spatial pictures into small cells which can be referred to as pixels - photoelements. clinical imaging isa field where researchers expand gear and generation to accu mulate, control and archive virtual snap shotswhich are utilized by the medical profession to offer higher care to the sufferers
Terrorists can also use steganography to preserve their communications secret and to coordinate assaults. All of this sounds fairly nefarious, and in fact the obvious uses of steganography are for things like espionage. however there are a number of peaceful programs. The only and oldest are utilized in map making, in which cartographers now and again add a tiny fictional road to their maps, letting them prosecute copycats. A comparable trick is to add fictional names to mailing lists as a test towards unauthorized resellers.

IV.Comparison of image steagnography techniques

To find the best and effective image steganography techniques following factors are taken in consideration which helps in finding the most effective and secure way of transmitting image from sender to receiver .The factors on which these techniques depends and measured are.

1. High capacity-Maximum size of information can be embedded in to image.
2. Perceptual transparency-After hiding process into cover image,perceptual quality degrades into stego image as compared to cover imge.
3. Robustness-After embedding,data should stay intact if stego images goes onto some transformation like cropping,scaling,filtering with addition of noise.
4. Temper resistance-It should be difficult to alter the message once it has been embedded into stego image.
5. Computation complexity-What is its cost of computation for embedding and extracting image.

The measure of these factors in those techniques will help to find the most suitable technique.

Measuring table:

Measure	Advantage	Disadvantage
High capacity	high	low
Perceptual transparency	High	low
Robustness	High	Low
Temper resistance	High	Low
Computation Complexity	low	High

V.Conclusion

This paper present the review of all existing steganographic methods for data hiding inside the text, image, audio and video channels. Some steganographic techniques need to advanceretreat by using cryptography against nasty attacks. The various steganographic techniques such as image, audio and video steganography need to be focused on hiding capacity, detectability, Level of Visibility and robustness against nasty and unintentional attacks. As the research in the field of steganography is an ongoing process. It will set a better platform for the beginners. By going through this survey paper beginners surely get some ideas for the future research in steganography techniques.

Technique name	Description	Capacity	Perceptual transparency	Robustness	Temper resistance	Computational complexity	Advantage	Disadvantage
Spatial domain	LSB	High	Low	Low	Low	Low	Integrity of hidden image is of high capacity	High extra bit of signature with hidden message
Transformation domain	DCT	Low	High	Low	Low	Low	High PSNR ratio	Noticable artifact of hidden data
Transformation domain	DWT	Low	Low	Low	Low	Low	Integrity of stego image inside the cove rimage	Computational complex
Masking and filtering	Masked data covered with significant bits	High	Low	Low	Low	High	High capacity of hidden image	Can cause degradation in cover image

.REFERENCES

[1] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.

[2] Yuk Ying Chung, fang Fei Xu , "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006.

[3] Singh, Nanhay, Bhoopesh Singh Bhati, and R. S. Raw. "Digital image Steganalysis for computer forensic investigation." Computer Science and Information Technology (CSIT) (2012): 161-168..

[4] AL-Shatnawi, Atallah M., and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71 (2013): 3545-3553.

[5] Bhattacharyya, Souvik and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)." International Journal of Computer network & Information Security 4.7 (2012)..

[6] K. Bennett, "Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text" center for Education and Research in Information Assurance and Security,Purdue University 2004.

[7] Hitesh Singh, Pradeep Kumar Singh, Kriti saroha "A Survey on Text Based Steganography" Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, February 26 – 27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.

[8] Hitesh Singh, Pradeep Kumar Singh, Kriti Saroha "A Survey on Tex Based Steganography" Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, February 26 – 27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

[9] Jain, Nitin, Sachin Mesh ram, and Shikha Dubey. "Image Steganography Using LSB and Edge–Detection Technique." International Journal of Soft Computing and Engineering (IJSCE) ISSN (2012): 2231-2307.

[10] M. M. Amin, M. Salleh, S. Ibrahim, M.R. Katmin, M.Z.I. Shamsuddin, "Information Hiding using Steganography" Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam , Malaysia, 2003. [11] Amin, Mohamed "Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd rozi (2003) Information hiding using steganography.

[12] Ibrahim, Rosziati, and Teoh suk Kuan. "Steganography Algorithm to hide secret message inside an Image." arXiv preprint arXiv: 1112.2809 (2011).

[13] Jenkins, Neil, and Jean Everson Martina "Steganography in audio." University of Cambridge CST Part II Dissertation (2009) ..

[14] Nosrati, Masoud, Ronak Karimi, and Mehdi Hariri. "Audio Steganography: A Survey on Recent Approaches." World Applied Programming 2.3 (2012): 202-205.

[15] Sunny dagar, " Comparative Study of Various Steganography Techniques **"**International Journal of Emerging Engineering Research and Technology Volume. 2, Issue 2, May 2014, PP 30-36