RESEARCH ARTICLE OPEN ACCESS

An Analysis of Recently Used Steganography Techniques on Images

Somya Rastogi [1], Achala Shakya [2]
Department of Computer Science
Banasthali University
Rajasthan - India

ABSTRACT
Now a days security is a big issue, the whole world has been working on the computer system and thus totally dependent on the computers. An analysis has been done of the commonly used steganography techniques on images. The paper consists of background and future perspective of steganography techniques and how these techniques can be improved.
Keywords:- Steganography, LSB, RSA, DCT, DWT, Spatial filtering & Transform domain

I. INTRODUCTION

Steganography is the technique to hide the data in an image, audio and video or we can say that it is the science of covered writing. Steganography is generally plays an important role in securing the secret messages. The main aim of this technique is to hide the message or information in such a way that no one can even suspect about the existence of the message apart from its sender or receiver. This technique embeds the message in a media which is given without making visible changes to the message. The techniques which are described in this paper are as follows:

RSA: This is used to encrypt and decrypt the messages inside the image.

DCT: It is for the transformation of a cover image representation into a frequency representation and this is done when the pixels of the images are divided into blocks of 8×8 pixels and then compute the 2-D Discrete Cosine Transform for each block and these blocks of pixels can further be transformed into 64 DCT coefficients.

YCbCr: YCbCr color space can be used to characterize the human visual system.

DWT: DWT is a sampled version of CWT & it consumes important quantity of our time and resources. This technique is discovered to decompose distinct time signals. This is widely utilized in signal process and compression.

EBCDIC: EBCDIC is used to convert plain text to the numbers and permutation which are used with the help of keys.

SPATIAL FILTERING AND MASKING: These techniques attach the information and then hide up to the noise level therefore the hidden message is very necessary to the cover image.

TRANSFORM DOMAIN: It is very complex way to hide the information in an image. There are various algorithms and transformations which are applied to hide information on an image.

II. CRITICAL ANALYSIS

This section deals with the analysis that we have done on the above stated techniques. Several papers have been critically analysed as follows:

Amol Bhujade, Prof. Sonu(2015).[1]
In this proposed paper, a digital image is taken and then applied for the MPEG-III (MP3) file as earlier this was applicable to only WAVE file because .WAV files are the easiest of all the formats for storing audio files therefore now a days MP3 file is providing to user the security and the flexibility to hide the message. LSB technique is used because of its robustness and the security measures. The DWT technique is also used because it is very simple and it attach the message bits to hide the image. Colored pixels are used to represent the color image and by using 3 bits of each color byte so that blurred image can easily be identified easily.

Neha Jain and SudhirGoswami (2015).[2]
This proposed paper presents LSB technique to hide the data from the image in different-different format due to its

simplicity. In digital image when we hide the data it provides protection and due to its simplicity. It is vulnerable to attack. When we transmit the data over any public media, we use steganography for the security purpose. LSB method replace the length fixed LSB with fixed length bits. By LSB substitution method we decrease the distortion in steganography. In this paper, key values are used to hide the characters in the image. With the help of key we can reduce the attacks & then decoding it to find out the secret information. With the help of public & private key we decode the original key i.e. used inside the encoding process for detecting the secret information. If size of message is large & message is small then the affected area is small & vice-versa. We propose a new & efficient experimental method for image which provides a better way for embedding more secret data into cover image. To increase the capacity of the steganography we alter the LSBs method then security, & capacity will improve.

Ms.RashmiJanbandhu and Mr.ViploveKarhade(2015).[3]

This paper presents network is an important factor of communication. It is a medium by which we can transmit the information from one side to another side. When we store the data in the computer data should be secure then Security is the necessary to transferring the data from intruders. This paper presents a 7 layer well-defined architecture. Only authorized person is allowed to send the data over the network between 2 computers. Before transferring the data it should not be public. After receiving the data it should be private. Alteration & modification is the method to protect the data via network. .bmp, .doc, .gif, .jpeg, .mp3,.txt, .wav are the most formats which are used by the researchers. With the help of image we hide the data after secret data is stuffed in the image, resulting image is known as steganography-image. Same as when data is hidden from video, known as video steganography. This paper used 2 types of codes: Open code is a method which hide the message behind a normal text message.Jargon code is a mechanism in which the sender and receiver create their own language by using a Specific set of symbols.

M. Divyavani And Ch. Madhavi(2014).[4]

Nursing knowledge concealment technique is proposed in this paper which is used in lifting schemes efficiently to hide the information in color image and winning knowledge secrecy should be required to extract the hidden data from the image. This paper proposed the approach of secret message in which wavelets are used which get splits into the stream into high level and low level frequency components. DWT is a technique which is widely utilized in signal process and compression & the signals are divided into the different sub-bands and frequency information. DWT is powerful tool for varied applications like signal analysis, signal compression and numerical analysis. DWT also supports progressive image transmission, simple compressed image manipulation, Region Of Interest to writing and so on. In the very first-level, the input image taken will be of N* N matrix, and therefore the outputs produced will be 3 sub bands which are as follows: HH, LH, & HL, and these sub bands will be of the size N/2*N/2. Now, in the second-level, LL band is considered as an input and they also produce the outputs in the 3 sub bands LLLH, LLHL, and LLHH, which are of the size N/4*N/4.

Prajakta B. Diwan, V. B. Bhagat(2013).[5]

This paper presents about communication in steganography. Steganography software tool is easy to use on the internet & also have the capability to exchange the secured data without detection of the information & also provide the opportunities for securities. The main advantage of image steganography is limited power of human visual system. In this, we fetch bits from our secured data in binary (0&1) form, data is hidden in this method, is converted into binary form and these are stored in the pixels form of the cover image. No. of 1's & 0's are stored in odd &even column form respectively. Which media is with secret information is known as stego media and which is without hidden information known as cover media. Steganalysis is opposite to steganography. Wavelet transform is helpful to convert an image from spatial domain to frequency domain. The security and data hiding technique are used toimplement steganography.

Mohamed Amin, Hatem M. Abdullkader, Hani M. Ibrahem1, and Ahmed S. Sakr (2013).[6]

This proposed paper presents security features in multimedia. Spatial embedding & transform embedding are the 2 methods of embedding the data in steganography.
In spatial embedding data are inserted into the LSB of the pixels of the images & in Transform embedding the messages and data are hidden inside the image. Stegnographic algorithms works on three types of images: Raw images (.bmp format), Palette based image (.gif format) & jpeg images. One new steganographic method is developed which is based on Jpeg-Jsteg algorithm to embed the data in a host image. Jpeg-Jsteg algorithm is based upon domain transformations which attach the secret message in the least significant bit of the quantized DCT coefficient. It is based on T- codes. T-codes are the variable-length codes i.e. VLC. DCT coefficient of image using new quantization

technique to quantize the DCT coefficient & it is used to transform each block in DCT coefficient. A new steganographic method to increase the message capacity in every block as the message is embedded in the quantization DCT coefficient except the last block which is used to hide the message size.

Dinesh Patil& S. M. Bansode(2013).[7]

This paper presents a steganography technique for hiding secret information and that to in the spatial domain of the grey scale and color image.

The paper used pixel value differencing (PVD). In color image each and every pixel value comprises of red, green and blue component. The range of red, green and blue component in 8-bit representation is from 0 to 255. Firstly, the red component matrix is taken and 1st pixel of the block of this component in bits need to be embedded, then green component matrix need to be embedded and then blue component matrix and after that 2nd block of red matrix is considered and same approach is applied on it and so on. The blocks are extended which are based on PVD from two to eight pixel block size by human eyes. Spatial-domain and Transform domain are the two techniques of steganography. In Spatial domain, directly we embed messages into the pixel value of the intensity of the images & in transform domain firstly we transform the image into another domain and then messages are embedded in transform coefficients. When we compared the transformed result with the PVD method we get the values far better than the PVD method.

Gandharba Swain and Saroj Kumar Lenka(2012).[8]

This proposed paper presents a novel approach to RGB channel which is based on the technique of steganography. A RGB technique is also used decryption of an image. The algorithm is used at sender and at receiver end. These techniques are useful for securing the secret date. RGB channel based steganography is used so that two levels of security can be provided and also the embedding capacity is good and also the imperceptibility. The image steganography algorithm is used which is categorized into two categories, spatial and frequency domain. The steganography technique also uses LSB method inside an image. In RGB image each pixels have 3 bytes which define the intensities of the image in RED, GREEN, BLUE, channel form.

B. Karthikeyan, V.Vaithiyanathan, B.Thamotharan, S. Sruti and M.Gomathymeenakshi (2012).[9]

The main idea behind this paper is to hide the plain text into the image using a randomly generated key, with the help of EBCDIC Code (Extended Binary Conversion Decimal in code) so that the plain text would be converted to the numbers and permutation which are used with the help of keys. XOR function with key is also performed which resulted in the plain text so that this plain text can be inserted into an image. This is done in such a way so that security measures can be increased and the communication medium is secured. This technique takes the cover message and attaches the secret information.

RamanpreetKaur and Prof.Baljit Singh(2012).[10]

Basically it is the survey of various steganographic techniques so that it may be known that which technique is to be preferred for which type of image and thus providing the security. This paper proposed many techniques for hiding the messages or the secret data inside the images and these images contains the numerical values of each and every pixel where the value of the pixel is the color and the pixel intensity. The two types of images are considered i.e. size of the image can be 24 bit images and 8 bit images. Some steganographic techniques for the image file format is also described i.e. Spatial Domain technique, Masking and filtering, and transform techniques to provide the security and robustness to the image. The image type i.e jpeg,png,gif,etc is considered so that which technique is to be preferred is known.

Ajay.B.Gadicha(2011).[11]

This paper presents a LSB audio steganography in 4th bit rate method that reduces noise rate of the host audio when we embed the watermark bit. By using this algorithm message bits are attached into 4th LSB layers, which can increase strength against distortion. LSB is one of the simple algorithms in the Time domain which have large amount of audio samples with some additional information. By this method, we shift the limitation for transparent data hiding in audio from the 1st LSB layer to 4th LSB layer. If we use 4th LSB layer during watermarking, introduces the smaller error which is absolute & if we use standard method in same condition causes constant absolute error.

Surbhi Gupta, AlkaHanda, ParvinderS.Sandhu (2010).[12]

The YCbCr model is described as itis the very simple model and also its computation is fast. They also presented various attacks and also new information hiding techniques. Many techniques are used such as digital watermarking is used to protect the data and steganography is used to keep the information secret. The Pixel indicator technique is proposed for YCbCr image steganography and it uses 2 or 4 least significant bits. Now to decide which type of lest significant bits would be used is based on the characteristics of the cover image. In this paper, RSB

model of the source or the sender image can be transformed into the four color models which are as follows HSV, HSI, YCbCr, YIQ and this model uses 2 or 4 least significant bits not more than that and also provides effective result in terms of capacity.

III. CONCLUSION AND FUTURE SCOPE

A survey on various techniques has been done in order to identify and classify which technique is more secured without changing the original message. Various techniques like LSB technique, DCT, YCbCr, EBCDIC, Filtering and masking, spatial domain and transform domain, MATLAB tools have been used. The LSB algorithm is easy to implement for both 8 & 24 bit image of the same size of cover and secret image. So it is used for both grey scale and color image. This paper focuses on those techniques which are used to increase the security and reduced the noise rate of the messages. YCbCr model is a popular method for skin color detection. So it will give the better performance for illumination problem. By using YCbCr technique we can extract the features which will be helpful to make gesture for human computer interaction. In future, steganographic technique can be used with other algorithms to provide more security to send the data more confidentially and secretly without changing the contents of the original data.

TABLE I

TECHNIQUES	NAME OF AUTHOR	ADVANTAGES	DISADVANTAGES
RSA	Gandharba Swain, Saroj Kumar Lenka (2010)	Maintains the secrecy of messages.	Stego approach using RSA is less secured.
LSB	1.Gandharba Swain, Saroj Kumar Lenka (2010) 2. AmolBhujade, Prof. SonuLal (2015) 3. Neha Jain, SudhirGoswami (2015) 4. M. divyavani, Ch. Madhavi (2014)	It is not fixed to the number of bits to hide the message.	Robustness is low
DCT	RamanpreetKaur, Prof.Baljit Singh (2012)	It has the ability to pack most information in fewest coefficients.	This technique is time consuming.
YCbCr	Surbhi Gupta, AlkaHanda, ParvinderS.Sandhu (2010)	1. It makes use of the human visual system characteristic. 2. Perfect in image compression.	Its color range is restricted in the color TV images as their required compression of the information for the displayed image.
DWT	M. Divyavani, Ch. Madhavi (2014)	1. It decomposes distinct time signals. 2. It provides higher compression ratios.	It provides lower frequency Resolution.
EBCDIC	B. Karthikeyan, V. Vaithiyanathan, B. Thamotharan, S. Sruti and M. Gomathymeenakshi (2012)	Converts the plain text to the numbers and permutation.	The plaintext is hidden column wise only.
SPATIAL FILTERING AND MASKING	RamanpreetKaur, Prof.Baljit Singh (2012)	Hide the information to the noise level.	Can be used only to grey scale images up to 24 bits only.

ACKNOWLEDGEMENT

We are thankful to our Prof. K.F. Rahman who has supported and encouraged us to do this work. He helped us during our tough times and in our work. We finished our Research paper under his guidance.

REFERENCES

[1] AmolBhujade, Prof. Sonu "Advanced Steganography: Embedding High Capacity Audio in color image"(2015),International Journal of Advent Research in Computer and Electronics (IJARCE)Vol. 2, No. 6,E-ISSN: 2348-5523.

[2] Neha Jain, SudhirGoswami "An Improved SteganographyTechnique of LSB Substitution Method"(2015), *International Journal Of Engineering And Computer Science ISSN:2319-7242*.

[3] M.S. RashmiJanbandhu, Mr.ViploveKarhade, "Introduction to Steganography" (2015), International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue:4.

[4] M. divyavani and Ch. Madhavi"Lifting DWT Based Steganography by FPGA"(2014), ISSN 2319-8885 Vol.03,Issue.33.

[5] Prajakta B. Diwan, V. B. Bhagat "A Steganography Approach to Protect Secret Information in Computer Network" (2013), International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[6] Mohamed Amin, Hatem M. Abdullkader, Hani M. Ibrahem1, and Ahmed S. Sakr "Steganographic Method Based on DCT and New Quantization Technique" (2013), *International Journal of Network Security, Vol.16, No.4*.

[7] Dinesh Patil& S. M. Bansode "Secured Information Hiding Using Variable Pixel Block Size of PVD Steganographic Techniques"(2013), Department of Computer Science and Engineering, Government College of Engineering, Aurangabad (MS), India.

[8] Gandharba Swain and Saroj Kumar Lenka "A Novel Approach to RGB channel based image using steganography technique"(2012), International Arab Journal of e-Technology,Vol.2,No.4.

[9] B. Karthikeyan, V. Vaithiyanathan, B. Thamotharan, M. Gomathymeenakshi and S. Sruti "LSB Replacement Steganography in an Image using Pseudorandomised Key Generation"(2012), Research Journal of Applied Sciences, Engineering and Technology, 4(5): 491-494, ISSN: 2040-7467.

[10] RamanpreetKaur and Prof.Baljit Singh "Survey and analysis of various steganographic techniques"(2012), [ijesat]International Journal of Engineering Science & Advanced technology, ISSN: 2250–3676 , Volume-2, Issue-3, 561 – 566.

[11] Ajay.B.Gadicha "Audio steganography"(2011), International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5.

[12] Surbhi Gupta, AlkaHanda, ParvinderS.Sandhu "Implementing Adaptive Steganography by Exploring the Ycbcr Color Model Characteristics"(2010),World Academy of Science, Engineering and Technology,Vol:4 2010-10-25.