International Journal of Digital Communication and Analog Signals
Vol. 1: Issue 1
www.journalspub.com

Text Data Hiding and Extraction of Image using Discrete Wavelet Transform

*Shashank Gupta[1] and Rachit Jain[2]
[1]Student, ITM Universe, Gwalior, (Madhya Pradesh), India
[2]Assistant Professor, ITM Universe, Gwalior, (Madhya Pradesh), India

Abstract

Now a day with the wide use of multimedia is increasing to a large extent, the visual information that contains the high quality and low complexity digital images plays a very vital role in daily life solicitations such as satellite television, magnetic resonance imaging, computer tomography, geographical information systems and astronomy and many other areas. Main purpose of this paper is to investigate or develop new concepts to design digital image security system with good capacity and minimum a limited distortion in image quality. We investigate to develop the system that can accept all kinds of images that is grayscale images with the minimum complexity and highest PSNR (Peak Signal to Noise Ratio) value.

Keywords: *Multimedia, digital images, digital image security, steganography, grayscale images, PSNR*

Author for Correspondence: *Email ID:gupta.shashank75100@gmail.com*

INTRODUCTION

The image processing is defined[1] as the method or system where we give input as the images where processing methods have been applied that produces output in the form of images. The output image also shows the parameters that are used in images. These parameters further helps in defining the image in the proper way.

The classification of Image Processing[2] can be done in three types:

1. Low level image processing (that includes noise removal, image improving, contrast improvement).
2. Mid-level image processing (that includes segmentation)
3. High level image processing (that includes analysis based on output of segmentation)

Low-level processes primarily consist of operations such as image pre-processing, contrast improvement, and image refining. In a low-level process both its inputs and outputs are in the form of images.

Mid-level processing consists of tasks such as segmentation. The segmentation means dividing an image into regions or objects, explanation of those objects to reduce them to a form suitable for computer processing, and classification (recognition) of individual objects. A middle-level process generally comprises inputs in the form of images, but its outputs are attributes extracted from those images (e.g., edges, contours, and the identity of individual objects).

Generally, higher-level processing comprises "making sense" of a collaborative of familiar objects, as in image analysis, accomplishment the intellectual functions normally associated with vision.

The digital image processing refers to the processing of two dimensional pictures by

a digital computer. In a larger context, the digital processing can be applied on any two dimensional data. The digital can be represented as an array of real numbers or complex numbers that is represented by finite number of bits. This processing technique further helps in manipulation of digital images by the use of computers[3].

The major building blocks[4] for the digital image processing system are as follows:

1. Acquisition
2. Storage
3. Processing
4. Display and Communication interface

These are the major blocks which constitutes the digital image processing system. These blocks are also considered as fundamental steps, where all of these steps also have sub steps. The block diagram with all the necessary steps in digital image processing system is mentioned below[5-7].

An Investigation into Image Hiding Steganography with Digital Signature Framework[8] shows that data hiding is considered to be one of the most powerful concepts in computer security. This is considered to be important concept because in this approach, the secure transmission of the data is done over the insecure channel. This transmission is done by concealing the original information into information which is also known as cover media[9-11].

On the hand, text data hiding is considered to be of the important phenomenon in computer security applications. Therefore image hiding is gaining rapid popularity in today's multimedia field due to its prevailing applications as an image is more controlling to contain useful information. Therefore in this we have proposed a new approach, by which we have carefully investigated the concept of steganography. This careful investigation is done by incorporating image hiding within another image with a secure structural digital signature framework[12-15].

Image steganography is most popular form of steganography. Here secret message is embedded into an image as noise, which is nearly impossible to detect by human eyes. Images also have high degree of redundancy and provide higher capacity and distortion tolerance. Many programs are already available based on image steganography to hide text as steganography tools[16].

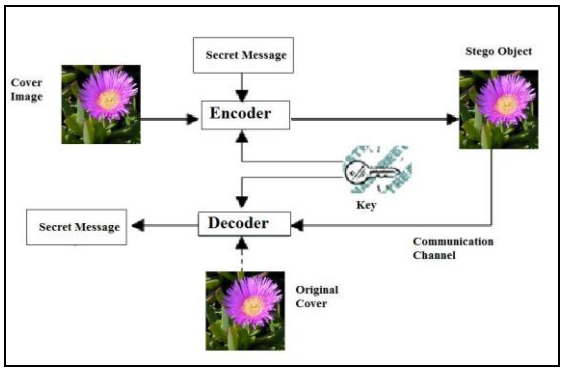

Fig. 1: *Working process of Image Steganography.*

RELATED WORK

The images now days play a very important role in the field of communication. The images are transferred from place to another in the form of signals. With the increase in the use of images, secret data can be transmitted from this place to that place. In image processing, the secret data can be transmitted in the form of images, where the secret data will be encrypted in another image with the help of secret key that is provided to both the sender as well as receiver.

1. Vladimir Banoci, Gabriel Bugar, Dusan Levicky[5]. The paper entitled "A Novel Method of Image Steganography in DWT Domain". This paper has provided a novel Steganography method for embedding the secret data in still greyscale images. To provide large capacity of

the secret data while maintaining good visual quality of stego-image, the embedding process is performed.

2. Shaveta Mahajan, Arpinder Singh[6]. The paper entitled "A Review of Methods and Approach for Secure Stenography" has provided a complete review of all the methods and approaches that has been used in making the concept of stenography secure. In this approach, we had survey several different Steganography techniques for encrypting the data.
3. Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir[7]. The paper entitled "Art of Hiding: An Introduction to Steganography", has provided the new approach that attempts to detect the requirements that are required for a good stenographic technique. This approach also determines which stenography technique is best suited for which particular applications. Since it is known that, Steganography is the art of hiding the fact that communication is taking place, by hiding information
4. F.I. Alam, M.M. Islam[8], The paper entitled "An Investigation into Image Hiding Steganography with Digital Signature Framework" shows that data hiding is considered to be one of the most powerful concepts in computer security.
5. S. Sajasi, A.M. Eftekhari, Moghadam[9]. The paper entitled "A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method", has provided a new novel approach for image stenographic for hiding a secret image in the cover image.
6. Xu Hongsheng, Jun lie Xu[10]. The paper entitled "An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding", has provided the new optical ways those posses many advantages like high processing speed, high parallel and high dimension etc.
7. Xu.Xikai Jing Dong , Wei Wang Tieniu Tan[11]. The paper entitled "Video Stegaanalysis Based on the constraints of motion vectors", focuses on detecting data hiding in motion vectors of compressed video and proposes a new steganalytic algorithm based on the mutual constraints of motion vectors. The constraints of motion vectors from multiple frames are analyzed and formulized by three functions. In this approach, the new method is being implemented against MV-based video steganography.
8. A.Kanwar, P.Upadhyay[12]. The paper entitled "An Appearance Based Approach for Gait Identification Using Infrared Imaging", has proposed a new novel approach for gait identification by the using of new imaging system. This imaging system is also known as infrared imaging. Recognition using gait is a behavioural biometric technique.
9. H.Kumar, A.Srivastava[13]. The paper entitled "A Secret Sharing Scheme for Secure Transmission of Colour Images", has provided a new approach that is based on secret image sharing and key safeguarding technique. This technique is based on effective and generalized schemes for the hiding of the colour image.

STEGANOGRAPHY METHODS AND TYPES

The ability of science of hiding the information is known as Steganography. Steganography is of Greek origin and means "concealed writing" where from the Greek word steganos meaning "covered" and the Greek word graphie meaning "writing. Steganography is the process of hiding of a secret message in such a way

that no one can able to read the message only the sender and receiver can read.

There are numerous diverse types of steganography that are widely used. Some of them are discussed here. These are as follows:

Pure Steganography

A steganograpic system can be called pure when there is no requirement before exchange of data like shared-keys. The definition can be mathematically described as The set ***(****C, M, D, E)* where C is the set of covers, M the set of messages with |M| <= |C|, E the embedding function which maps *E: C x M -> C* and D is the extracting function which maps from *D:C -> M* and the property *D(E(c,m))= m* for all (m E M, c E C) is a pure steganographic system[14].

Shared-secret Steganography

A steganographic system is called a shared-secret or shared-key or secret when it do not require prior exchange of data like shared-keys. The definition can be mathematically described as the set *(C,M,S,Ds,Es)* where C is the set of covers, M the set of messages with |M| <= |C|, e the embedding function which maps *C x M -> C* and S is the set of shared-secrets; *Ds: C x S -> M* and *Es: C x M x S -> C* and the property *Ds(Es(c,m,s) , s) = m* for all (c E C, m E M, s E S) holds is called a shared-secret stenographic system[14].

Public-key Steganography

This kind of steganography does not rely on shared-key exchange. Instead it is centered on the public-key cryptography principle in which there are two keys, one being the public key which can be usually obtained from a public database and the other a private key. Usually in this case the public key is used in the embedding process and the private key in the decoding process [14].

Different types of cover objects[15] like text, image, audio or video files can be used to hide secret data.

Text Steganography: It is one of the latest and most problematic types of steganography. It is a technique of using inscribed natural language to obscure a secret message. Text steganography is most challenging due to the presence of lesser redundancy in text documents as compared to the images and audio files[15].

Audio Steganography: Audio steganography embeds the message as noise into a cover audio file at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding messages in other media, compassion to additive random noise is also acute. Commonly used methods for audio Steganography are LSB coding, parity coding, phase coding, spread spectrum, and sound coming back hiding[15].

Video Steganography: It pertains to hide information in video files, which are generally collection of sound and images. Steganography methods that are appropriate to sound and images are also appropriate to video files. Advantage of this method is that large amount of data can be hidden inside video with smaller amount of distortion because of continuous flow of information and that might go unobserved by observer.

Image steganography: Images are used as the well-liked cover objects for steganography. A message is embed in a digital image through an embed algorithm, using the secret key. The resulting stego image is send to the receiver. On the other face, it is processed by the extraction algorithm using the similar key.During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't

guess the existence of the hidden message[16-19].

PROPOSED METHODOLOGY

We are investigating an algorithm by going through entire above related work we have discussed, to secure the data by using various different types of image Steganography techniques. We will develop an algorithm to implement discrete wavelet transform (DWT) technique to compress the image with robustness against various attacks for protection of data and Inverse Discrete Wavelet Transform (IDWT) technique to decompress the image to get the original image.

The brief presentation is given below:

DWT Technique

After LSB encryption technique the DWT is applied to the stego image. By using DWT the image is compressed. DWT is found to be more robust against various attacks. The Discrete Wavelet Transform (DWT) is being increasingly used for image code. This is due to the actuality that DWT supports features like progressive image transmission (by quality, by resolution), ease of compressed image handling, section of interest coding, etc. DWT has usually been implemented by complication. Such an implementation demands mutually a large number of computations and a large storage features that are not attractive for either high-speed or low-power applications.

IDWT Technique

After the DWT Compression, in order to get the original image the decompression is done using Inverse Discrete Wavelet Transform (IDWT) technique. By this we obtain the original stego image which consists of cover image and the secret message. After this LSB decryption is done in order to separate the hidden message from the cover image[20]. We have also analyzed Steganography based on domain type and Least Significant Bit (LSB) method is most useful method, which replaces least significant bits of cover object with secret message. It is most popular and simple technique when selling with images. It has low computational complexity and high embedding capacity[18].

In Frequency domain schemes, the secret data will be embedded into transform coefficients which are transformed first into frequency domain by various frequency domain methods like Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) etc. then secret data will be embedded into transform coefficients. A transform maps image data into a different mathematical space via a transformation equation. Discrete transformations are performed, which are based on precise functions called the basis functions[19]

CONCLUSION AND FUTURE WORK

To secure the data by using Discrete Wavelet Transforms (DWT) stenographic method for embedding confidential messages into cover images without producing any major changes has been proposed. And Inverse Discrete Wavelet Transforms (IDWT) technique to decompress the image to get the original image. Discrete Wavelet Transform is used for steganograhy which transforms image into frequency domain by into four different frequency sub-bands.

For the future work we can check our method with other steganalyser algorithms. We can extend our algorithm to a different transform domain such as contourlet transform and compare the result with our method. Also for further improvement can be done in these methods to aim fully on three estimation parameters

imperceptibility, robustness and capacity. This Improvement in PSNR and capacity can be achieved by using fusion approach rather than using only approach. More over better edge detectors can be used to have more number of edge pixels that can be used for embedding. These techniques can also be shared with many steganography techniques to provide another layer of security.

REFERENCES

1. Wawryn K., Wirski R., Suszynski R. 2D image processing for auto-guiding system, *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS).* 2011; 1–4p.
2. Khan S.A., Nazir M., Akram S., *et.al*. Gender classification using image processing techniques: A survey, *IEEE 14th International multi topic conference.* 2011; 25–30p.
3. Akshmi J.K., Punithavalli M. A Survey on Skeletons in Digital Image Processing. *IEEE International Conference on Digital Image Processing*, 2009; 260–9p.
4. Haixia Y., Xin H., Zhonghui W. A Digital Image Processing System Based on DSP. *IEEE International Conference on Information Engineering and Computer Science (ICIECS)*. 2010; 1–4p.
5. Banoci V., Bugar G., Levicky D. A novel method of image steganography in DWT domain. *IEEE International conference on Radioelektronika.* 2011; 1–4p.
6. Mahajan S., Singh A. A Review of Methods and Approach for Secure Stenography, *International Journal of Advanced Research in Computer Science and Software Engineering*.2012; 2(10): 67-70p.
7. Singh M., Rana, Sangwan B.S., *et.al.* Art of Hiding: An Introduction to Steganography. *International Journal of Engineering And Computer Science*.2012; 1(1): 11-22p.
8. Alam F.I., Islam M.M. An Investigation into Image Hiding Steganography with Digital Signature Framework, *IEEE International Conference on Informatics, Electronics & Vision (ICIEV).*2013*;* 1–6p.
9. Sajasi S., Eftekhari A.M. A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method, *IEEE Conference of AI & Robotics and 5th RoboCup Iran Open International Symposium (RIOS).* 2011; 1–7p.
10. Hongsheng X, Xu J.L., An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding. *IEEE Fifth International Conference on Computational and Information science (ICCIS).* 2013; 302–5p.
11. Xikai X., Dong J.,Wang W. et.al. Video Stega analysis Based on the constraints of motion vectors. *IEEE 20th International Conference on Image Processing (ICIP).2013;* 4422–26p.
12. Kanwar A., Upadhyay P. An Appearance Based Approach for Gait Identification Using Infrared Imaging, *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*.2014; 719-24p.
13. Kumar H., Srivastava A., A Secret Sharing Scheme for Secure Transmission of Colour Images, *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* 2014, 857–60p.
14. Baykara M., Das R. A steganography application for secure data communication. *International Conference on Electronics, Computer and Computation (ICECCO).* 2013; 309–13p.
15. Mehboob B., Faruqui R.A. A Stenography Implementation *International Symposium on*

Biometrics and Security Technologies (ISBAST). 2008; 1–5p.

16. Altaay A.A.J., Sahib S.,Zamani M. An Introduction to Image Steganography Techniques, *International Conference on Techniques Adavance Computer Science Applications and Technologies (ACSAT)*. 2012; 122–6p.
17. Hussain M., Hussain M. A survey of image steganography Technique. *International Journal of Advanced Science and Technology*. 2013; 54: 113-24p.
18. Kairm S.M.M., Rahman M.S., Hossain M.I. A new approach for LSB based image steganography using secret key. *IEEE 14th International Conference on Computer and Information Technology (ICCIT)*. 2011; 286–91p.
19. Kaur S., Bansal S., Bansal R.K. Steganography and Classification of Image Steganography Techniques. *International Conference on Computing for Sustainable Global Development (INDIA Com*). 2014; 870–5p.
20. Uday K.P., Vidyasagar K.D. An Efficient Implementation of LSB Steganography using DWT technique.10th *IRF International conference*. Chennai, 2014; Oct 8-6 1–3p.