A Review of Image Stegnography Methods Using Wavelet and Neural Networks

Anupriya Sohal
M Tech Scholar
Department of Computer Science Engineering College
SVIET (Swami Vivekananda Institute of Technology), Banur, Mohali, Punjab.

Dr.Lalita Bhutani
Associate Professor & Head
Department of Computer Science Engineering College
SVIET (Swami Vivekananda Institute of Technology), Banur, Mohali, Punjab.

Abstract- **In communication system hiding capacity of a system plays an important role for transmission. Many different ways are for hiding information such as image steganography. Image steganography is used for hiding the important information using various techniques so that it is not accessed by the unauthorized persons. Most importantly image steganography is used by two parties for sending the important documents. Image Steganography mainly uses for long distant transmission. It is used occasionally, in such cases also when encryption is not allowed. In image Steganography, useless bits of data are replaced by important useful information. While steganography has been around for centuries, the Digital Revolution has sparked a renewed interest in the field. For instance, the mass media industry has shown increasing interest in steganography to fight piracy.**

Keywords: Discrete Cosine Transform (DCT), Neural networks, RMSE (Root Mean Square Error), PSNR

I. INTRODUCTION

Over the rapid increase in development of internet requires it has become important to protect the confidential Information from the unauthorized users. This is done by various methods like data hiding using steganography. Steganography comprises of two words stegas and grafia. Stegas means cover and grafia means writing that is referred to as “covered writing”. stegnography is the science used for hiding information into information, so that it appears to nothing to be human eyes. There are many different ways for hiding the information such as in hiding inside an image, audio/video, document etc [1].Many different carrier file formats can be used for hiding the data but digital images are the most popular because of their frequency on the Internet. Image Steganography techniques are discussed for different file formats. Covered communication can be done by encrypting the password for information to be protected and the receiver used to decrypt the information using that password.

The Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) is used for JPEG images as it transforms them into frequencies. DCT is a mathematical transform (typically a cosine function) that converts the pixels by seemingly ’spreading’ the location of the pixel values over part of the image. It does this by grouping the pixels into 8 x 8 blocks and transforming

them from 64 values into 64 frequencies (DCT coefficients. By modifying just a single DCT coefficient, the entire 64 pixels in that block will be affected.

Neural networks

The network will receive the 960 real values as a 960-pixel input image (Image size ~ 32 x 30). It will then be required to identify the face by responding with a 94-element output vector. The 94 elements of the output vector each represent a face. To operate correctly the network should respond with a 1 in the position of the face being presented to the network all other values in the output vector should be 0. In addition, the network should be able to handle noise. In practice the network will not receive a perfect image of face which represented by vector as input. Specifically, the network should make as few mistakes as possible when classifying images with noise of mean 0 and standard deviation of 0.2 or less.

Architecture of neural network

The neural network needs 960 inputs and 94 neurons in its output layer to identify the faces. The network is a two-layer log-sigmoid/log-sigmoid network. The log-sigmoid transfer function was picked because its output range (0 to 1) is perfect for learning to output Boolean values.

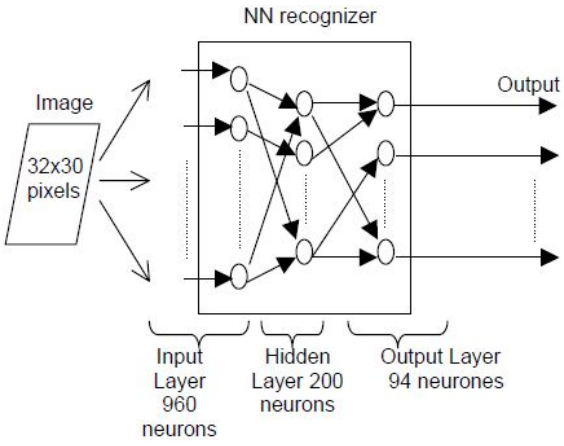

Figure 1. Architecture of neural network

The hidden layer has 200 neurons. This number was picked by guesswork and experience. If the network has trouble learning, then neurons can be added to this layer.

The network is trained to output a 1 in the correct position of the output vector and to fill the rest of the output vector with 0's. However, noisy input images may result in the network not creating perfect 1's and 0's. After the network has been trained the output will be passed through the competitive transfer function. This function makes sure that the output corresponding to the face most like the noisy input image takes on a value of 1 and all others have a value of 0. The result of this post-processing is the output that is actually used.

II. LITERATURE SURVEY

A novel approach is implemented for digital image stegnography so that secret information inside an image remains invisible to human eyes. In Image Domain, most accurate technique discussed is known as LSB for hiding information particularly inside a BMP file format

DCT (Discrete Cosine Transform) was also discussed with another tool that is named as Invisible Secret for performing Steganalysis [1]. An overview of image steganography, its uses and its technique are discussed and compared. Some approachess is more accurate as compared to than another, as the patchwork approach has high level of robustness against different type of attacks, but it can hide only a very small amount of information. Other two approaches named BMP and GIF makes up but both approaches result in suspicious files and increase the probability of detection [2]. Steganography and cryptography, both are used for data hiding using codes. Different steganography algorithms and techniques are discussed in this paper. The proposed approach provides higher security and protects the message from different stego attacks. The image resolution doesn't change much and negligible when the message is embed into the image using personal password. Therefore it is not possible for unauthorized personnel to damage the data [3].Steganography and steganalysis are important for hiding information.

Survey on steganography and steganalysis for digital images are discussed in this which mainly consists of fundamental concepts. Commonly used strategies for improving steganography security and enhancing steganalytic capability are summarized and possible research trends are discussed [4]. Steganography is the process used for hiding a secret message within in such a way that none can understand the presence or hidden within message .The main purpose of Steganography is to maintain the secret communication between two parties. Steganography is used in a modern context while providing a practical understanding of it [5].Overview of different steganographic techniques its types are discussed.Analysesof different proposed techniques is done which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. And many techniques show the indication of alteration of image as it is incorporated by noise [6].Novel approach is proposed for steganographic technique for images. To hide the secret information in original image or cover image, the effective channel selection technique is used .In image steganographic technique, information is hidden in the secret data which consist of two, three or four bits or at most five bits of a pixel in a image and gives the poor value of peak signal to noise ratio (PSNR) and high value of root mean square errors (RMSE).These two parameters shows the better results using proposed algorithm for image steganography[7].Steganography technique is used to hide the secret information in conventional media for safe transport from various public channels such as the internet. Secure random key can be shared between transmitter and receiver for blind steganography techniques for image steganography.

III. CONCULSION

Due to rapid increase of data over internet it has become very important to prevent it for unauthorized users. Image steganography is one the best technique for hiding the important information with different algorithms as it maintains secret communication between two users.

REFERENCES

1. R.Poornima, “An Overview of digital image Steganography”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.
2. T. Morkel (et.al), “An Overview of image Steganography”.
3. Ravinder Reddy Ch (et.al), “The Process of Encoding and Decoding of Image Steganography using LSB Algorithm” , IJCSET Vol 2, Issue 11, 1488-1492, |November 2012 |.
4. Bin Li(et.al), “A Survey on Image Steganography and Steganalysis”, Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011.
5. Nick Nabavian, “CPSC 350 Data Structures: Image Steganography”.
6. Mehdi Hussain (et.al), “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013.
7. Vijaypal Dhaka(et.al), “A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique”, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 8, August 2013.
8. Fariba Ghorbany Beram , “Effective Parameters of Image Steganography Techniques”, International Journal of Computer Applications Technology and Research,Volume 3,Issue 6, 361 -363, 2014,