Abstract

The idea and practice of hiding information has a long history. Cryptography came into existence for securing the secrecy of communication and many methods were developed to encrypt and decrypt data in order to keep the data secret. Using Cryptography only scrambles the data so that it is converted into a form not understandable by normal observation or it is almost impossible to know the encrypted message without the key. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called as Information Hiding or Steganography. A number of common methods of steganography are implemented and evaluated in spatial, transform domain and compressed domain using Image as well as Audio as the medium to hide Confidential Information. The strengths and weakness of the chosen methods are analyzed.

Information Hiding in Image Files

Information hiding in image files is done in three different domains.

- Spatial Domain
- Transform Domain
- Compressed Domain

Spatial Domain Methods:

In spatial domain three new methods of LSB replacement by encrypting the message before hiding are proposed. Further two new methods Kekre’s Multiple LSB Algorithm (KMLA) and Modified Kekre’s Multiple LSB Algorithm (MKMLA) to increase the cover capacity are introduced and compared with the existing algorithm. The proposed algorithms KMLA and MKMLA give better results than the existing Pixel Value Differencing (PVD) method Next
transformation functions are applied on the cover image to further increase the capacity and then PVD, KMLA and MKMLA are use to hide information in these enhanced images. Information hiding is also done in all the 3 planes of 3 different color spaces YUV, YCbCr and KLUV and their performance is compared Here KMLA is used to hide information. It is observed that L plane of KLUV gives better results compared with other planes and other color spaces used. Also as the secret message is embedded in one of the planes of the color space and then the image is converted back to Stego image, this technique is very robust from Steganalysis point of view.

**Transform Domain Methods**

Information Hiding is done using the Discrete Cosine Transform (DCT) and Discrete Walsh Transform. Instead of embedding the message in the middle frequency components a different approach is applied. Based on the threshold value considered, coefficients are found and these coefficients are replaced with secret message byte. This not only give an increase in the embedding capacity but also give the security as these elements are not sequentially located. Next, Information Hiding in the Transform domain is done for Discrete Sine Transform, Discrete Cosine Transform and Discrete Walsh Transform. To hide information two different scaling techniques are applied and their performance is compared. Normalization technique of scaling give better results than slope intercept method of scaling. Further Information Hiding in Transform Domain using Haar transform and Proposed Kekre’s Wavelet using Slope Intercept form and Normalization Technique is done and the results are compared. Here generation of Kekre’s wavelet from kekre’s transform and using it for information hiding is introduced. Here the normalization method is simplified. Here also normalization method gives better results than slope intercept form of scaling.
**Compressed domain methods**

Information hiding in a vector quantized codebook by using 1,2,3,4 and variable number of LSBs is proposed. Codebooks are prepared using four different codebook generation algorithms namely Linde Buzo Gray (LBG), Kekre’s Proportionate Error (KPE), Kekre’s Median Codebook Generation (KMCG), and Kekre’s Fast Codebook Generation (KFCG) & their performance is compared using MSE as a parameter. Further Information Hiding is done using Kekre’s Mixed Codebook Generation Algorithm. Codebooks of cover image & secret message are combined using the Shuffle Algorithm. In the existing VQ hiding approach, information is hidden inside index based cover image which results in limited hiding capacity. However, through the proposed approach by combining the codebook 100% hiding capacity can be achieved. There is only one distortion caused by VQ while reconstructing the image, no other error is introduced for images while for text, since the codebook is prepared directly by converting it into ASCII character set, no error is introduced after extraction. It is not necessary to use same VQ algorithm for both cover and secret image. This adds to the secrecy of embedded message. The algorithm is tested for Hiding Image as well as Text Information. Further Dictionary sort method is used with LSB technique and then Information hiding using VQ based on cluster size is proposed. Here regarding the different codebook generation techniques used to generate the codebooks, KPE gives better results for dictionary sort method whereas KFCG gives better results for the rest 3 methods of information hiding that are proposed over here

**Information Hiding in Audio Files**

Here, WAV audio files are used for hiding information in two different domains.
Information Hiding in Image and Audio Files

- Time Domain
- Transform Domain

Information is hidden in audio files in time domain as well as transform domain. Many novel methods are proposed in time as well as transform domain to increase the capacity of the host audio signal. In time domain two methods sensing first MSB and first two MSB’s are used to decide the number of multiple LSB’s to hide information. In this case 1 MSB gives better performance considering computational complexity as well as hiding capacity. Secret message hidden is Audio, Image or text. In the transform domain two transforms are used namely DCT and Haar transform. Different dividing factors from 2 to 100 are used for scaling the coefficients. In this case considering Bit Error Rate (BER) performance of DCT is better for dividing factor upto 10 only and thereafter performance of Haar is better.