CHAPTER 6

SUMMARY AND CONCLUSION

Information hiding for secret communication is an art of science that has been of interest for the past several decades. Steganography, the science of hiding secret message into digital medium, has gained popularity both with human, public and government organization. Recent developments in the communication and transmission medium have revolutionized the method of sharing contents among different users. This has increased concerns on security concerned with both the channel used during communication and communication message. This research work proposes techniques to address both these issues. The study focuses on strengthening the security aspects of message routing in Peer-to-Peer (P2P) networks and uses steganography to protect the messages.

An important component of any multimedia component is the images. The tremendous growth in computer hardware, software and network technologies have made it possible to distribute these images in easy, cost-effective manner, which is a golden benefit to the modern communication medium. In the 21st century, the number of people using images during communication has increased tremendously and therefore is used as the medium to conceal secret messages during P2P communication using steganography.

Thus the main objective of the research work is design and develop steganography algorithm for secure communication in P2P network. To achieve this goal, the design of the secure steganography framework consisted of two stages, where the first stage focused on developing a secure message
routing algorithm for P2P networks and the second stage focused on developing steganography algorithms.

In the first stage (Phase I of the study) used three main concepts called private key generation, peer-id signature and tracer routing to develop the secure message routing algorithm. Experimental results analyzing the proposed tracer message routing algorithm showed that the combination of the three concepts was successful in providing a secure routing environment in P2P networks.

The second and third phase of the study focus on developing steganography algorithms for hiding secret message. Two forms of secret message were considered in the study, they are text message and image. All the proposed algorithms used three steps to hide data. The first is the preparation of cover image, second is the preparation of secret data and last step is concerned with the manner of embedding and extracting the secret data. During preparation of cover and secret data, care was taken to increase the protection of the concealed messages by using different concepts like Visual Cryptography and encryption using scrambling algorithm.

The second phase explored the Least Significant Bit (LSB) algorithm while the third phase analyzed the applicability of feature based and transformation based techniques to hide secret digital data. Two algorithms were proposed in the second phase of the study. The first algorithm enhanced the LSB algorithm by increasing the payload of the algorithm. This was done by using more number of LSBs during embedding process. Moreover, a restrict pixel procedure was used to select bits that cause minimum distortion in the cover image.

The second algorithm used the enhanced LSB and combined it with enhanced DCT to further improve the steganographic process. The DCT was
enhanced by combining it with a Huffman coding. Different types of DCT variants were also analyzed. The DCT variant types considered are 1-DCT, 2-DCT, 3-DCT and 4-DCT. The algorithm first applied any one of the DCT types on the cover image to obtain DCT coefficients. Next, Huffman coding was used to encode the secret message. The DCT bits of the cover image were then replaced by the Huffman bits of the secret image using enhanced LSB algorithm. After transmission, to extract the original secret message, an inverse DCT is applied.

In the third phase of the study, a feature based algorithm called KP-Gilles was enhanced for steganographic purposes. The enhancement methods include usage of regions instead of single pixels during feature detection and after identifying salient features an inverse operation was used to select non-salient features that will cause minimum distortion after embedding the secret data into the cover image.

The transformation based method proposed enhanced Discrete Wavelet Transformation (DWT) with Singular Value Decomposition (SVD) and VC. The cover data was decomposed using DWT and the secret data was decomposed using SVD. After preparing the cover and secret data, a shuffling algorithm was used to embed the secret data into the cover data. The extraction process is the reverse operation of the embedding process.

The proposed steganography algorithms were analyzed on their embedding capacity (payload), perceptibility (transparency), robustness, security against attacks and complexity in terms of time required to embed and extract the watermarks. The analysis was based on Peak Signal to Noise Ratio (image quality), Figure of Merit (edge preservation capacity), Mean Structural Similarity Index (MSSI), Normalized Correlation (resistance to attacks) and Execution Speed (time complexity). During performance evaluation a total of ten attacks, categorized into four groups, were selected. They are compression
attacks (JPEG 50%, JPEG 2000 50%), Filtering attacks (Gaussian Noise, Median Filter), Distortion attacks (Blurring, Gamma, Cropping, Resize and Rotation) and transformation attacks (Affine). A dataset was created with 50 cover images (≤512 x 512), 50 secret images (≤256x256) and 50 secret message files (≤5000 bytes after encryption). From the experimental results, the following findings were ascertained.

1. In all phases of the study, the proposed models performed better than its existing counterparts, indicating that the enhancement procedures incorporated are successful in hiding secret data.

2. From Phase I of the study, it can be understood that the proposed tracer message routing is resistant to attacks and offers secure routing in P2P networks.

3. The introduction of Visual Cryptography during the preparation of cover and secret data has enhanced the security of all the proposed steganography algorithms.

4. The high PSNR and NC values obtained in both Phase I and Phase II by the proposed models while analyzing with the various attacks, indicates that the proposed steganography algorithms are highly resistant to different types of attacks and hence are more efficient in concealing and protecting the secret image.

5. The high PSNR, FoM and MSSI values obtained by the proposed algorithms reveal that the stegano images after embedding secret data is very similar to the cover image. This indicates that the secret data embedded in the cover image introduces minimal distortion to the cover data.

6. In Phase II, with all parameters, the L2LSB model performed better than the LSB model. From the results obtained for the
selected properties of steganography (capacity, invisibility, resistance against attacks, robustness, imperceptibility and speed), it can be understood that the LSB model is best suited to hide text data rather than image data into the cover image.

7. Comparison between the coupled DCT models revealed that the application of coupled 2-DCT with L2LSB and Huffman coding improved the performance of steganography with respect to all selected parameters. Moreover, it was also found that these algorithms produced competent results while using it for hiding image data.

8. Analysis of the VCBPM algorithm experimental results revealed that the algorithm produces high performance with respect to all parameters when used to hide image data into the cover image.

9. Similarly, the results of VCWS algorithm showed that again the algorithms are more comfortable to store image data into cover image.

10. Thus, the proposed L2LSB algorithm is best suited for text steganography, while the CL2DCT, VCBPM AND VCWS algorithms can be used to store secret image into cover image. The winning algorithm among the three algorithms suited for hiding image data is VCBPM, followed by VCWS.
FUTURE RESEARCH DIRECTIONS

The following points can be considered in future to enhance the operations of the proposed steganography algorithms.

1. The introduction of hybridization has paved way to increase the efficiency of an application by combining the advantages of different models into a single frame. In a similar fashion, the following hybridization can be considered and developed to enhance the operation of hiding secret data into images.
   a. 2-DCT and DWT + SVD algorithms
   b. Enhanced KP Gillies can be combined with 2-DCT or 2D DWT
   c. Enhanced KP Gillies with L2LSB algorithm

2. The binary Visual Cryptography algorithm used in this study can be extended to gray scale and color images and their effect on watermarking properties can be studied.

3. While performing experiments, the images considered were of high quality only. Future research methods, can consider noisy images, images with different intensity and frequency.