International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5, January 2019

A Secure Model for Hiding Multimedia Files within Two Cover Images

Najla Nazar, R. Satheesh Kumar, M.Rajeswari, G. R. GnanaKing

Abstract: ***Steganography, technology of information hiding that allows people to communicate secretly, in which actual data will be kept hidden inside the cover object. This paper deals with multimedia hiding system in which secret multimedia file is kept hidden in dual cover images. The proposed model takes the secret multimedia file and divided it among two cover images of same dimensions and size. The multimedia files are considered as a continuous byte and then it is vertically split into two halves, in which one half is the most significant half bytes, and the other half is the least significant half bytes. Then the two halves are embedded inside the two cover images using a four bit least significant replacement technique. To avoid capture of stego images by an attacker, it is expected to sent stego images separately through different channels. The secret multimedia file can be extracted by combining least significant half bytes of two stego images. The recovered secret multimedia file is similar in structure and content with original hidden multimedia file.***

Index Terms: ***steganography; multimedia file; dual hiding; cover image; vertical splitting; stego image.***

I. INTRODUCTION

The type of information traded over the computer network has shifted from text to multimedia files including images, audio files and video files. Sometimes such file contains confidential information that need to be protected from intruders. Protecting multimedia files requires preventing them from illegitimate users. Two methods for data protection are Cryptography and Steganography. In cryptography the data is converted to unclear format which makes it difficult to understand by an attacker. But the main drawback of cryptography is that it attracts the attention of attacker and also the key management used in cryptography is difficult for users.

Whereas in steganography the secret data is kept hidden inside the cover file. Three basic terms used in steganography are

- Cover file: Original file in which secret information will be stored. It can be text, image, audio and TCP/IP packets.
- Secret file: Information which is to be hidden.
- Stego file: File in which the information is hidden that is combined cover file and secret file.

Based on the cover file used there are different types of steganography like image steganography, text steganography, audio steganography and TCP/IP steganography. Our system comes under image steganography as we are using image as the cover file.

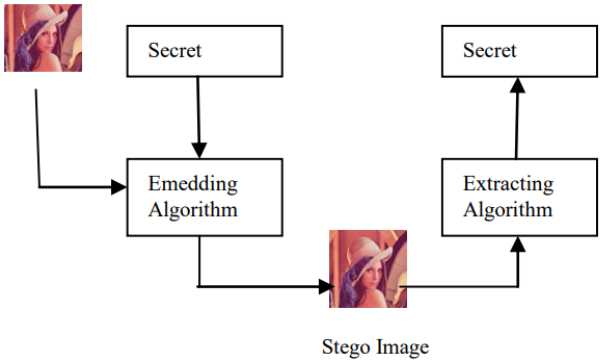

Fig 1: Image Steganography

A multimedia hiding system is comprised of two steps: embedding and extraction. In embedding process, the secret file is hidden inside the cover file. It is done by replacing the bits of cover file with bits of secret file. And in extraction step the embedded file is recovered from stego file.

The main objective of our work is designing a multimedia hiding system that enhance the security of audio/video files, by hiding it in two RGB cover images, with the objective of decreasing the size of the cover image, improving the capacity of hiding, and using a safe division protect the secret multimedia file.

II. BACKGROUND

Usually audio and video files are larger in size than image and text documents, so it requires cover files with high embedding space. As in the work in [2] data compression is one method for reducing the capacity of hiding, but most of the multimedia files will be in compressed form; as with video and audio files, therefore, compressing further can affect the quality of video and audio.To improve the hiding space that is required for embedding a audio/video file of large size is to use a cover with large size or more than one cover can be used. Large size of cover has its disadvantage like limitations of file size on file transfer systems and email.

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author
Najla Nazar*, PG Scholar, Sahrdaya College of Engineering and Technology, Thrissur, Kerala.
Dr. R. Satheesh Kumar, Associate Professor in CSE, Sahrdaya College of Engineering and Technology, Thrissur, Kerala.
Dr. M. Rajeswari, Associate Professor in CSE, Sahrdaya College of Engineering and Technology, Thrissur, Kerala.
Dr. G. R. Gnana King, Associate Professor in ECE, Sahrdaya College of Engineering and Technology, Thrissur, Kerala.

So, it is more sensible to divide the secret audio/video file over multiple covers[13], thereby the covers size required can be reduced, but the question is about the best cover number.

Increase in the covers number can result in more overhead as it is difficult to manage more than one cover, while decreasing the covers number results in covers of larger size. In this work, two covers are selected for embedding a audio/video file, that can be increased to more covers if required.

Although data embedded inside stego medium are treated to be secure from access by intruders, but extra steps for the security of embedded data is found as necessary, as there is development in the steganalysis measures that can recognize and also recover the embedded secret data [3, 4, 5, 6].

Many researches have presented to merge steganography and cryptography [7]. With cryptography, as the second layer for security has its disadvantages, as explained before. Hiding in multilayer can increase safety, but by each new layer, the capability of hiding is decreased. In this work we have selected a method for giving more protection for the embedded data by dividing the audio/video file into two part where one fragment is not able disclose any part of the hidden data on its own.

The LSB (Least Significant Bit) replacement method is an apt method for high hiding capacity which does not include compression and it also gives excess area for hiding secret file in the cover file [8]. There are different types of the LSB technique based on the number of bits to be replaced, such as 1 bit, 2 bits, 3 bits, and 4 bits. Replacing bits will be least significant bits. Some LSB techniques in RGB images replace only the least significant bit of the blue channel (right most byte), while other techniques replace the LSB of all channels [9]. The use of 4 bit replacement for hiding in the all medium allows fifty percentage capability of hiding in the selected cover file, which has been proven to have sufficient visual perfection among cover and stego images [10].

III. THE PROPOSED SYSTEM

The proposed data hiding model performs actions required for embedding multimedia files in cover images, recovering the embedded file without any alteration and evaluate the image quality between the original and stego images.

The model comprised of two modules: Embed and Extract.

a. Embed

Through this process the secret file is stored in two cover images. The multimedia files are considered as continuous bytes then it is vertically split into two halves, in which one half is the most significant half bytes and the other half is the least significant half bytes.

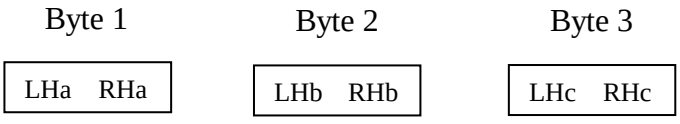

Fig 2: Secret File

Then each half byte is embedded in two covers using four-bit LSB replacement method, the MSB half byte (LH) can be embedded in cover1 and LSB half byte (RH) in cover2 or vice versa. In 4 bit least significant replacement technique four least significant bits of cover image are altered based on the secret message.

Fig 3: Stego Images after Embedding

b. Extract

Through this process the hidden multimedia file can be retrieved without alteration. It is done by combining the four least significant bits from the two stego images. The recovered multimedia file is same in structure and content with the hidden multimedia file.

A. Design Factors

The design factors that need to be considered are:

1. The secret multimedia files are stored in two BMP RGB cover images, such that one stego image will contain fifty percentage of the hidden data. Same cover image is allowed to use two times (as cover1 and cover2), or use two images with same dimensions and size.
2. The 4-bit LSB replacement technique is used to hide secret data in the all medium of the two cover images, where the least significant half bytes of the cover's red, green and blue channel replaced with the secret file half bytes.
3. Recovered multimedia file will be a multimedia file that is similar to the original multimedia file. The secret audio/video file and the recovered file undergo a bitwise comparison using Windows command File Compare (FC) which shows no differences.
4. The Peak Signal to Noise Ratio (PSNR) value which compares the cover images and the stego images must be similar to the value computed by a standard software for comparing the image like ImageMagick.
5. The RGB BMP cover image size should be almost same as the secret file size or only an increase of 54 bytes from the size of secret file is allowed, which is the header size of BMP file. The cover image's Embedding Capacity (EC) is same as the the secret file size will be adequate cover image is equal for storing the half bytes of the audio/video file, using the four bit least bit replacement. For each cover the EC in bytes can be computed as:

$$EC = Width \times Height \times {}^{3}/_{2}$$

IV. RESULTS AND DISCUSSIONS

The multimedia hiding system was used for hiding audio/video files of different sizes, and of various formats. The secret multimedia files can be MP4 video, MP3 audio, WMV files, JPG, PNG, BMP, TIF and GIF images. Two RGB images which is uncompressed and in BMP format is the cover images with adequate embedding capability for hiding the audio/video files. The dataset of multimedia files and cover images has been available online in [11].

The proposed model relies on the least significant bits (LSB) method for hiding secret data in 4-LSB bits of each of the RGB channels, in two cover images of same size and type, with the aim of achieving high hiding capacity as well as to enhance security. All secret audio/video file is divided vertically, and the two fragments are embedded in two cover images separately, as Stego1 and Stego2, to protect the privacy of the hidden data, in case if it is recovered by an attacker.

The PSNR values for the covers and the two stego images are calculated for all embedding step. The SCR ratio is computed as the fraction of size of hidden audio/video file and the size of one cover image. This measure was presented in [7], as an important metric for utilizing the hiding capacity and can be used in combination with the PSNR measure.

A. Visual Imperceptibility Results

In this experiment, we have used a collection of secret multimedia files ranging in size from 4.8 KB to 9.01 MB, of various types. The cover images are large BMP images that can accommodate the largest secret multimedia file of our selected dataset. The visual imperceptibility comparison is demonstrated using a set of cover and stego images, for selected secret files of large, medium and small sizes, as shown in Figures 4 to 7.

Figure 4 shows Lena.BMP (36.2 MB, dimensions 3560 x 3560) and Stego1, and Stego2. The two stego images was embedded with the image renoir4-512.BMP (588 KB).

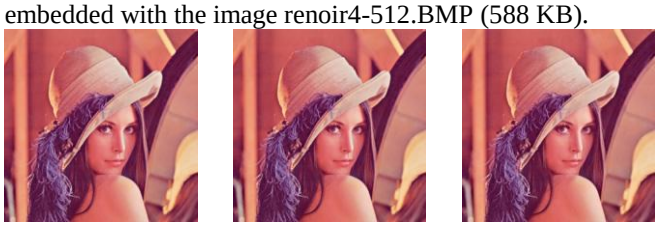

Fig 4: Lena Cover +renoir4-512.BMP with Stego1 and Stego2

Figure 5 shows Labelle.BMP (36.2 MB, dimensions 3560 x 3560) and Stego1, and Stego2. The two stego images was embedded with the audio Elisa.MP3 (1.46 MB).

Fig 5: Labelle Cover + elisa.mp3 with Stego1 and Stego2

Figure 6 shows Labelle.BMP (36.2 MB, dimensions 3560 x 3560) and Stego1, and Stego2. The two stego images was embedded with the video First-day-of-spring.MP4 (76.6 KB).

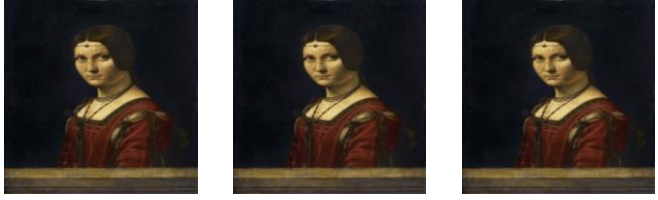

Fig 6 Labelle Cover + First-day-of-spring.mp4 with Stego1 and Stego2

Figure 7 shows Lena.BMP(36.2 MB, dimensions 3560 x 3560) and Stego1, and Stego2. The two stego images was embedded with the image Vase512.JPG (490 KB).

Fig 7 Lena Cover + Vase512.JPG with Stego1 and Stego2

V.CONCLUSION AND FUTURE WORK

This work investigated the enhancement of securely sending multimedia files, over communication channels, through embedding them within two RGB images. The advantages of using two RGB cover images are higher hiding capacity, which is needed for multimedia files and better protection of the hidden data. The proposed system and its implementation have presented a solution in which the secret multimedia file is split vertically into two fragments, where each half is stored in a separate cover. Using this method, one vertical half of the secret message will not provide any clue to the attacker about the contents of the secret message, if she/he succeeds in capturing a stego image and extracting its contents.

Some of the interesting extension to this work include hiding multiple secret files in several covers, experimenting the idea of multiple covers into video and audio, and increasing security of the proposed system by randomly placing the secret data in the covers.

ACKNOWLEDGMENT

The authors acknowledge the use of the publically available images and multimedia files in the dataset website [11].

REFERENCES

1. A. Cheddad, J. Condell, K. Curran, & P. McKevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, 90(3), 727-752, 2010.
2. R. R. Koppola, “A high capacity data-hiding scheme in LSB-based image steganography, Master thesis, University of Akron, 2009.
3. H. G. Schaathun, “Machine learning in image steganalysis”, John Wiley & Sons, 2012.
4. A. Aljarf & S. Amin, “Filtering and Reconstruction System for Grey-Level Forensic Images”, 17th International Conference on Image Processing (ICIP 2015) Zurich, Switzerland, 2015.
5. A. Aljarf, S. Amin, J. Filippas, & J. Shuttelworth, “Develop a detection system for grey and colour stego images”, International Journal of Modeling and Optimization, 3(5), 2013.
6. A. D. Ker, “Batch steganography and the threshold Game”, in Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505 of Proc. SPIE, pages 04 1–13, 2007.
7. K. Joshi, K., & R. Yadav, “A new LSB-S image steganography method blend with Cryptography for secret communication”, 2015 Third International Conference on Image Information Processing (ICIIP), pp. 86-90, IEEE, 2015.
8. T. Morkel, “Image steganography applications for secure communication, Master thesis, University of Pretoria, 2012.
9. G.R. Manjula & Ajit Danti, “A novel hash based least significant bit (2-3-3) image steganography in spatial domain”, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, 2015.

10. M. Qasem, “Hiding secret image within RGB images using an enhanced LSB method”, Master thesis, Middle East University, Amman, Jordan, 2014.
11. M. T. Al-Bayati & M. M. Al-Jarrah, “DuoHide Steganography Dataset”, available online on: www.duohide.com, viewed on 30/6/2016.
12. M. T. Al-Bayati, “The hiding of multimedia secret files in dual RGB cover images using LSB steganography techniques, Master thesis, Middle East University, Amman, Jordan, 2016.
13. Marwa Tariq Al-Bayati, Mudhafar M. Al-Jarrah. "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images", 2016 9th International Conference on Developments in eSystems Engineering (DeSE), 2016
14. Johncy John, K.R. Joy. "Large Scale Image Search Using Data Compression Technique and Relevance Feedback in Raspberry Pi3", 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018
15. Sherin Sugathan. "An improved LSB embedding technique for image steganography", 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 Crossref
16. Raftari, Neda, and Amir Masoud Eftekhari Moghadam. "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", 2012 Sixth Asia Modelling Symposium, 2012. Crossref
17. Anita Babu, Vince Paul, Dimple Elizabeth Baby. "An investigation of biometric liveness detection using various techniques", 2017 International Conference on Inventive Systems and Control (ICISC), 2017