A Secure Image Steganography Technique to Hide Multimedia Files in RGB Images

Revathy N, Vijitha G (Assistant Professor)
Dept. of Electronics and Communication Engineering.
JCET, Palakkad, India

Abstract**—***Steganography the art of concealing a secret message inside a cover medium is a field that is still being investigated. A lot of developments are happening in steganography, as information security is a need of the hour. In the present scenario, communications no matter whether private or public is happening through Internet and other social networking sites. Internet is not a safe area for secret communication because hackers and eavesdroppers are flying around to get into the secret communication space. This paper deals with hiding multimedia files in true color RGB cover images with an aim of reducing the cover image size, increasing hiding capacity and enhancing security of the hidden data. A secure image steganography technique is presented in which a secret audio, video and image files are hidden inside two RGB cover images, regardless of its type, and is processed without compression. The cover images can be same images or images of same size. The multimedia files are split vertically into two parts; one part contains the least significant half-bytes, and the other part contains the most significant half-bytes. The two parts of secret files are hidden inside two uncompressed RGB cover images using a least significant 4-bit replacement technique. The embedding of the secret files is performed in RGB components of the image. The resulting dual stego images are sent through a communication channel. Extraction of the secret file is achieved through merging of LSB and MSB of the secret files. The extracted files are identical to the original embedded files. The proposed model provides better security of the hidden file, in case an attacker captures any one of the stego images and recover the hidden content the attacker will only get* a *set of half-byte bits, using these half bytes the original hidden data cannot be formed. The proposed method can be used for communication in applications that limit the cover image size.The other advantage of the proposed system is that hiding a video file inside an image is not commonly used due to the large video size compared to the cover image.Here two cover images are used to hide a video file so the problem of selection of large cover image is over come.Also the hiding of video file inside an image affects the visual quality of an image. But if the idea of splitting and hiding is used, along with a video file, an audio and image files can also be embedded without compromising the visual transparency, capacity and security***.*** *The performance of the proposed system is evaluated using PSNR, MSE and SSIM and is implemented using MATLAB.*

Keywords—cover image; stego image; vertical splitting; PSNR; LSB substitution.

I. INTRODUCTION

Multimedia file transfer over the Internet is becoming an important part of information technology usage. The data is exchanged over the Internet without sufficient protection. The use of social networking sites for sending data of critical importance like official data of national importance through an unprotected world is very dangerous. Sending unprotected sensitive documents over the Internet is risk prone, especially in this imperfect world where criminals and hackers are flying over the Internet to get into our private space. Therefore, it is high time to demand for better security measures and procedures, to prevent unauthorized access to our private documents, during transmission over the Internet and other unprotected local networks. Best use of the available technologies should be incorporated to improve the security of information that is to be transmitted. Securing our multimedia data means preventing unauthorized users from access, distortion, destruction, detection or modification of the data during its transfer, and any system that transmit such data through communication channels should provide necessary security mechanisms to protect the transmitted data. The security level of certain information will be very high; for example banking and military applications. The information exchanged in this field is very sensitive and are vulnerable to different type of attacks. Such data require high-level sophisticated security measures to preserve the data.

The proposed system hides multiple multimedia files in RGB color images without causing significant visual quality distortion to cover images. The multimedia files are nothing but an audio, video and image files. Embedding of all the three-multimedia files require large cover size, But in the proposed system a vertical splitting of multimedia files is done to split the secret files into two halves, one portion LSB and second portion MSB. The two halves of the input files are concealed in two cover images. The two cover images are used to reduce the cover image size that is required when embedding the three files in a single cover image. Vertical splitting is performed to enhance the security of the system. If only one portion of each files is embedded in a single cover image, an intruder cannot guess what type of information is embedded in it, so splitting and hiding increases the security level as well as capacity of the system. The hiding is performed using LSB substitution technique. LSB substitution reduces the embedding time and complexity. As hiding a video inside an image itself is a complex task, using an appropriate method for embedding the input files can reduce further complexity. The secret files are hidden in Red, Green and Blue portions of the image. Embedding in all the three planes will provide enough space to embed large size files.

II. PROPOSED SYSTEM

The proposed system comprises of two phases:

- Embedding phase
- Extraction phase

In the embedding phase the multimedia files are hidden inside two cover images. The multimedia input files are an audio file, a video and an image file. Processing of a video file is a complex process compared to processing of an image. A video is actually collection of frames or high-resolution images where movement of these frames at a fixed rate provides the effect of a moving object or a scene.

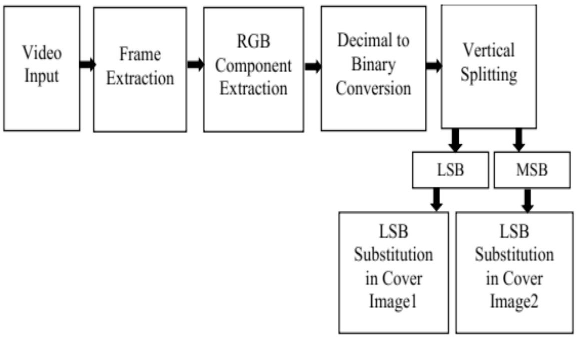
Video Input
Frame Extraction
RGB Component Extraction
Decimal to Binary Conversion
Vertical Splitting
LSB
MSB
LSB Substitution in Cover Image1
LSB Substitution in Cover Image2

Fig 1: Block diagram of hiding video file

Along with a video file an audio file is embedded. Hiding of audio file is given in figure 2

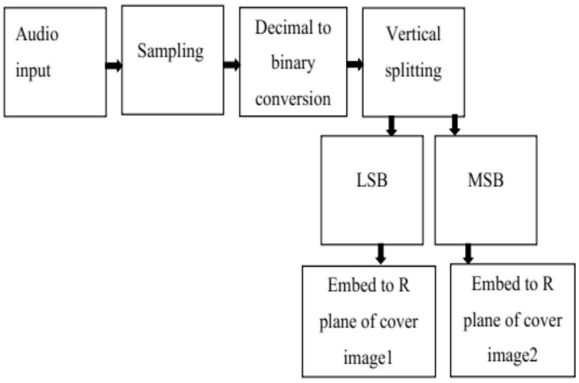
Audio input
Sampling
Decimal to binary conversion
Vertical splitting
LSB
MSB
Embed to R plane of cover image1
Embed to R plane of cover image2

Fig 2: Block diagram of hiding audio file

A secret image is hidden inside the selected cover images as shown in figure 3

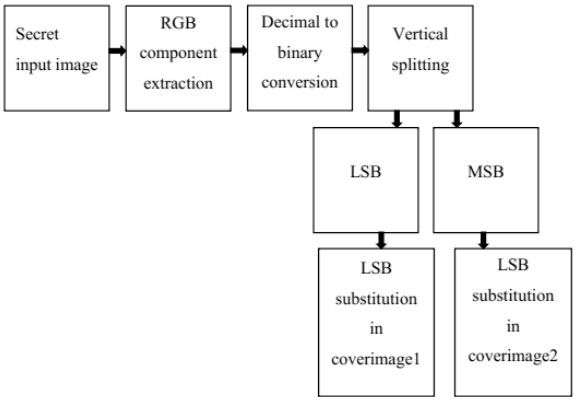
Secret input image
RGB component extraction
Decimal to binary conversion
Vertical splitting
LSB
MSB
LSB substitution in coverimage1
LSB substitution in coverimage2

Fig 3: Hiding secret image

The cover image 1 contains the LSB portions of the secret video,audio and image file.The resulting file after hiding the secret files is called stego image 1.The cover image 2 contains the MSB portions of the secret files.The resultant file is called stego image 2. In the extraction phase, the input to this phase is two stego images. The stego images carry the secret video, audio and image. Only half of the audio, video and image will be present in each stego image. So in the extraction phase the LSB and MSB of the audio, video and image are extracted from the stego images in the hidden order and combined together to get the original audio, video and image.

The various steps involved in the embedding and extraction procedure is given below.

- Select the cover image that is used to hide the multimedia files.
- The images are converted to RGB format and then convert the RGB components to corresponding bits. Extract the LSB portion from the first cover image
- Select the video file to be hidden. Separate the frames and calculate the number of frames.
- Separate R, G and B from each frame and convert to bits
- Consider the first frame. Extract the LSB of the first frame. Embed the LSB bits in the R plane of the first frame to the LSB bits in the R plane of the cover image. Repeat the LSB replacement in the R plane until the LSB bits in the R plane of the last frame is replaced with that of LSB bits in the cover image 1.Next consider the G plane of the first frame. Extract the LSB bits in the G plane and embed the G plane bits of the first frame to the G plane bits of the cover image 1. Repeat this step until the bits of G plane bits of the last frame in the video is reached. Next consider the B component in the video frame.

Extract the LSB bits of first frame and replace the LSB bits of B component in the cover image with the LSB bits of B component in the video frame. Continue this embedding procedure until the last frame is reached. Half portion of the input video embedding procedure is finished.

- Next consider the second cover image. Extract the RGB components in the selected image. Now consider the first frame. Embed the MSB bits of the R, G, and B components of the first frame into the LSB bits of the R, G, and B components of the cover image 2 respectively. This process is repeated until the MSB bit of the last frame is hidden inside the cover image.
- From the last position of the LSB replaced in the R, G and B components of the cover images the secret image hiding starts. It is very important to note this last positions otherwise when a single bit gets interchanged the entire data hiding process will be effected. Now 65, 66,400 locations are used to hide a video file. As per the design the total cover image size>=68, 87,488 locations. After embedding the LSB and MSB of the video file, remaining cover image size is calculated. Also note the last position where the bits of last frame is embedded. The secret image file is embedded from this position onwards.
- The secret image to be hidden is selected. The image is vertically split into MSB and LSB after RGB component extraction. The LSB of the R, G and B components of the cover image 1 is replaced with the LSB of the R, G and B components of the secret image respectively. The LSB of the R, G and B components of the cover image 2 is replaced with the MSB of the R, G and B components of the secret image respectively.
- The audio file is embedded in the R component of the cover images. Sample the recorded audio data and convert it to binary value. Then split the audio data into MSB and LSB. The LSB portion of the R component in cover image 1 is replaced with LSB bits of audio data. The MSB portion of the R component in cover image 2 is replaced with that of the MSB portion of the audio file.
- The hiding of video, audio and image file is implemented.
- The next process is extraction of the embedded files.
- In the extraction process at first the video file is extracted. Extract the first 65, 66,400 bytes of stego image 1 and store it as the LSB bits of the video file. Next extract the first 65, 66,400 bytes of stego image 2 and store it as the MSB bits of the video file. Combine both MSB and LSB and reconstruct the frames. After reconstructing the frames assign the frame rate at which the original video was played. The original video is extracted from the stego images without any change
- Next step is to extract the secret image. The secret image is hidden from 65, 66,401 to 66, 24,001 locations in the stego images. The LSB bits of the stego image 1 is extracted and stored as secret image LSB and then the MSB bits of the stego image 2 is extracted and stored in secret image MSB. next the MSB and LSB are combined to form the original secret image.
- In order to extract the audio file extract the R components of the stego images 1 and 2.The audio data is embedded from 66,24,001 to 66,87,489 in the R component of both stego images. Thus the extraction of data in these locations results in the original audio data. The LSB of the R component in stego image 1 is extracted and saved as LSB of audio signal. After that the LSB of the R component in the stego image 2 is extracted and saved as MSB of the audio data. Now combine both MSB and LSB and the embedded audio file is extracted.
- All the three hidden multimedia files are extracted successfully.

III. RESULT

The image shown in fig 4 is used as cover image and is in jpeg format

Fig 4: Cover Image

The video shown in Fig 5 is used as secret data to hide inside the cover image (fig 3). This video file is in avi format.

Fig 5: Secret Video Frame

The secret audio file shown in Fig 6 is used to hide inside the cover image (fig 3).

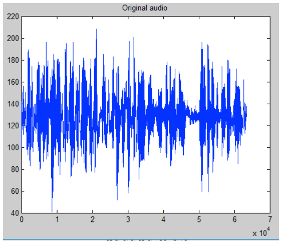

Fig 6: Secret audio signal

The secret image shown in the Fig 7 is used to hide inside the cover image (fig 3). The image is in Jpeg format.

Fig 7: Secret image file

The above secret files are embedded inside the two cover images and the resultant stego images are obtained. The resultant stego images are shown in the below fig 8.

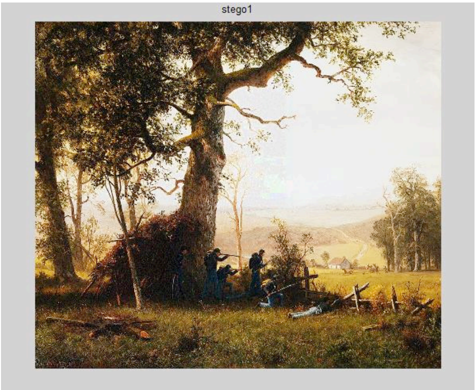

Fig 8: Stego image1 with multiple files embedded

The LSB portion of the secret files are embedded inside the cover image1 resulting in the ouput stego file 1.The MSB portions are hidden in second cover image and the resultant stego file 2 is shown below fig 9

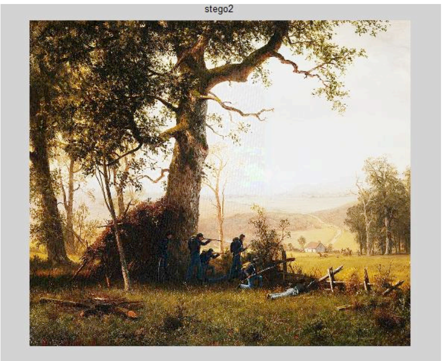

Fig 9: Stego image 2 with multiple files embedded

The visual quality of the stego images is calculated using the performance evaluation metrics. The experiments are conducted in the presence of a noicy channel and then the PSNR is calculated. The standard PSNR value for maintaining visual imperceptibility is PSNR of the stego images with above 30 DB .If the PSNR is above 30 DB then the secret data hidden cannot be detected by a normal vision. The obtained PSNR value of stego 1 is 33DB and of stego 2 is 34 DB. The PSNR values are calculated by comparing the stego images with original cover images.

CONCLUSION

The proposed system embeds multiple multimedia files in dual RGB images. The proposed system uses two cover images for hiding a video, audio and an image file. The secret data is split into two halves and one half is embedded in one cover image and other half in second cover image by using LSB substitution method. The PSNR values of both stego images are calculated and is above acceptable level, which means embedding multiple multimedia files in RGB images will not degrade the visual quality of the cover images.

Acknowledgment

At the outset, I thank God almighty for making my endeavour a success. I am very much grateful to Dr. V. P Sukumaran Nair, the Principal of our college for supporting all the way long. I also express my gratitude to Prof. C.Venugopal, Head of the Department of Electronics and Communication Engineering, JCET for providing me with adequate facilities, ways and means by which I was able to complete the project. I express my sincere gratitude to my guide Ms. Vijitha G, Assistant Professor, Department of Electronics and Communication Engineering, JCET for her constant support and valuable suggestions without which the successful completion of this project would not have been possible. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Electronics and Communication Engineering, JCET for their cooperation and support. Last but not the least I thank all others and especially my classmates and my family members who in one way or another helped us in the successful completion of the project.

References

[1] "Image Steganography Applications For Secure Communication", Tayana Morkel, 2012

[2] "Steganography And Its Applications In Security",Ronak Doshi et.al;International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012"

[3] DuoHide: a Secure System for hiding multimedia files in dual RGB cover images, Marwa Tariq Al Bayati & Mudhafar M Al-Jarrah, 9th international conference on developments in eSystem engineering.

[4] "Steganography based on random pixel selection for efficient data hiding",Shamim Ahmed Laskar and Kattamanchi Hemachandran , International journal of computer engineering technology (ijcet)

[5] "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain", G.R.Manjula and ajitdanti, International Journal of Security, Vol4, 2015

[6] "Image Steganography Technique Based On Predetermined Pattern And Histogram Analysis",Haya Mohammad Al Haj

[7] "Pixel Indicator Technique For RGB Image Steganography", Adnan Abdul-Aziz Gutub, Journal of Emerging Technologies in Web Intelligence, February2010

[8] "High Capacity Image Steganography Technique Based On LSB Substitution Method", marghny h. Mohamed, loay m. Mohamed, applied mathematics & information sciences an international journal, 2016