www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 17038-17044

Image Steganography with the password authentication using CHAP protocol

Pooja S Devagiri, Dr S L Desphande

Visvesvaraya Technological University Belagavi

Introduction

The growth of technology to exchange information in the field of computer network like Internet, mobile communication has been increased and for exchange of information between two users Internet is used as the main source and this exchange of information is not safe which has led to many serious problems such as hacking and duplications. Consequently it is important to give a security of data. Cryptography and steganography are the two important methods which are used to provide a security for the information. Cryptography is a process of study of hiding the information and it deals with the encryption of message, so that user is unable to read the message but the communication is being visible. steganography is the procedure of covering the message so that the correspondence is imperceptible from the client.

Steganography has some of the terminologies like cover file, secret message, stego image and the stego password. The cover file is the carrier for hiding the secret information and secret message is the actual data that need to be shared. And secret data can also be in encrypted form which provides more security and after embedding secret message in cover file new file is generated called stego file which has the secret message in it and stego password is used for embedding and extracting the data from both the cover file and the stego file.

The use of cryptography it is possible to encrypt the message in which user is unable to read the message but as communication is visible, and the third person may comes to know that the message

DOI: 10.18535/ijecs/v5i6.44

is sent in encrypted format and tries to hack the message. On the other hand steganography avoids the drawing suspicion of the presence of the hidden message, which is statistically undetectable. In this article both the cryptography and steganography is used which is called dual steganography.

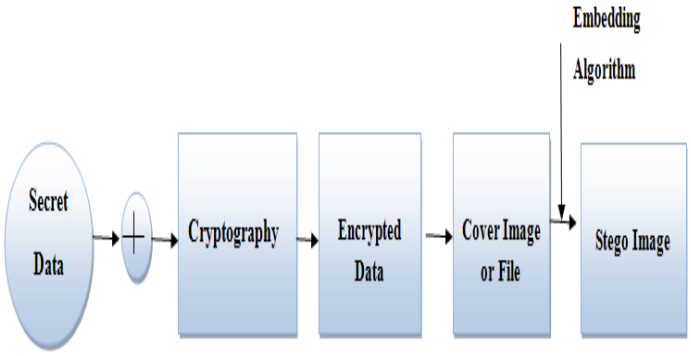

Figure 1 Dual Steganography

The figure shows the dual steganography process which contains the secret data which is audio file and cover image or cover file is one which contains the original message and stego image is one which has the secret message within cover file that is after embedding the audio file within the digital image. First the secret information is encrypted and then in digital image the information is embedded and the new image formed that is stego image is same as the cover image in human perceptible way which provides the high security.

Index Terms

Stegnography, Dual Stegnography, Cryptography, Least significant Bit [LSB], Digital Image, Challenge Handshake Authentication Protocol [CHAP][6].

I. Objective

The principle of this article is to give the safe correspondence between the two clients by concealing the audio file with in the digital image.LSB technique is being utilized to hide the information which is more effective and basic. Each sample of audio file is being encoded before concealing it digital image which gives secure information exchange with no any third party intervention. And the password is needed for encoding and for security of password CHAP[6] is used.

II. Proposed Method

Many of the techniques are used to embed the data in an image, like changing

DOI: 10.18535/ijecs/v5i6.44

the Most Significant Bit (MSB) of an image, Least Significant Bit (LSB) of image, for embedding the data in an image if we change MSB, there will be some noticeable impact of color of image and hence there will be some amount of difference from the original image and the stego image which forms the drawback and the human eye can easily able to detect that the secret message is present in the image and also leads to the image distortion. And hence the LSB technique is used which is simple and more efficient than the MSB technique. The main advantage of using the LSB technique is it does not result in any image distortion and thus the stego image will look identical as the cover image.

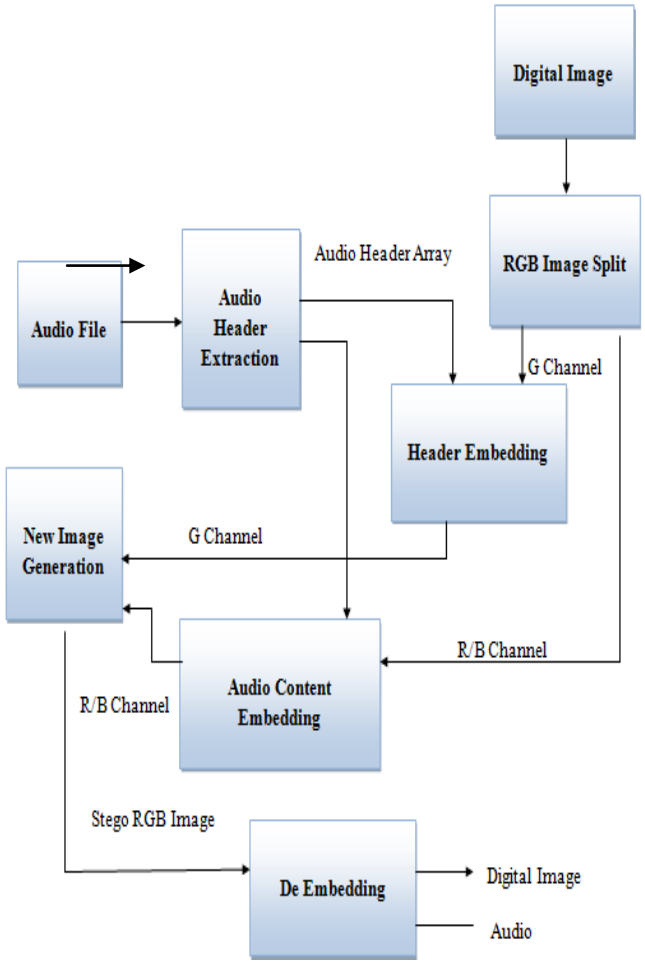

Figure 2 Architecture of the Image stegnography

It contains the some of the following terms like:

Audio File:It is a secret message that is needed to embed into the digital image. .WAV format audio file is used.

Audio Header Extraction: It takes the audio file as input and uses the audio header

array and audio content array for embedding audio and header.

RGB Image Split: It takes cover image that is the digital image as input and RGB channel is used to embed the image content with audio content.

Header Embedding: G channel is used for header embedding for image generation.

Image Generation: After embedding both image and audio content the final new image is being generated .And the output will be the stego image.

De embedding: It takes the stego image as input for de embedding the content.

Above figure shows the architecture diagram of process of embedding and extracting the audio file from the digital image. The audio file is selected first that need to be embedded within digital image. Here the audio file is the secret message and the digital image is the cover file. Digital Image is one which is made of pictures called pixels, and the image resolution is fixed. The contents of audio file are being separated and then converted it into Bit Array. Here .WAV format audio file is taken and then embedded into the digital Image, PNG format digital image are used as each image of PNG has Red, Green and Blue channels. After the audio file converted into Bit Array it is being embedded into digital image bit by bit into least significant bit of green channel and it is not mandatory that green channel of image should be used first even Red and Green channel can also be used. The sound samples of audio file is being taken and then embedded into red and blue channel also. The audio file is encrypted first and then embedded in image, in which dual steganography is used. The Size of audio file should be larger than that of digital image.

After embedding processes is completed it can be sent to the other user. In order to get secret message the user should be having the accurate password as audio file is in encrypted form. And if the third party attacker tries to detect the secret message he is unable to read the message until he gets the password. As password is main source for the third party attacker to read the secret message and hence security of password is needed. For the security of

DOI: 10.18535/ijecs/v5i6.44

password Challenge Handshake Authentication Protocol (CHAP) [6] is used.

CHAP [6] is mainly used for security purpose. Here both the user will be provided with plaintext message which provides a protection against replay attacks. It uses the three way handshake mechanism for the validation. The Cryptanalysis of CHAP is as follows, first the link is being established and the user sends the "challenge" message that is password to peer, and the peer respond by calculating the values using one way hash function. The authentication after performing some own calculation using expected hash value. Hence authenticates the password.

After sending the stego image other user needs to extract the hidden message which is de embedding process, the header fields of audio are being extracted from the secret position of green channel of image which is stored in Bit Array and each Bit Array is converted into bytes to append it into audio file. The secret position of channel should be known for extracting the secret file.

Table 1 Shows the Embedding and Extraction of Image Stegnogrphy

Cover Image name in PNG	Cover Image Size	Audio file name in .WAV	Audio file size	Amount of Data Hidden In Image	Stego Image size	PSNR in db	MSE
Nature	16560 KB	God	2,335 KB	1973 KB	18,533 KB	7.4236	11768.38
Plant	22,967 KB	Sare	3,368 KB	3772 KB	26,739 KB	7.4963	11572.88
Waterlilies	25559 KB	Test	824 KB	374 KB	24,655 KB	7.4878	11595.59
Ballons	25,564 KB	Anthem	3,937 KB	4900 KB	30,464 KB	7.6112	11270.72
Tulips	29,318 KB	Flute	3,799 KB	4694 KB	34,012 KB	7.5685	11382.15

Table 1 demonstrates the embedding and extraction processes of the image steganography. It contains the parameters like cover image which is in PNG format. PNG is the raster positions utilized on the web. PNG format file is used in this article as it as many advantages like it has less compression loss, the quality of image is not being changed, it supports the multiple level of transparency and the main advantage of the PNG format is after resaving the image the quality of image is not lost and next parameter is it contain the cover image size which defines the size of the digital image

other parameter is audio file which is the secret message which is in .WAV format. .WAV is abbreviated as Waveform Audio File which is being used for storing the audio data based on the Resource Interchange File Format(RIFF).The main advantage of using the .WAV file in this article is it has less arrangement and can preserve the audio recording in which storing of the file is not difficult. Next parameter is audio file size which defines the size of the audio file and other one is the amount of data hidden in image and other parameter is the stego image size which contains audio file inside the digital image. Last two parameters are the PSNR and MSE. PSNR is Peak Signal to Noise ratio and MSE is the Mean Square Error. "MSE is being defined as the square of the error between the cover image and stego image" .Error also defines the distortion of an image.

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2$$

Where Xij=Pixel value of Cover image.

Xij=Pixel value of Stego image.

"PSNR is used to measure the quality of an image".The mathematical equation for the PSNR is

$$PSNR = 10 \times \log \frac{255^2}{MSE} \; db$$

From the table we can conclude that the quality of the image is high i.e PSNR so that the human eye cannot suspect that it contains the secret message with in the image and hence it does not lead to any image distortion and it has less mean square error MSE. It ensures high embedding rates moreover keeping up a lot of security.

IV. Conclusion

The article describes a procedure for concealing the secret message that is audio file with in the digital image. The audio file is being scrambled and afterward covered up into the digital image .Least Significant Bit procedure is being utilized to implant the audio file with in digital image. The Sound samples of audio file is taken and then

converted into Bit Array and then embedded into digital image, bit by bit of red, green and blue channel of the image. The password is needed for encryption and decryption of audio file and for security of password CHAP authentication protocol is being used. This procedure additionally gives the safe exchange of information between the two clients, so that the expected hacker or an attacker can't sense the presence of the secret information.

References

[1] Ms. Khushali Pandit, Ms. Varsha Bhosale "Implementation of Location based Steganography on mobile Smartphone using Android Platform" International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, PP 2606-2609.

[2] Chandrakant Badgaiyan, Kaushal Kumar Sinha, "A new steganographic technique: image hiding in mobile application" International Journal of Advanced Computer and Mathematical Sciences, Vol. 3, 2012, PP 556-562

[3] M.I.Khalil, "Image Steganography: Hiding the short audio message within Digital Image", JCS&Z , Vol. 11,2012,PP 68-73.

[4] Savithri G, K.L.Sudha "Android Application for Secret Image Transmission and Reception Using Chaotic Steganography", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, 2014, PP 5107-5113.

[5] Hemang A. Prajapati1, Dr. Nehal G. Chitaliya, Vasad, Anand "Secured and Robust Dual Image Steganography", International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, 2015, PP 30-37.

6] Guy Leduc, "Verification of two versions of the Challenge Handshake Authentication Protocol (CHAP)" 2015.