An Efficient approach to hide audio signals in Cover Image using Key Based Substitution Method

SOMULA SIVA LOVALAKSHMI[1], K.S.RUPA[2]

[1] Student, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam
[2] Assistant Professor, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam

---

Abstract – An efficient approach based Least Significant Bit positioning has been used that overcomes the demerits of the Traditional cryptography techniques like substitution and finally obtain key positioning algorithm and helps to embed the audio in the color image. The audio is embedded in the blue color stream of the 24 bit color image sequentially by the key based LSB positioning algorithm. Here the audio threshold is another major area where we have focused, i.e increasing the size of the audio which can be sent through an image without losing the quality of the audio. This method of hiding the audio through an image helps to authenticate the sender and also to verify whether the data has been really being sent to the valid user or is it being morphed by the attacker in the middle. The proposed algorithm has been tested against various existing algorithm to study how effectively the algorithm is working, and how effectively it is overcoming the drawbacks of the present algorithms. The algorithm is projected to serve the purpose of authenticating the user and also to identify that the message is reaching only the valid user.

Key Words: Least Significant Bit positioning, audio steganography, Image hiding.

1.INTRODUCTION

Steganography is the art of the hiding a message in an image. It has its origin dated in 13th century. In this method, we will be hiding various files such image, audio, video in another files which can be image, or videos files. Steganography provides an add-on advantage of sending the data from under the nose of the attacker. The Steganography techniques utilize the concept of embedding the data rather than encrypting the data. They use a cover file to veil up the data and send it through an insecure network channel. The receiver will receive the file unless he knows what file is being sent and how is it being sent.

The word Steganography is basically combination of two words, namely Steganos (from greek) which means "covered" and Graphy (from english) which means "writing", together we get the word Steganographia (which is in modern latin).The English word steganography is derived from the modern Latin word steganographia. Steganography is the art of concealing messages or information within other non-secret text or data. Steganography can also be defined as the data hidden within the data.

The four main file formats that can be used for steganography are :-

1) Text.
2) Images.
3) Audio/Video.
4) Protocol.

Steganography is an emerging area which is used for secured data transmission over any public media. Steganography is a process that involves hiding a message in an appropriate carrier like image or audio.

Steganography is an ancient technique of concealing the data in any other file and sending it. It has its origins dated back centuries. Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications.(Ref [4])

With the advance of technology, Steganography has increased applications and varied ways of applying the techniques of Steganography. Steganography majorly consists of a cover file that carries the image through an insecure channel called as "Cover Image". Depending on the type of cover image, Steganography has been classified into 4 types. They are:

1. Image
2. Audio/Video
3. Prototype
4. Text

In this work, we have used the concept of Image Steganography.(Ref [3])

2.2 Image Steganography:

Image Steganography deals with the hiding of data within the image. The data can be any file, be it be an image , audio, text or another file. We have to wrap up the data using an image. We have chosen to bind audio data in an image. This kind of embedding an audio in an image helps to authenticate the sender, verify whether valid user is receiving the data or not and to find whether a third party attacker is present in the channel of communication or not.

Since, image is used as a cover file, we have to make sure that the image must be acquaintable for the data that is being embedded. Hence a 24 bit image format proved to be the best solution for hiding the data, since it holds a large memory space and convenient to hide a considerable amount of data. Furthermore, the threshold size of the image must be calculated for the given image size which will be explained in the later parts.

The conditions that the input image must follow are that it must be distinct and of high resolution and must only be available with the sender. It should not be a monotonic pattern of color rather it should be hew of colors which can effectively veil the audio data .

2. LSB Positioning Method

This method is the simplest method of hiding data within the given image. I utilizes the LSB bits of the pixels within the given in the image. When converting an analog image to digital format, we usually choose between three different ways of representing colors:

- **24-bit true color method**: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- **8-bit basic color method**: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.

8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.
LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

The most basic of LSBs insertion for 24-bit pictures inserts 3 bits/pixel. Since every pixel is 24 bits, we can hide

3 hidden_bits/pixel for 24 data_bits/pixel = 1/8 hidden_bits/data_bits

So for this case we hide 1 bit of the embedded message for every 8 bits of the cover image.

But, being the simplest, LSB positioning has its own drawbacks. It is highly vulnerable to noise and the data can be easily corrupted when passing through a noisy channel. This can distort the data and fail the main purpose of Image Steganography.

Thus, to overcome this drawback we have improvised this LSB positioning to a key Based LSB positioning Algorithm, which can withstand the noisy channel and can hide the data effectively both in quality and quantity.

3. RELATED WORK

The proposed algorithm is to hide the audio data effectively in an image without any suspicion of the data being hidden in the image. It is to work against the attacks by using a distinct new image that isn't possible to compare.

The main challenge lies in increasing the amount of audio that can be sent through the image and, how can it be securely sent over the network till the receiver. Also we need to ensure that image will not be giving rise to any suspicion of the data being carried while travelling through the network (hence the condition of being distinct is mandatory).

4. EXISTING WORK

The aim of the paper is to hide the audio in an image using steganography, and ensure that the quality of concealing data must not be lost.

We used a method for hiding the audio in a distinct image file in order to securely send over the network without any suspicion the data being hidden. This process sends audio that can be used as an authentication for the user by the voice sent from the sender. This algorithm though requires a distinct image which we can use as a carrier and hide the audio which is well within the limits of the threshold that the image can hide, that will secure the audio and get the attacker deceived from its true nature. The person will not be able to know until unless he gets to know the intention and the method of hiding, and thus cannot guess the data that is being sent through the image.

Steganography is a technique used to hide a file , a message ,an audio or any other file within another image or file, or an image. This technique doesn't encrypt any data but the data will be hidden within the image and can be only be revealed when the person knows how it is being hidden. This provides an add on advantage of the attacker not suspecting, that the data is actually being hidden in a plain image. The concept masking the vulnerable information with an image and sending it through an insecure channel with a veil actually reduces the chances of attacks on the information. Steganography and Cryptography differ in the concept of embedding and encrypting the data respectively. Cryptography encrypts the very data which is self evident and the attacker can use various known techniques to decrypt the information. Steganography actually embeds the data in

another file and deceives the attacker with a pose of being a plain image.The other techniques which are as good as steganography for hiding the data are Watermarking, Scatter and Encrypt, and Fingerprinting. These technologies are mainly concerned with the protection of intellectual property. But, Steganography differs with the mentioned techniques by hiding the data in another files like image, video, text etc.

Hiding information into a medium requires following elements.

1. The Cover medium (C) that will hold the secret message.

2. The secret message (M)may be plain text, digital image or any type of data.

3. The Steganographic techniques.

5. PROPOSED WORK

5.1 Algorithm:

1. Get a distinct image (16 * 16 bit format image).

2. Convert the image into a binary file with each pixel being specified in terms of its red, green and blue channels.

3. Record an audio within the range of the threshold for the resolution of the image specified.

4. Convert the audio into its binary format.

5. Now place the binary audio data in the place of the channel of each pixel along each row until the data has been completely placed.

6. Now, send this stego-image through the insecure channel.

7. After the receiver receives the data, he must extract the green channel bits from the stego- image.

8. Now the bits are integrated to get the audio back and to authenticate the sender.

5.2 Key Positioning Methodology:

We have used the concept of Least Significant Bit algorithm of the Steganography and have modified it to strengthen the algorithm to overcome its drawbacks. We chose to replace green stream of a 24 bit image and replace the audio in those bit positions.

The following steps are applied for the algorithm:

Step 1: Consider a 16 * 16 bit image as cover image. (Make sure the image is distinct and has a lot of color channels unlike a monotonous image of only a few colors and the colors are well spread)

Step 2: Calculate the size of the image and find the threshold of the audio that can be embedded in that image from the table below.

Step 3: Record an audio of the given size.

Step 4: Convert both the image and audio into their corresponding binary formats. **Step 5 :** Now replace the green channel of the 24 bit image with the audio bits.
Step 6: Send this image through the insecure channel .
Step 7: The receiver will receive the image.

Step 8: The receiver then extracts the green channel and get the audio that has been embedded.

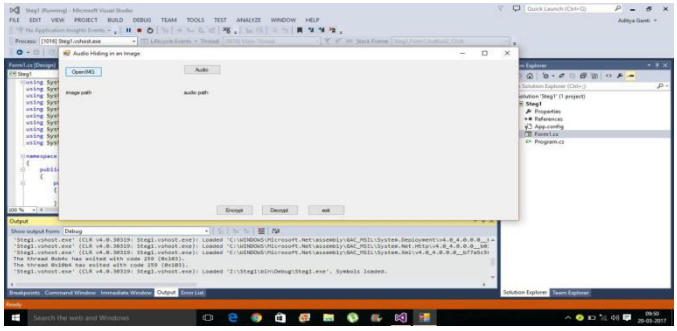
Threshold audio values of various image sizes:

S.No	Size of the image	Threshold audio size
1.	1200*780	245.8kb
2.	980*660	189kb
3.	420*368	48 kb
4.	340*218	34 kb

Table 1: Threshold Values of audio that can be embedded for a given image size

5.3 Calculating the threshold size of an audio for a given Image Size:

Let the size of image be of dimensions p*q. Since it is a 24 bit image, No. of bits in the image are given by : p*q*24.
We are embedding the data of audio only in green channel, which will be of 8 bits . Hence number of such bits that can be replaced are : (p*q*24)/8 = (p*q*3)
This gives the number of bits of audio that can be placed in the given image . To calculate bytes : (p*q*3)/8.
To calculate the size in Kb : (p*q*3)/8*1024.



5.1 Home Page for inserting an audio

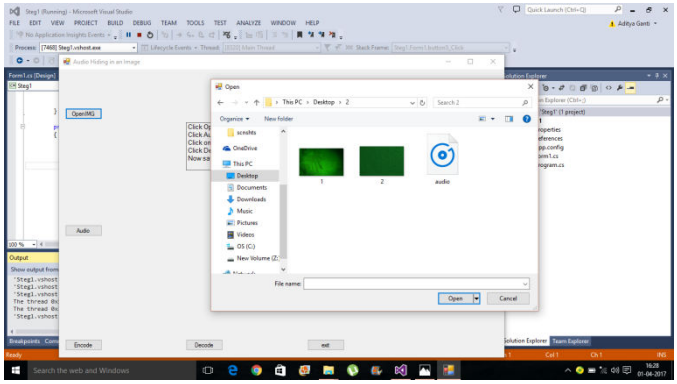


Fig 5.2 Selecting the cover image

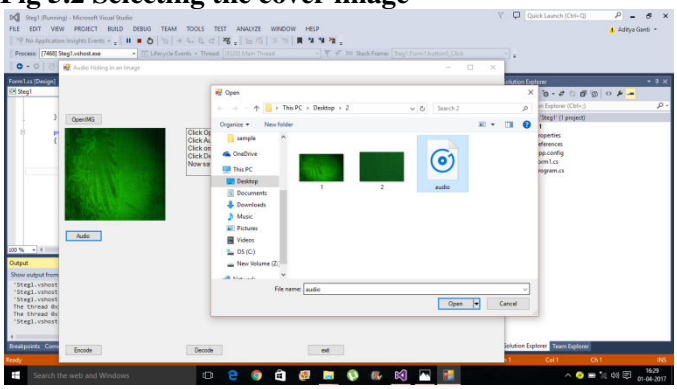


Fig 5.3 Selecting an audio for getting into the image

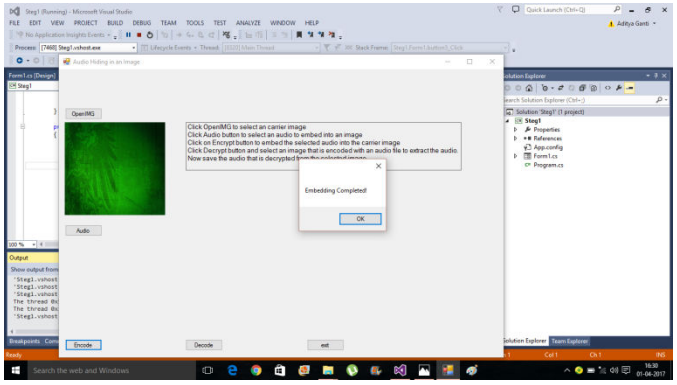


Fig 5.4 Embedding the audio into the Image

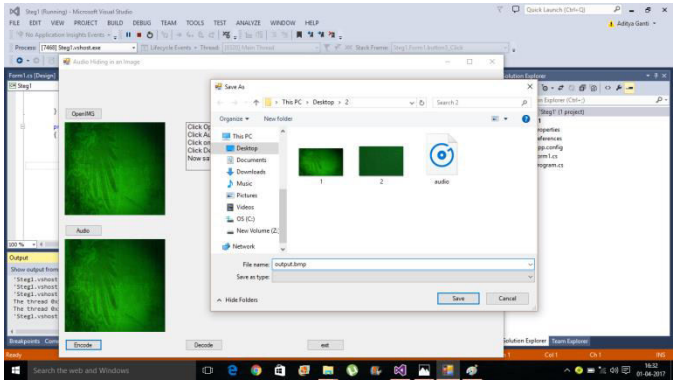


Fig 5.5 Saving the image and audio

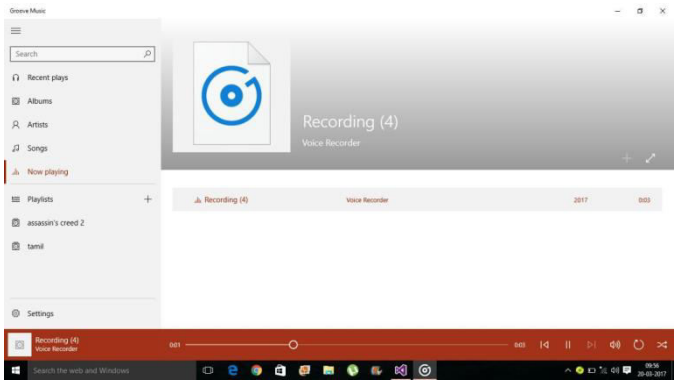


Fig 9: Extracting the audio and playing audio

6. CONCLUSION

This paper addresses the issue of hiding audio in images for the sake of sender authentication that needs to be sent from the sender. This helps to ensure that the data is being received from an authenticated person and only the desired receiver will be getting the actual audio from the receiver. This is done by utilizing the concept of steganography . In this methodology, we have actually hid the audio in an image by converting it into a binary file and embedding it in the green channel of a 24 bit image. This stego-image will be unwrapped and the audio will be detected only if the person knows the size and the places where the audio is hidden. The other important factor is the threshold of the size of the audio that can hidden in various sizes of the image.

The embedding of the audio is done in the green channel of the image. By choosing a distinct and a new image, we can prevent the chance for the attacker to compare and detect the data being hidden. Also since the audio is hidden in the image there will be almost no chances for the attacker to know that the data is being hidden in the image, i.e we can send the audio from under the nose of the attacker without the suspicion of the image being a carrier.

REFERENCES

1. Kamran Ahsan, Deepa Kundur “Practical Data Hiding in TCP/IP”,.

2. Moni Naor and Adi Shamir(1994).“Visual cryptography. in Proceedings of Advances in Cryptology”, EUROCRYPT 94, LNCS Vol. 950, pages 1- 12. Springer - Verlag,.

3. Mr. Vikas Tyagi(2012),.“Data Hiding in Image using least significant bit with cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4,.

4. Neil F. Johnson,(1998).“Exploring Steganography-Seeing the Unseen” , IEEE Computer, February , vol 31, no 2, pp.26-34.

5. Reena Kharat and P.Sanyasi Naidu ,“Secure Authentication in Online Voting

System Using Multiple Image Secret Sharing.

6. R.Poornima1 and .J.Iswarya2, (2013)"An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February.

7. W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb,(2000) "

Applications for data hiding", IBMSystems Journal, 39 (3&4) 547-568.

BIOGRAPHIES

I am K.S. Rupa, M.Tech working as a Assistant Professor –CSE in Avanthi Engineering College, Visakhapatnam. She had 6 years experience in Big Data and Data mining subjects.

This is SOMULA SIVA LOVALAKSHMI, completed B.Tech in computer science and engineering. I am pursuing M.Tech –CSE in Avanthi Engineering College, Visakhapatnam.