MULTIMEDIA INFORMATION HIDING USING STENOGRAPHY

D.Saravanan ,S.Vaithyasubramaniyan,R.Sahayananthini
Department of MCA , Sathyabama University,
Chennai -600112.

ABSTRACT

The least-significant-bit (LSB)-based approach is a popular type of stenographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover audio mainly depends on a pseudorandom number generator without considering the relationship between the audio content itself and the size of the secret message. Thus the smooth flat regions in the cover audios will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those audios with many smooth regions. In this paper, we expand the LSB matching revisited audio stegnography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover audio. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The experimental results evaluated on 6000 natural audios with three specific and four universal steganalytic algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stegno audios at the same time.

Key Terms: Steganography, Audio Data, Encryption, Decryption, Stegno Audios.

1. INTRODUCTION

Steganography is the practice of hitting information .This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer – the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message , hiding its existence in a non-secret file. Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding. In general information are hided inside of Picture, Audio and Video files. The two most common methods are LSB (Least Significant Byte) and Injection.

Multimedia data hiding techniques have developed a strong basis for steganography area with a growing number of applications like digital rights management, covert communications, hiding executables for access control, annotation etc. In all application scenarios given above, multimedia steganography techniques have to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stegno object (object containing secret message) must be perceptually

indiscernible. The second constraint is high data rate of the embedded data.

LSB coding is one of the earliest techniques studied in the information hiding and watermarking area of digital audio (as well as other media types) . The main advantage of the LSB coding method is a high bit rate of hidden bits and a low computational complexity of the algorithm, while the main disadvantage is a low robustness against signal processing alterations. Steganography is a subject which is rarely touched upon by most IT Security Enthusiasts. Most people don't see Steganography has a potential threat, some people don't even know what Steganography is.

2. EXISTING SYSTEM

The files will sent to the destination using stegnography method. Here, we take any area for the data hiding. On the way to more secure steganographic algorithms, the development of attacks is essential to assess security. We present both *visual attacks*, making use of the ability of humans to clearly discern between noise and visual patterns, and *statistical attacks* which are much easier to automate. The visual attacks presented here exemplify that at least EzStego v2.0b3, Jsteg v4, Steganos v1.5, and S-Tools v4.0 suffer from the misassumption that least signi.cant bits of image data are uncorrelated noise. This paper draws together two methodologies for the detection of bit replacement steganography: the principle of maximum likelihood, which is statistically well-founded but has lead to weak detectors in practice, and so-called structural detection, which is sensitive but lacks optimality and can suffer from complicated exposition. The key novelty is to extend structural analysis to include a hypothetical "pre-cover", from which the cover object is imagined to derive. Experiments show that the new detectors are the best performers yet, very significantly so in the detection of replacement of multiple bit planes. We consider the problem of detecting spatial domain least significant bit (LSB) matching steganography in grayscale images, which has proved much harder than for its counterpart, LSB replacement. We use the *histogram characteristic function* (HCF), introduced by Harmsen for the detection of steganography in color images but ineffective on grayscale images.

In this paper, we investigate the calibration technique used in stegnoanalysis of LSB matching. Instead of working on the original image, we propose to calculate the calibration-based detectors (e.g. Calibrated HCF COM) on the difference image,

which is defined as the difference of the adjacent pixels of an image. The theoretical reliability of the new detectors is carefully studied. The extensive experimental results clearly illustrate that the new detectors outperform the previous. Indeed, the new ones perform well even when the embedding rate is low.

3. ISSUES IN THE EXISTING SYSTEM

- The area selected for the data hiding may be not enough. So, the data can come outside the selected area.
- The information for hiding will not be placed exactly in the area.
- There will be a difference in the stegno information and normal information.
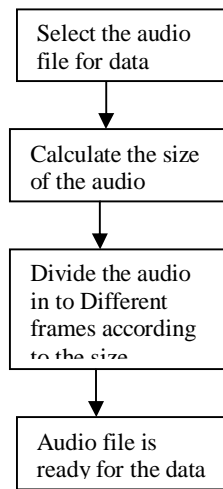
4. RELATED WORK

Steganography is no routine means to protect confidentiality. Normally, cryptography is used to communicate confidentially. Cryptographic algorithms—the security of which can be proven or traced back to known hard mathematical problems—are widely available. However, in contrast to steganography, cryptographic algorithms generate messages which are recognizable as encrypted messages, although their content remains confidential. Steganography1 embeds a confidential message into another, more extensive message which serves as a carrier. The goal is to modify the carrier in an imperceptible way only, so that it reveals nothing—neither the embedding of a message nor the embedded message itself.

5. FUNCTION OF EXISTING SYSTEMS

5.1 Selection of stegano object
5.2 Applying Cryptography
5.3 Data Embedded in waves
5.4 Extracting of information

5.1 Selection of Stegano Object With frames

The information should be hidden in the audio and it becomes a stegano audio. So the audio for information is to be selected. There should not be any difference between the audio and stegano audio. The Audio file which is going to be used for the data hiding is divided into frames or bytes for the fixation of the data.

```
┌─────────────────┐
│ Select the audio │
│ file for data    │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Calculate the size │
│ of the audio     │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Divide the audio │
│ in to Different  │
│ frames according │
│ to the size      │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Audio file is    │
│ ready for the data │
└─────────────────┘
```
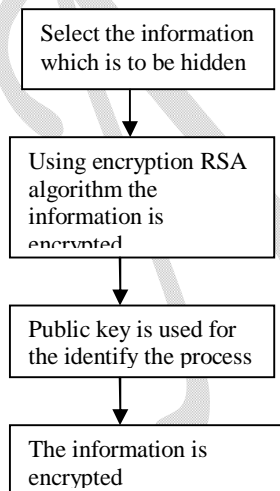
5.2 Applying Cryptography

The information is selected for data hiding and it is to be sent in the encrypted manner using cryptography Technique. This is done for the safe transaction of the information. Cryptography uses two keys for encrypting and decrypting the information.

5.2.1 PRIVATE KEY:

It is the key for the use for decrypting purpose. This key should be unique to the person.
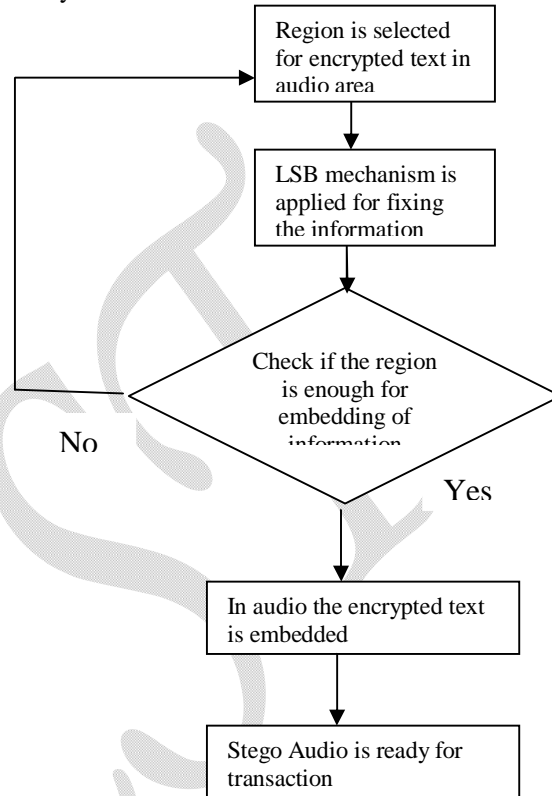
5.2.2 PUBLIC KEY:

This is the key is used for the purpose of encrypting the information and it is used by the users in a group only.

```
┌─────────────────┐
│ Select the information │
│ which is to be hidden │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Using encryption RSA │
│ algorithm the    │
│ information is   │
│ encrypted        │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Public key is used for │
│ the identify the process │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ The information is │
│ encrypted        │
└─────────────────┘
```
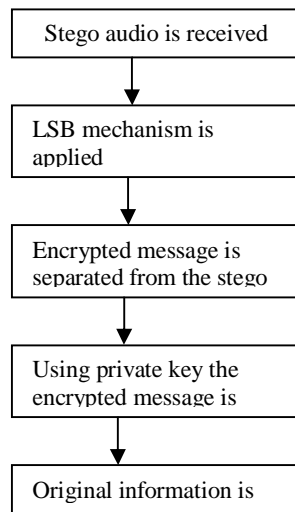
5.3 Data embedded in wave

Here, the encrypted data is embedded with the audio file. The region is selected for the encrypted text. Then LSB mechanism is applied for fixing the information with in the frames. If the region is not enough for the information again there will be a process of region selection. Now the encrypted file is embedded with the stegano file. Stegano audio is ready for the transaction

```
┌─────────────────┐
│ Region is selected │
│ for encrypted text in │
│ audio area       │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ LSB mechanism is │
│ applied for fixing │
│ the information  │
└─────────────────┘
         │
         ▼
       ◇ Check if the region
         is enough for
         embedding of
         information
   No ◄──┘        └──► Yes
         │
         ▼
┌─────────────────┐
│ In audio the encrypted text │
│ is embedded      │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Stego Audio is ready for │
│ transaction      │
└─────────────────┘
```

5.4 Extraction of in formations

The information is sent to the destination. Now the decryption process is done. By receiving the stegno audio, again LSB mechanism is applied for separating the encrypted text from the audio file. Using private key the information is decrypted and the Original text will be extracted

```
┌─────────────────────────┐
│ Stego audio is received │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│ LSB mechanism is        │
│ applied                 │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│ Encrypted message is    │
│ separated from the stego│
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│ Using private key the   │
│ encrypted message is    │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│ Original information is  │
└─────────────────────────┘
```

6. IMPLEMENTATION

The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover audio mainly depends on a pseudorandom number generator without considering the relationship between the audio content itself and the size of the secret message. Thus the smooth/flat regions in the cover audios will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those audios with many smooth regions. In this paper, we expand the LSB matching revisited audio steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover audio. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The experimental results evaluated on 6000 natural audios with three specific and four universal steganalytic algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stegano audios at the same time.
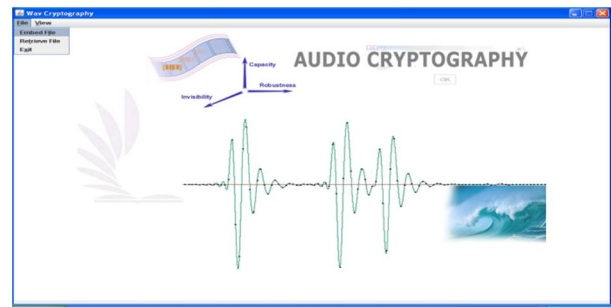
Experimental Results:
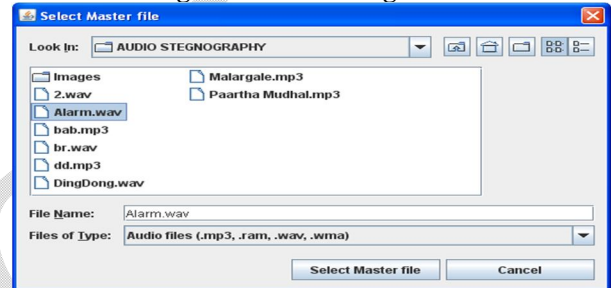

Figure 1: Embedding file
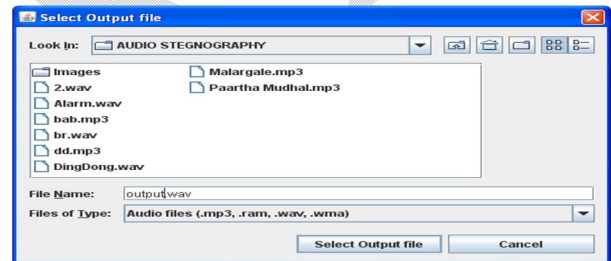

Figure 2: selection of master file
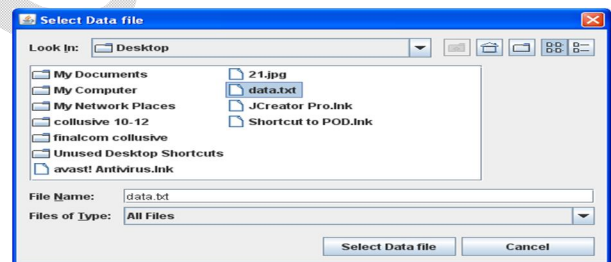

Figure 3: Selecting output file
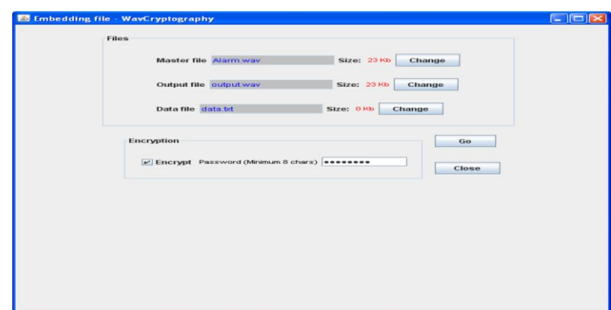

Figure 4: selecting of data file
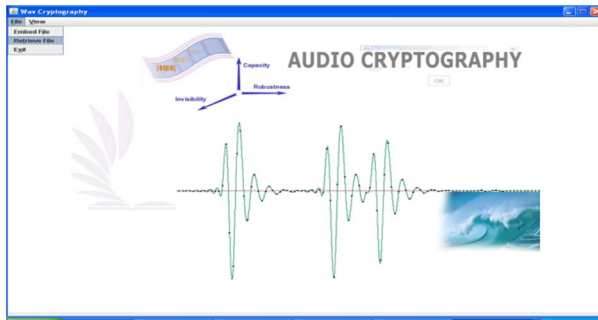

Figure 5: Encrypting the file
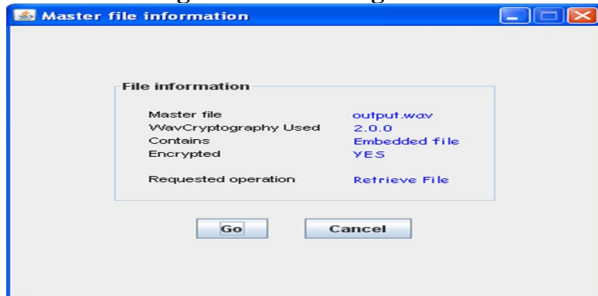
Figure 7: Retrieving file

Figure 9: Details of stego audio

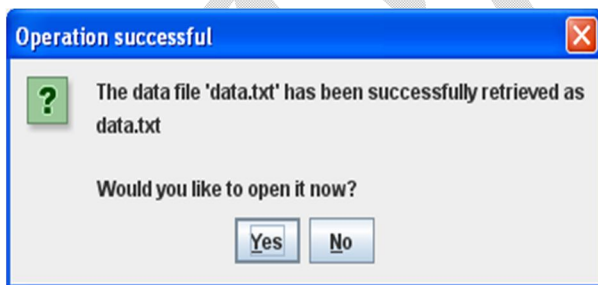**Figure 10: entering password to decrypt**
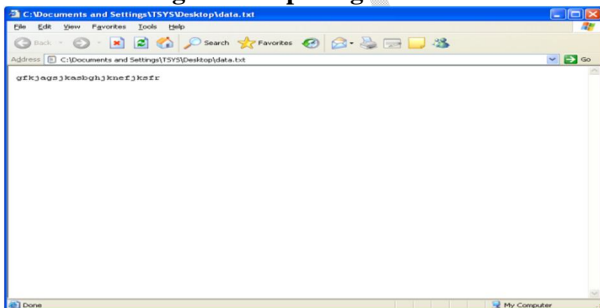

Figure 11: opening of the file

Figure 12: received final output

7. CONCLUSION

This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust.

In this paper, an edge adaptive audio steganographic scheme in the spatial LSB domain is studied. There usually exist some smooth regions in natural audios, which would cause the LSB of cover audios not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stegano audios becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover audios, we have proposed a novel scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. The experimental results evaluated on thousands of natural audios using different kinds of steganalytic algorithms show that both audio quality and security of our stegano audios are improved significantly compared to typical LSB-based approaches and their edge adaptive versions.

8. FUTURE ENHANCEMENT

- First of all, testing on a large public dataset will be conducted for deeper understanding of the proposed approaches.
- Basically, we are embedding the information. As an enhancement we are taking an audio file as waves for embedding the information.

- The important tool provided in our project is steganography that provides the user to send the private messages by hiding it into any image, audio, video files. To increase its

efficiency, reliability, performance we can implement it on the bit level, this will not affect the entities of the files so as to increase the performance by preserving the entities of the files up to some extent.

REFERENCES

[1]Andreas Westfeld and Andreas P.tzmann " Attacks on Steganographic SystemsBreaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned "

[2] Andrew D. Ker "A Fusion of Maximum Likelihood and Structural Steganalysis"

[3]Andrew D. Ker "Steganalysis of LSB Matching in Grayscale Images",2005.

[4]Xiaolong Li, Tieyong Zeng, Bin Yang "Detecting LSB Matching by Applying Calibration Technique for Difference Image"

[5]Mehdi Kharrazi , Husrev T. Sencar , Nasir Memon "Cover selection for steganographic embedding"

[6]R.Sridevi, Dr. A. Damodaram , Dr.Narasimham " Efficient Mehthod of Audio Steganography By modified LSB Algorithm and Strong Encrypiton"2005.

[7] **Zameer Fatima1** and **Tarun Khanna" Audio Steganography Using DES Algorithm",** Proceedings of the 5th National Conference; INDIACom-2011, Pages 01-03.