An Efficient Higher LSB Method for Hiding Encrypted Data into Audio and Video Frames of AVI Video Carrier

Renu R. Dandge  
Department of Computer Science  
S.G.B.A.U. Amravati (MS)  
Amravati (MS)

V.M. Thakare, PhD  
Department of Computer Science  
S.G.B.A.U. Amravati (MS)  
Amravati (MS)

ABSTRACT

Steganography can be applied in various domains using mobile and devices especially mobile phones. Since ancient days of technology, communication was and is still one of the novel techniques of data security. One of the many ways of implementing a secure communication on mobile devices is using a method to hide information. The domain that represents this concept is steganography which focuses on hiding specific messages using specialized techniques in such a way that only the sender and the intended receiver are able to decipher it. This paper focuses on hiding maximum data in carrier video (AVI) with minimum quantization error by applying higher LSB method and increasing the data secrecy level.

General Terms

Security, Algorithm.

Keywords

Higher LSB, Data Hiding, Extraction, Mean Square Error, AVI Video.

1. INTRODUCTION

Since ancient days of technology, communication was and is still one of the novel techniques of data security. The confidentiality, integrity and authenticity of data are of great importance whenever communication takes place over a network and computer security rests on these three concepts. Due to various critical aspects, sensitivity of the security facts and issues in the field of information security, methods like cryptography and steganography have been invented and used. The process of converting the plaintext into ciphertext is termed as enciphering and the reverse process is termed as deciphering. Many schemes involved for performing the techniques used for deciphering a message without any knowledge of enciphering details fall into the study of cryptanalysis encryption constitutes the area study called as cryptography. The areas of cryptography and cryptanalysis together are called as cryptology. However, application of cryptography gives the idea about the awareness of a secret cipher. Therefore to deal with such a problem one can place the secret information in such a way that users do not come to know that something is hidden, and due to this fact the secrecy is achieved. This can be achieved through steganography. Steganography is the phenomenon of hiding any message in unsuspected multimedia data and is used in secret communication between known parties. The information security problems over the Internet can be addressed by Cryptography and Steganography. A novel Video Steganography can hide an uncompressed secret video stream in a host video stream with almost the same size. A plaintext message may be hidden in one of the two ways. The methods of steganography conceal the existence of message whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. Steganography involves hiding information so it appears that no information is hidden at all. The most common way of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password. A steganographic technique should not be easily detectable and if the corresponding steganographic technique fails to achieve then it is considered to be invalid. Similar to cryptography, steganography may also suffer and can be attacked and that method is called as steganalysis. Steganalysis is nowadays becoming the highlighted research area in the field of information security which focuses on exposing the presence of the hidden data in cover object [6-7]. One of the methods is based on the concept of blind steganalysis. The classifier should be trained to learn the differences between cover and stego-image feature.

2. LITERATURE SURVEY

Due to various critical aspects, sensitivity of the security facts and issues in the field of information security. The computer and network security is becoming both fascinating and complex. Mobility now a days has become the working and researching aspect and due to the need of this the secure transmission of data and sensitive information over internet comes into interest. Three types of steganographic algorithms proposed are: algorithms based on the LSB method, algorithms based on the YUV method and algorithms based on the Karhunen-Loeve Transform (KLT) are proposed. The algorithms based on the LSB method usually operate by hiding the most significant bits of the secret message image pixels within the least significant bits of the carrier image pixels. The YUV method is mainly based on the LSB method. Before applying a LSB based algorithm the images are converted from the RGB format to the YUV format. A Karhunen-Loeve Transform (KLT) based algorithm also uses LSB based algorithms. In the algorithms based on the LSB method the most significant bits of the secret message in image pixels are hidden within the least significant bits of the carrier image pixels. Tests and comparisons were made using 3 hosts: ARM7 based microcontroller, a multi-core architecture digital signal processor and a personal computer. LSB method based algorithm on the three platforms mentioned above using different sets of images of different sizes. Thus it concluded that the execution time of a steganographic algorithm is highly influenced by the size of the carrier image [1]. Medical imaging is an important and vital aid in diagnostic and management decisions. A watermarking method is proposed for medical images based on the least significant bits (LSBs). The methodology proposed involves data insertion and detection. The techniques used are:-

1) Harris Corner Detector: To detect differences pixels carry the message to be inserted.
2) The Error Correcting Code “TurboCode”: To contribute to the data confidentiality, data
Steganalysis is the art of detecting the presence of the hidden message. Thus one can apply hidden information with more space better than other steganography media [4]. The steganalysis is an art of covert signal detection of hidden message, has gained much attention in the field of information security. It is easy to hide message into video and send it the intended recipient by uploading it to social networking and media sharing websites e.g. YouTube. Here an adaptive SS embedding method on 4 × 4 block is considered. This adaptive SS embedding scheme is robust to H.264 compression. Due to the good decorrelation ability of 3D DCT, it has widely been used for image compression, video compression, video denoising and so on. The proposed scheme uses 3D DCT transform to capture traces of message temporal-correlation from the YouTube video [5]. Based on the H.264/AVC Video coding standard, a new video steganography algorithm is proposed and realized. The algorithm designed a motion vector component feature to control embedding and also to be the secret carrier. The proposed methodologies are as follows: 1) Analysis of Original Steganography Algorithm Based on Motion Vector Components. 2) Improved Steganography Algorithm Based on Motion Vector Components Differences.

3) Visual Invisibility. The proposed algorithm is tested on a PC (1.8 GHz Core2 320 CPU, 1.0 GB RAM). Thus a video steganography algorithm used is based on motion vector components differences. This algorithm obtains higher carrier utilization and embedding efficiency, and also has large embedding capacity with good visual invisibility and statistical invisibility [6]. The proposed framework for CVSS consists of four function parts: the video sequence parser, the scene change detector, the secret message embedded and the video steganalysis. Thus one new secure and file-size preserving compressed domain steganography is proposed [7]. Steganalysis is the art of detecting the presence of the hidden information transmitted through the cover object. The method includes the secret message to be hidden by a slight modification of the motion vectors. Subsequently, some improved algorithms about the steganographic scheme in motion vectors were proposed. A feature based algorithm is proposed and the support vector machine (SVM) classifier is utilized to determine the existence of hidden message. The proposed steganalysis scheme analyses the altered statistical characteristics introduced by the embedding process from both the spatial and temporal domain and employing the SVM as a discriminator can detect the presence or absence of the hidden message [8]. Lossless steganography techniques are used in which messages can be sent and received securely. The advantage of using video files in hiding information is the added security against hacker attacks due to the relative complexity of video compared to image files. Here two steps are followed Embedding Stage and Extraction Stage. Steganography is characterized mainly by two aspects; imperceptibility and capacity. The Proposed algorithm was implemented using MATLAB. The proposed model is more secure against attacks because it depends on a list of security parameters. These security parameters are the novel algorithm to extract the message from the video file, the number of the embedded LSB bits, the selected transform domain, and the stego key data [9].

3. PROPOSED METHODOLOGIES
The proposed methodologies include two main steps: first is to hide information in images and in audio and then on the other side extract the secret data. The algorithms for data hiding and extracting are proposed as follows.

Proposed Algorithm (Data Hiding):
1. Select AVI Video
2. Check AVI header.
3. If AVI is uncompressed then go to step 4 else go to step 9.
4. Separate Frames and Audio from AVI Video.
5. Hide Secret Data using higher LSB bits Algorithm in Frames and Audio.
6. Create Video from Stego Frames.
7. Insert Sound into Created Video.
8. Play stego video.
9. Stop.

Proposed Algorithm (Data Extraction):
1. Select Stego AVI video
2. Check it’s Header
3. If AVI is uncompressed then go to step 4 else go to step 7
4. Separate Frames and audio from AVI video.
5. Extract hidden Data from Frames and audio.
6. Decrypt data
7. Stop.

Higher LSB method for data embedding will be implemented. This new method for data hiding will be proposed that achieves high data hiding capacity along with greater robustness. An individual pixel is represented with 24 Bits in RGB format as shown

Proposed Higher LSB Algorithm
Step 1: Select Pixels.
Step 3: if ((R + 32) > 255) || (R-32) < 0), (G + 32) > 255) || (G-
32)<0, ((B + 32)>255) ||((B-32)<0), then discard pixel components else replace its 5 LSB side bits with data bits.

Step 4: Repeat step 2 to 3 until all guard pixel region not scanned.

Step 5: Stop

Data Hiding in Audio Wave fileA new method can be proposed that is able to hide data in audio using the fourth LSB layer, which uses a two-step approach. In the first step, a data bit is embedded into the ith LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by data embedding is shaped in order to change its white noise properties. The standard LSB coding method simply replaces the original host audio bit in the ith layer (i=1... 16) with the bit from the data bit stream.

Fig. 1: 4th bit LSB replacement algorithm

4. RESULT ANALYSIS

Image steganography results

Fig 2: Input image

Table 1. Modified LSB audio stegno Method

<table>
<thead>
<tr>
<th>Hiding method/music</th>
<th>Country</th>
<th>Violin</th>
<th>Pop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrimination value(%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard algorithm(3 LSBs)</td>
<td>52</td>
<td>53</td>
<td>48</td>
</tr>
<tr>
<td>Standard algorithm(3 LSBs)</td>
<td>55</td>
<td>70</td>
<td>67</td>
</tr>
<tr>
<td>New algorithm(3 LSBs)</td>
<td>51</td>
<td>48</td>
<td>49</td>
</tr>
<tr>
<td>New algorithm(4 LSBs)</td>
<td>53</td>
<td>46</td>
<td>53</td>
</tr>
<tr>
<td>Mean Opinion Score(MOS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard algorithm(3 LSBs)</td>
<td>5.0</td>
<td>4.9</td>
<td>5.0</td>
</tr>
<tr>
<td>Standard algorithm(3 LSBs)</td>
<td>4.2</td>
<td>3.5</td>
<td>4.0</td>
</tr>
<tr>
<td>New algorithm(3 LSBs)</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
</tr>
<tr>
<td>New algorithm(4 LSBs)</td>
<td>5.0</td>
<td>4.8</td>
<td>5.0</td>
</tr>
</tbody>
</table>

Table 2. Resultant audio samples after embeding data bit into 4th LSB & flipping

<table>
<thead>
<tr>
<th>Audio Stream</th>
<th>Original</th>
<th>Resultant</th>
<th>Databit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1011011011011111</td>
<td>0000000110110111000</td>
<td>0000000110110111000</td>
<td>1</td>
</tr>
<tr>
<td>01010100010100001</td>
<td>01010100010100001</td>
<td>01010100010100001</td>
<td>0</td>
</tr>
<tr>
<td>00000011100100000</td>
<td>00000011100100000</td>
<td>00000011100100000</td>
<td>0</td>
</tr>
<tr>
<td>01000100011001110</td>
<td>01000100011001110</td>
<td>01000100011001110</td>
<td>1</td>
</tr>
<tr>
<td>0001110101011010</td>
<td>0001110101011010</td>
<td>0001110101011111</td>
<td>1</td>
</tr>
<tr>
<td>00000000110000011</td>
<td>00000000110000011</td>
<td>00000000110000011</td>
<td>0</td>
</tr>
<tr>
<td>10111100101011011</td>
<td>10111100101011011</td>
<td>10111100101011011</td>
<td>1</td>
</tr>
</tbody>
</table>
5. CONCLUSION
After implementing the proposed method the aim which is to increase the data hiding capacity without affecting the quality of image will be achieved. The resultant stego image in which the secret data is embedded will be obtained. This resultant image will appear to be same as input image. Through proposed method, quantization error of 32 bit occurs which may affect image intensity but preserves it’s quality. Also the 4th LSB method implemented in audio will increase the depth of data embedding without affecting the transparency of audio signal. The steganalysis of the proposed algorithm will be challenging since bits flipping will take place and hence any intruder will not be able to identify the hidden data.

6. FUTURE SCOPE
To improve the data hiding capacity even more, the future work includes modifying and implementing 6th LSB method. Thus ultimately increasing the depth of hiding the secret data in required video and send it securely to intended party.

7. ACKNOWLEDGMENT
I sincerely thank my guide Dr.V.M. Thakre for guiding me throughout my research work and project. I would also like to thank him for his valuable time and knowledge he gave me to accomplish my project.

8. REFERENCES


