

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. The 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 problem one can place the secret information in such a way that users does 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 method 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 "Turbo code": To contribute to the data confidentiality, data

verification and eventually error correction. (3) Cryptographic Hash Function SHA-1: To generate the hospital center signature and verify the integrity of the received medical image. Thus here the delicate watermarking is inserted whose objectives are to verify the integrity of the medical image and preserve the confidentiality of patient data. [2]. The security problems of various data communication via Internet can be addressed by Cryptography and Steganography. The proposed technique is the time-domain method which tries to get a larger data-hiding capacity without causing any kind of distortion in the host video stream. Therefore a video stream can be embedded into the host video stream after encoding the secret video by applying the non-uniform rectangular partition. Thus a novel secure large-capacity uncompressed video steganography algorithm has been proposed which is based on image steganography algorithm. Experimental results show that there is no major visual distortion happening in host video stream while the quality of the reconstructed video stream is also not showing any major difference and is acceptable for the practical use [3]. As discussed steganography conceal the existence of message by hiding private or sensitive data or information within something that appears to be nothing. A proposed system program is able to hide data in digital video files i.e. in the images or frames which are extracted from the digital video file (like AVI files). And each extracted frame is said to be an image. The suggested algorithm is based on LSB (Least significant bit insertion) method. By using the algorithm the result that we obtain on instant images show that it can reach saving up to 33.3% of the image for data hiding; which is considered as an enhancement for LSB method (12% of the image). Thus with this technique, 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 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 :- 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 (1.8GHz Core26320 CPU, 1.0GB 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.

Algorithm (Data Hiding):

- Select AVI Video
- Check AVI header.
- If AVI is uncompressed then go to step 4 else go to step 9.
- Separate Frames and Audio from AVI Video.
- Hide Secret Data using higher LSB bits Algorithm in Frames and Audio.
- Create Video from Stego Frames.
- Insert Sound into Created Video.
- Play stego video.
- Stop

Proposed Algorithm (Data Extraction):

- Select Stego AVI video
- Check it's Header
- If AVI is uncompressed, then go to step 4 else go to step 7
- Separate Frames and audio from AVI video.
- Extract hidden Data from Frames and audio.
- Decrypt data
- 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

Step1: Select Pixels.

Step 2: Select R, G, B components.

Step 3: if $((R + 32) > 255) \parallel ((R - 32) < 0), ((G + 32) > 255) \parallel ((G -$

$32) < 0$, $((B + 32) > 255) \parallel (B - 32) < 0$, 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 file A 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 i th 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 i th layer ($i=1 \dots 16$) with the bit from the data bit stream.

```

if host sample a > 0
  if bit 0 is to be embedded
    if ai-1 = 0 then ai-1 ai-2 ... a0 = 11...1
    if ai-1 = 1 then ai-1 ai-2 ... a0 = 00...0 and
      if ai+1 = 0 then ai+1 = 1
      else if ai+2 = 0 then ai+2 = 1
      ....
      else if ai5 = 0 then ai5 = 1
    else if bit 1 is to be embedded
      if ai-1 = 1 then ai-1 ai-2 ... a0 = 00...0
      if ai-1 = 0 then ai-1 ai-2 ... a0 = 11...1 and
        if ai+1 = 1 then ai+1 = 0
        else if ai+2 = 1 then ai+2 = 0
        ....
        else if ai5 = 1 then ai5 = 0
      else if bit 1 is to be embedded
if host sample a < 0
  if bit 0 is to be embedded
    if ai-1 = 0 then ai-1 ai-2 ... a0 = 11...1
    if ai-1 = 1 then ai-1 ai-2 ... a0 = 00...0 and
      if ai+1 = 0 then ai+1 = 1
      else if ai+2 = 0 then ai+2 = 1
      ....
      else if ai5 = 0 then ai5 = 1
    else if bit 1 is to be embedded
      if ai-1 = 1 then ai-1 ai-2 ... a0 = 00...0
      if ai-1 = 0 then ai-1 ai-2 ... a0 = 11...1 and
        if ai+1 = 1 then ai+1 = 0
        else if ai+2 = 1 then ai+2 = 0
        ....
        else if ai5 = 1 then ai5 = 0
      else if bit 1 is to be embedded

```

Fig. 1: 4th bit LSB replacement algorithm

4. RESULT ANALYSIS

Image steganography results



Fig 2: Input image

Mean Intensity of Original Image1=0,
Entropy of an Original Image1=0,
Mean Intensity of Enhance Image1=0,
Entropy of an Enhance Image1=0
PSNR of Image1=Inf
Mean Intensity of Original Image2=0,
Entropy of an Original Image2=0,
Mean Intensity of Enhance Image2=0,
Entropy of an Enhance Image2=0
PSNR of Image2=Inf
Mean Intensity of Original Image3=0.36863,
Entropy of an Original Image3=0.59415,

Fig 3: Video Steganography Result showing parameters involved

Table 1. Modified LSB audio stegno Method

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

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

Audio Stream		
1011011011011111		
Original	Resultant	Databit
0000000110111000	0000000110111000	1
0101010001010001	0101010001010001	0
0000001110010000	0000001110010000	0
0100010001100110	0100010001101000	1
0001110100110010	0001110100111111	1
0000000011000011	0000000011000011	0
1011110010101101	1011110010101101	1

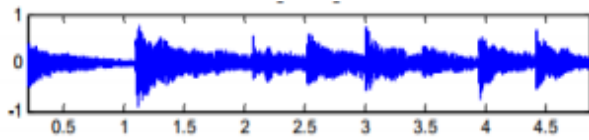


Fig 4: Original Audio Wave

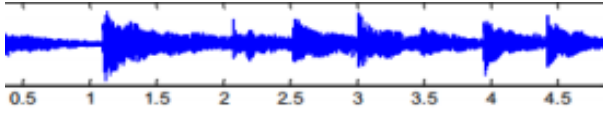


Fig 5: Result Audios stego wave

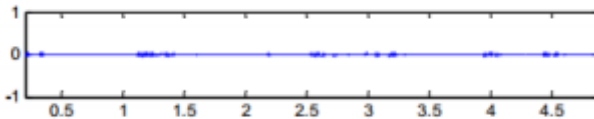


Fig 6: Difference Audio Signal

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 its 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

- [1] Daniela Stanescu,ValentinStangaciu, MirceaStratulat "Steganography on new generation of mobile phones with image and video processing abilities"(ICCC-CONTI 2010) Timisora, Romania.IEEE International Joint Conferences on Computational Cybernetics and Technical Informatics, 978-1-4244-7433-2/10, May 27-29, 2010
- [2] MohamedAliHAJJAJI ,AbdellatifMTIBAA , El-beyBOURENNANE "A Watermarking of MedicalImage: Method Based "LSB" Journal of Emerging Trends in Computing and Information Sciences", ©2009-2011 CIS Journal, VOL.2, NO.12, PP 714-721, December2011
- [3] ShengDunHu,KinTak U," A Novel Video Steganography based on Non-uniformRectangularPartition" The 14th IEEE International Conference on Computational Science and Engineering, 978-0-7695-4477-9/11, PP: - 57 – 61, 2011
- [4] Mohamed ElsadigEltahir, MissLaiha Mat Kiah , Bilal BahaaZaidan ,AosAlaaZaidan," HighRateVideo Streaming Steganography" IEEE, International Conference on Future Computer and Communication, 978-0-7695-3591-3/09, PP: - 672-674, 2009
- [5] HongZhao Hongxia Wang, Hafiz Malik,"Steganalysis Of Youtube Compressed Video Using High-Order Statistics In 3d DctDomain",EighthInternationalConferenceon IntelligentInformationHiding and MultimediaSignalProcessing, 978-0-7695-4712-1/12, PP:- 192-194, 2012
- [6] WANGJue, ZHANGMin,SUN Juan-li," Video Steganography Using Motion Vector Components"2011 IEEE, 978-1-61284-486-2/11, 2011
- [7] Bin Liu,Fenlin Liu,Chunfang Yang andYifeng Sun Zhengzhou," Secure Steganography in Compressed Video Bitstreams",The Third International Conference on Availability, Reliability and Security, 0-7695-3102-4/08, PP: - 1382-1389, 2008
- [8] ChengqianZhang,Yuting Su,ChuntianZhang,"A New Video Steganalysis Algorithm against Motion Vector Steganography",National High Technology Research and Development Program of China(NO. 2006AA01Z407), 978-1-4244-2108-4/08 2008 IEEE, PP 1-5, 2008
- [9] Amr A. Hanafy,Gouda I. Salama and Yahya Z. Mohasseb,"A Secure Covert Communication Model Based On Video Steganography" ,2008 IEEE,978-1-4244-2677-5/08, PP:- 1-6, 2008
- [10] VivekSampat, Kapil Dav, JigarMadia," A Novel Video Steganography Technique using Dynamic Cover Generation" National Conference on Advancement of technologies-Information System & Computer Networks, PP 26-29, 2012
- [11] PadmashreeG,Venugopal P S,"Audio Steganography and cryptography: using LSB algorithm at 4th and 5th LSB layers" ,International journal of Engineering and Innovative Technology(IJEIT),VOL.2, Issue 4 , PP 177-181,October 2012
- [12] Y. J. Dai., L. H. Zhang and Y. X. Yang.: "A New Method of MPEG Video Steganographying Technology". International Conference on Communication Technology Proceedings (ICCT), 2003.