International Journal of Advances in Applied Sciences (IJAAS)
Vol. 4, No. 2, June 2015, pp. 66~72
ISSN: 2252-8814

Audio Encryption and Digital Image Watermarking in an Uncompress Video

Amit Dengre*, A. D. Gawande**
* Information Technology, Sipna COET, Amravati, India
** Department of Computer Science & Engineering, Sipna COET, Amravati, India

Article Info

Article history:

Received March 20, 2015
Revised May 17, 2015
Accepted May 28, 2015

Keyword:

Digital image watermarking
Ratio analysis
Security analysis
Singular value decomposition
Watermark embedding algorithm
Watermark extracting algorithm

ABSTRACT

The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size. Enhanced Audio Steganography (EAS) is one proposed system which is based on audio Steganography and cryptography & watermarking, ensures secure data transfer between the source and destination.

Corresponding Author:

Amit Dengre,
Information Technology,
Sipna COET,
Amravati.
Email: amit_dengre@rediffmail.com

1. INTRODUCTION

Steganography is the practice of hiding information "in plain sight". 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 by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence1.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. There are numerous methods used to hide information inside of Picture, Audio and Video files. The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial.

Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it. There are many to embed information into a popular media using steganography. A good example of this is the relationship between a recoded song, and its lyrics. The audio file containing the recording is much larger than the song lyrics stored as a plain ASCII files. Therefore it is probably safe to assume that the smaller file could be steganographically embedded into the larger one without impacting the quality.

Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices especially mobile phones. In this project we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. The LSB method used for this project which satisfies the requirement of steganogaphy protocols. This research will include implementation of steganographic algorithm for encoding data inside video files, as well as technique to dynamically extract that data as original.

2. LITERATURE REVIEW

For studying the concepts of video steganography, we have surveyed many latest papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography. These papers were very important to us for studying the basic concept Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas [2], the main requirements of any data hiding system are security, capacity and robustness It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image. Ahmed Ch. Shakir [1], the confidential communications over public networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security.

To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital color bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information. Andreas Westfield and Gritta Wolf [3], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding.

In this algorithm security is established by indeterminism within the signal path. Sherly A P and Amritha P [14], in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hidden compressed domain. The data are embedded in the macro blocks of I, P frames and in B frames. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed videos without degradation in visual quality. Saurabh Singh and Gaurav Agarwal [13], have presented a novel approach of hiding image in a video. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So It is very difficult to find that image is hidden in the video of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the video.

The intruder requires full video to unhide image. Authors have described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely. S.Suma Christal Mary [12], have proposed new Real time Compressed video secure Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity. At present we are hiding the data in video format, so in the future implementation of uncompressed formats may possible as well, so it may support MPEG4 format [16]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

3. PROPOSED ALGORITHM

The existing systems lack good user interface, non provision of choosing the key and more encode-decode time consumption. There are lots of steganographic programs available. A few of them are excellent in every respect; unfortunately, most of them lack usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems. The proposed application will take into account these shortcomings, and since it will be written in Java, operability over multiple operating systems and even over different hardware platforms would not be an issue. This proposed stego machine provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. The proposed algorithm, both for encoding and decoding along with application are given in this section. Encoding technique and decoding technique is given.

3.1. Steps of Proposed System (Data Hiding)

1. Select input AVI video.
2. Check for uncompressed format of an AVI video
3. If input video is uncompressed, extract frames & audio from video.
4. Select extracted audio wave file & again check for its header.
5. Audio stenography
   a. Select Key file for audio file samples selection.
   b. Select data & encrypt it using symmetric key cryptography,
   c. Select Samples of an audio wave file based on the content of key file.
   d. Hide encrypted data into LSB bit position of selected samples.
   e. Assembles audio samples so that result stego audio file will generate.
   f. Save Result stego audio file containing secrete data in an encrypted format.
6. Generated AVI uncompressed AVI video from extracted images/.
7. Add Watermark frame in AVI video.
8. Add Stego audio into AVI video & thus result AVI video with secrete information is generated.

3.2. Steps of Proposed System (Data Extraction)

1. Select AVI video & check for its format
2. If input video is uncompressed then extract frames & audio from input AVI video.
3. Check for extracted audio wave file header.
4. Audio Stegnography
   a. Select Key file for audio file samples selection
   b. Extract secrete encrypted data from input audio file.
   c. Select password & decrypt cipher text using correct symmetric algorithm.
   d. Save Result.
5. Stop

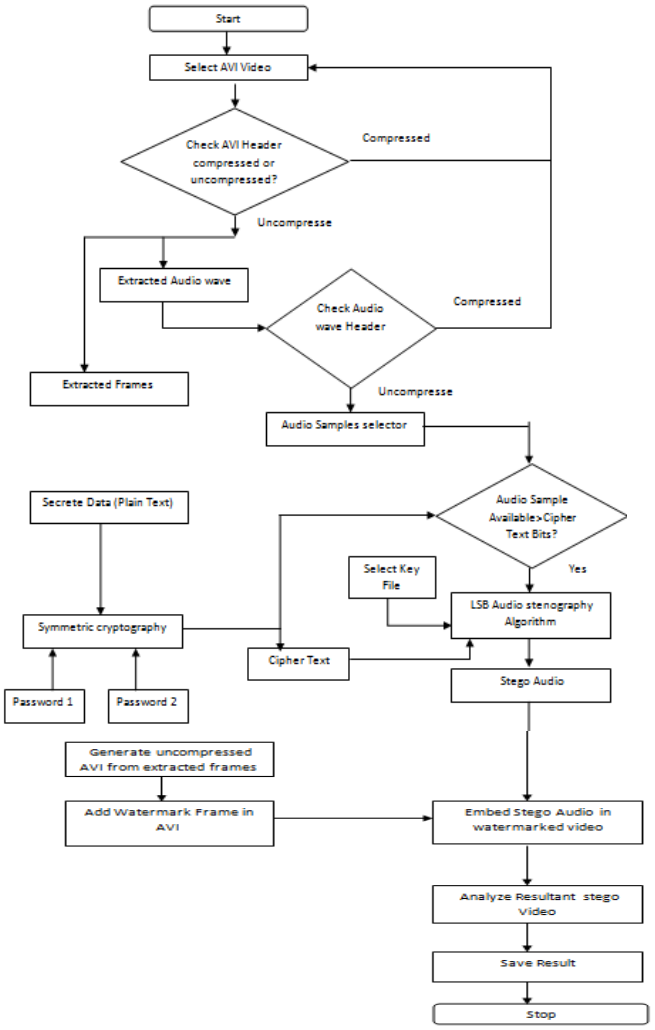

Figure 1. Data Flow Diagram of Proposed system (data Hiding)

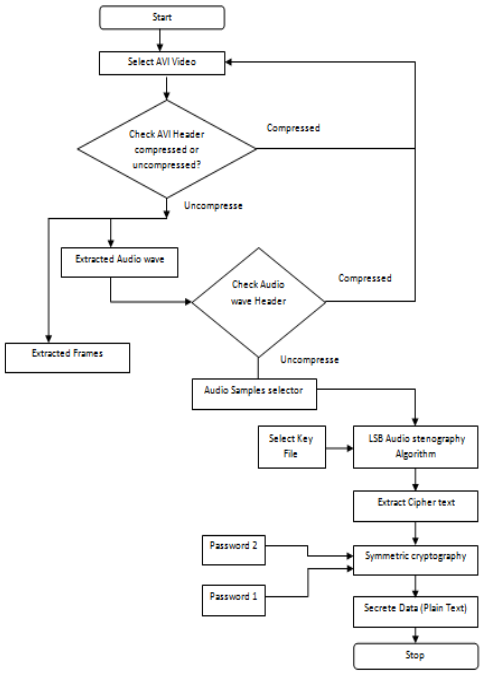

Figure 2. Data Flow Diagram of Proposed system (data Extraction)

3.3. LSB Audio Stegnography

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

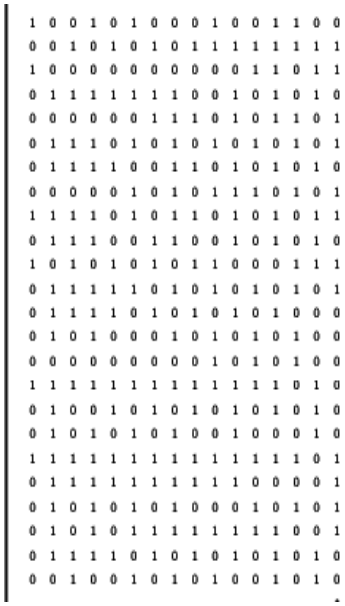

Figure 3. Original Audio Samples

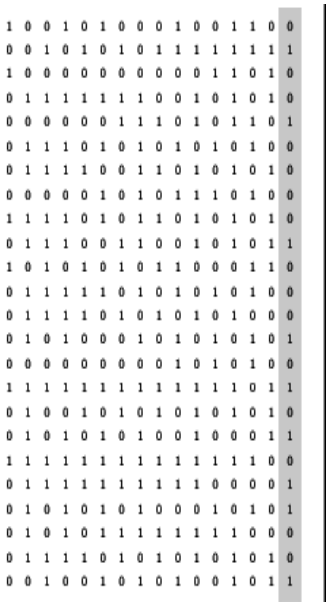

Figure 4. Stego Audio Samples

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage: As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable.

4. EXPERIMENT RESULT

Hiding method/music	Country	Violin	Pop
Discrimination values (%)			
Standard algorithm (3 LSBs)	52	53	48
Standard algorithm (4 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 (4 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

Figure 5. Modified LSB audio stegno Method

LSB Method	*Discriminates Value*
Country	60
Violin	56
Pop	65
Quantization error	
Method	***Error***
LSB	-1 to + 1
3rd LSB	-8 to + 8
4th LSB	-16 to + 16
5th LSB	-32 to + 32
6th LSB	-64 to +64

Figure 6. Proposed LSB Audio stegno Method

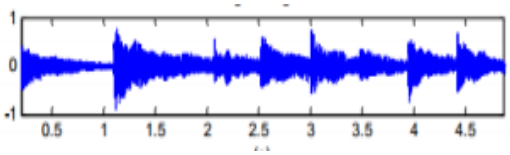

Figure 7. Original Audio Wave

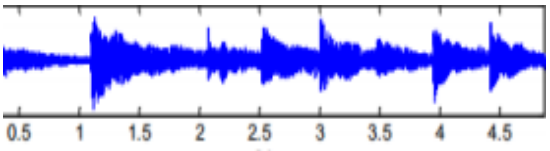

Figure 8. Result Audios stego wave

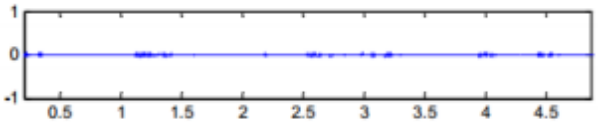

Figure 9. Difference Audio Signal

Table 1. Comparison of proposed LSB with modified LSB method

Method	Data Hiding Capacity	Data Extraction	Flipping Required
LSB	One bit/Sample	100%	No
3rd LSB	One bit/Sample	100%	Yes
4th LSB	One bit/Sample	100%	Yes
5th LSB	One bit/Sample	100%	Yes
6th LSB	One bit/Sample	100%	Yes

5. CONCLUSION

We presented a reduced distortion algorithm for LSB video steganography. The key idea of the algorithm is watermark bit embedding that causes minimal embedding distortion of the host audio. Listening tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 4th to 6th LSB layer without affecting the perceptual transparency of the watermarked audio signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant cryptography provided for data security.

REFERENCES

[1] Ahmed Ch. Shakir, "Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", *Journal of Computer Science*, Vol. 6, No. 3, pp. 320-322, 2010.
[2] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O.Balitanas, "Data Hiding in Video", *International Journal of Database Theory and Application*, Vol. 2, No. 2, June 2009.
[3] Andreas Westfeld and Gritta Wolf, "Steganography in a Video Conferencing System", Information Hiding, Springer-Verlag Berlin Heidelberg, pp. 32-47, 1998.
[4] Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method".
[5] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", *i-manager's Journal on Software Engineering*, Vol. 4 l, No. 3, pp.65-71, March 2010.
[6] D. P. Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-

PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai, 2010.
[7] Richard E. Woods & Rafael C. Gonzalez, "Digital Image Processing", Book.
[8] Fridrich, J. R. Du, M. Long, "F 5 algorithm implementation", Steganalysis in Color Images, Binghamton, 2007.
[9] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", George Mason University.
[10] S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream", *International Journal on Computer Science and Engineering*, Vol. 02, No. 03, pp. 764-766, 2010.
[11] Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB replacement", *International Journal of Engineering Science and Technology*, Vol. 2, No. 12, pp. 6999-7003, 2010.
[12] "*Steganography on new generation of mobile phones with image and video processing abilities*", Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference, Timisoara, Romania, May 2010.
[13] 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.
[14] D. C. Wu and W. H. Tsai. "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.
[15] F. Hartung, B. Girod, "Steganoing of uncompressed and compressed video", *Signal Processing,Special Issue on Copyright Protection and Access Control for Multimedia Services*, Vol. 66, No. 3, pp. 283-301, 1998.
[16] Sherly A. P., and Amritha P. P., "A Compressed Video Steganography using TPVD", *International Journal of Database Management Systems (IJDMS)*, Vol. 2, No. 3, August 2010.