International Journal of Computer Science Engineering Research and Development (IJCSERD), ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online), Volume 3, Number 1
Jan- March (2013), pp: 60-69
© PRJ Publication, http://www.prjpublication.com/IJCSERD.asp

IJCSERD

© PRJ PUBLICATION

KEY BASED LEAST SIGNIFICANT BIT (LSB) INSERTION FOR AUDIO AND VIDEO STEGANOGRAPHY

Sateesh Gudla [1], Suchitra Reyya[2], Aswini Kotyada[3], Aditya Sangam[4]

[1]Associate Professor, Department of CSE, LIET, Vizianagaram
[2]Assistant Professor, Department of CSE, LIET, Vizianagaram
[3,4]Department of CSE, LIET, Vizianagaram

ABSTRACT

Today the security threats through modern malicious technology, confidential information is at risk such as medical records and banking or financial data and military information where the issue of authentication and authorization has become a critical factor. A solution to this problem is steganography which hides the sensitive information inside a medium (text, image, audio and video). This paper proposes how Least Significant Bit (LSB) insertion has been used to hide secret data in both audio and video with the help of key exchange. Diffie Hellman key exchange is considered to enhance the security aspects and also to generate the key based index for LSB insertion. This proposal can reduce the probability of attacks on secret data.

Key Words: Steganography, Video Steganography, Audio Steganography, Secret data, Least Significant Bit (LSB), Diffie Hellman, key based indexing.

1. INTRODUCTION

Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn [4] as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication.” The medium where the secret data is hidden is called as cover medium, which can be image, video or an audio file. Any Stego algorithm removes the unnecessary bits in the cover media and inserts the secret data into the space [3]. Throughout history Steganography has been used to secretly communicate information between people.

There are many applications in the area of Steganography namely Enables secret communication, Tremendous use in Military applications, Alleged use by terrorists and intelligence services etc., Conventionally, there are masking & filtering, Mathematical Transformations, Least Significant Bit [1],[9],[10],[11]algorithms existed in the area of steganography. Most of them are hiding secret information either only in images or audio or

video files. But up to date work suggests that there has been rising curiosity among research organization in applying steganographic techniques to both in video files as well as audio files in a secured manner.

Audio steganography is the scheme of hiding the existence of secret information by concealing it into audio file [11], [12] which result slight altering of binary sequence of the corresponding audio file. Video Steganography is the process of hiding some secret information inside a video [1],[6],[13]. The advantage of using video files and audio files in hiding information is the chances of finding the hidden information by an attacker are lesser. Higher the quality of video and audio sound more redundant bits are available for hiding.

Least significant bits (LSB) insertion is a simple approach to embedding information in a medium. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane [5],[11] of the cover-media in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this work LSB technique is considered in the spatial domain. The working is explained with WAV (WAVEform audio format Sound) audio files, and mp4 (MPEG Layer-4 Audio), AVI (Audio Video Interleave), FLV (Flash Video) video files as medium. In order to do indexing here key exchange is considered. Key exchange procedure is used to exchange a secret key between two users over an insecure medium without any prior information exchange between them. There are RSA, conventional-cryptography, Diffie Hellman key exchange algorithms, among them Diffie Hellman is the Standard Algorithm. Considering Key Exchange concept together with Steganography enhances the security.

The paper is organized as follows; section 2 describes related work. Section 3 shows Diffie Hellman Key Exchange. Section 4 describes the audio & video steganography using LSB insertion. The proposed algorithm is in section 5 with an illustration. Section 6 gives the working model. Conclusion and future work are presented in Section 7.

2. RELATED WORK

As mentioned earlier, steganography is the science of writing hidden messages to guarantee information which is accessible only by authorized parties, and to the one has the secret key and it is inaccessible to others [2],[8]. It is the practice of hiding information usually text messages, inside other file (host file). This practice of hiding information (steganography) is normally called stego. Information can be hidden (or embedded) inside any type of multimedia file; Distinctive image files, audio files and video files are the most widely used today. The host files can then be exchanged over an insecure medium without anyone knowing what really lies inside of them.

Computer Steganography is basically categorized into two methods; lossless method and loss method. Lossless method is a computerized image or sound or video files [8] can be replaced without losing their functionality. Since the loss method depends on the inability of human optic to differentiate any changing in image color or sound quality.

Audio Stenography has wide range of applications such as Covert communication, Digital water marking, access control, etc there are several methods are available for audio steganography. Some of them are LSB Coding, Phase Coding, Spread Spectrum, and Echo Hiding. Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

Least Significant Bit (LSB) [7] method is one of the most important methods in insertion steganographic method. It is a simple approach for hiding a significant amount of information in a multimedia file. Usually modern computer system uses 8-bit (gray scale), 24-bit (BMP) or 32-bit (CMYK) files to store digital files. However, to hide information inside digital media by using the LSBs, each byte of a 24-bit media file can store 3 bits in each pixel . This process actually needs a secret key that is called stego-key. The stego-key [2] is used to control the stego process such as the selection of pixels. The selected pixel is then will be used to embed the secret binary information.One of such technique is Hash based Least Significant Bit (LSB) [1] technique for video steganography. A hash function is used to select the position of insertion in to LSB bits.

In this paper a Key based Least Significant Bit (LSB) technique is proposed where it is generating Stego key as well as enhancing the security.

3. DIFFIE-HELLMAN KEY EXCHANGE

The Diffie-Hellman key exchange protocol was the initial system to operate public-key or two-key cryptography. The Diffie-Hellman [2],[8] procedure is used to exchange a secret key between two users over an insecure medium without any prior information exchange between them. Normally, the exchanged secret key is then used as the key (password) for security applications. In a secret key algorithm, both parties share the same secret key. However, the process of sharing the secret key between both the sender and the recipient, introduces a problem, i.e. the key distribution problem. Public key exchange crypto system alleviates the key distribution problem by using two keys, a private and a public key. By exchanging the public keys, both parties can calculate a unique shared key, known only to both of them.

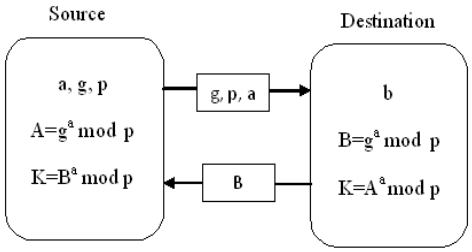


Figure 1: Diffie -Hellman Key Exchange protocol.

Algorithm for key exchange

Source must do the following:

a) Choose a prime numbers p randomly, and choose a primitive root g, and private key a.
b) Compute the A (Source public key), as follows: $A = g^a \bmod p$.
c) Send the public value A to Destination.
d) Compute the secret value K, as follows: $K = B^a \bmod p$.

Destination must do the following:

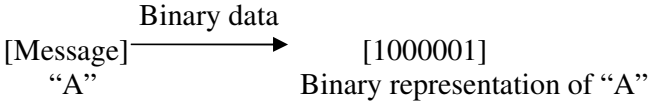
a) Choose a private key b randomly.
b) Compute the B (Destination public-key), as follows: $B = g^b \bmod p$.
c) Send the public value B to Source.
d) Compute the secret value K, as follows: $K = A^b \bmod p$.

Now source and destination are having a unique key for secured communication. First, it resolves the authentication problem and then it is used to select frame for insertion and to generate the key based index for LSB algorithm.

4. AUDIO AND VIDEO STEGANOGRAPHY USING LSB INSERTION

Least significant bits (LSB) insertion is a simple approach to embedding information in a medium. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-media (audio and video) in a deterministic sequence. This is the simplest of the steganography methods based on the use of LSB, and therefore the most vulnerable. The embedding process consists of the sequential substitution of each Least Significant Bit (LSB) of the cover media pixel for the bit message. For its simplicity, this method can camouflage a great volume of information. The following steps illustrate hiding the secret data "A" in the cover media.

Step 1: Reading the message.

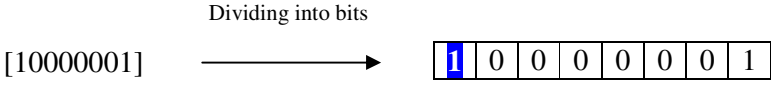


Step 2: Read required information of Cover media.

10010000	10011010	10011100	10010010
00111100	10101010	11110000	11001100
01010101	01001111	11110001	11110011
01111111	10111111	01000000	11100101
01111000	01111101	10000011	10000100
01111100	10000101	10000111	10000011
10001010	10011001	10100111	10011010

Figure 2: pixel representation of cover medium

Step 3: Break the message to be hidden into bits.



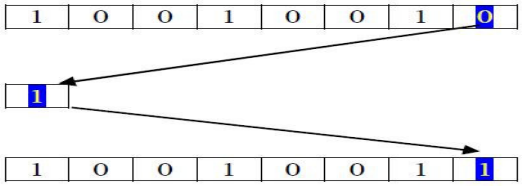
Step 4: Extracting the Cover frame.

10010010	10011010	10011100	10010010

Step 5: Hiding message bits into cover media using least significant bit insertion.

1	0	0	1	0	0	1	0

Replace the least significant bit:



Step 6: Regeneration of cover media frames after hiding the message.

10010011	10011010	10011100	10010010

The audio and video stream consists of collection of frames and the secret data is embedded in these frames as payload. The information of the cover audio and video such as number of frames (n), frame speed (fp/sec), frame height (H) and width (W) are extracted. The cover video is then broken into frames. Now the proposed key based LSB technique has been applied to conceal the data in the carrier frames. The size of the message does not matter in audio and video medium as the message can be embedded in multiple frames of audio and video.

5. PROPOSED ALGORITHM

The proposed algorithm takes the secret data and conceals them in LSB of RGB (Red, Green and Blue) pixels of the cover frames of video and the selected frames of audio in order to retain the quality of audio and video.

As the key value is unique for both the source and destination using the Diffie Hellman, we can use it for selection of audio and video frames as well as for generating the position of LSB bits both for insertion and extraction.

The frame selection is done using

Frame = (Key) modulus (Number of Frames) (1)

Where,

Frame – Frame for data insertion.
Key – Generated Diffie Hellman key.
Number of frames – The total number of frames in audio or video.

The embedding positions of the secret data in the LSB is computed using

Index = (Key) modulus (Number of LSB bits) (2)

Where,

Index – LSB insertion position.
Key – Generated Diffie Hellman key.
Number of LSB bits – The total number of LSB bits for the insertion of secret data.

When the number of LSB bits is 'm' (1 to 8 for 1 Byte) then the index for LSB insertion can be 0 to m-1.

The proposed algorithm, both for hiding and unhiding are given in this section. Hiding techniqueis given in section 5.1 whereas unhiding technique is given in section 5.2.

5.1. Algorithm for Hiding the secret information

Algorithm : Hiding the secret information

Input: An audio file, video file and text message.
Output: Stego files.
Method: Hiding the secret data in carrier media using LSB insertion.

1. Begin
2. Reading required information from cover video and audio.
3. Extract the audio and video frames.
4. Split the secret data to insert into audio and video frames.
5. Find four (4) LSB bits of RGB pixels of cover video and LSB bits of the audio frames.
6. Obtain the position of secret data for inserting into the cover audio and video frames using key based indexing.
7. Insert the bits of secret data into the cover frames using the position obtained.
8. Regenerating audio and video frames.

5.2. Algorithm for Unhiding the secret information

Algorithm : Unhiding the secret information

Input: Stego files.
Output: Secret message.
Method: Unhiding the secret data from carrier media using LSB insertion.

1. Begin
2. Reading required information from stego video and audio file.
3. Extract the audio and video frames.
4. Find four (4) LSB bit positioning of RGB pixels of stego video and LSB bits positioning of audio frames.
5. Obtain the bit position of inserted secret data using key based indexing.
6. Retrieve the respective bits from RGB pixels of the stego frames using the position obtained.
7. Reconstructing the secret data.
8. Regenerating audio and video frames.

6. THE WORKING MODEL

First, the Diffie Hellman key exchange is done to authenticate the communication and then the key is used to generate the index for the LSB insertion of both the audio and video with the proposed algorithms. At the source the secrete message is broken into two parts one is inserted into audio and the other one is inserted in to video. And at the destination extraction of data is done from audio and video, these are combined to get the original data, which is shown in Figure 3. As it consists of authentication, insertion into both audio and video this is secured than considering only audio or video.

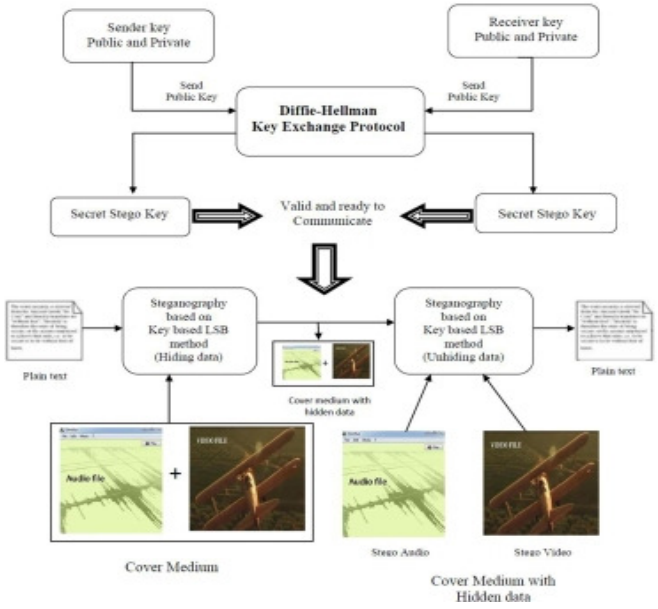


Figure 3: Model of Key based LSB Audio and Video Steganography

7. RESULTS

The working model has been implemented and the results are shown. Figure 4 shows hiding the secret data into "myaudio.wav" audio file and myvideo.avi" video file and Figure 5 shows unhiding the data form stego audio and stego video.

Figure 4: Screen to hide data

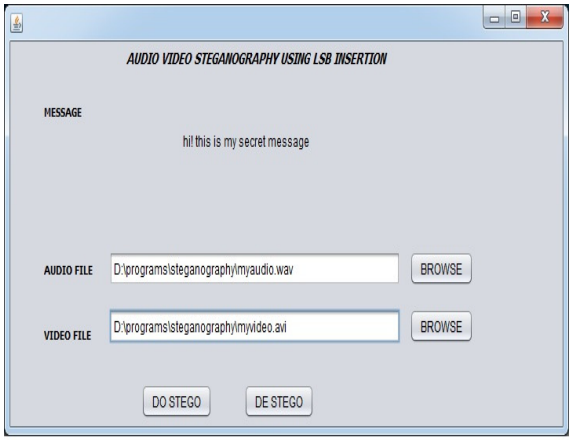


Figure 5: Screen to unhide the data

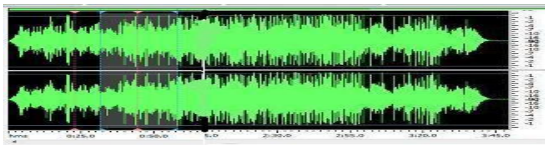


Figure 6: Audio file before insertion of data

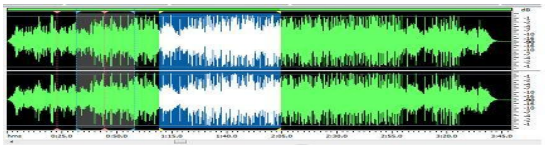


Figure 7: Audio file after insertion of data

Figure 8: Video before insertion of data

Figure 9: Video after insertion of data

8. CONCLUSION

A key based LSB technique has been presented. This technique is used to cover video and audio files in spatial domain to hide the secret data. The security aspects of proposed technique are quite improved as it considers the combination of audio and video with key distribution. The technique is verified using WAV audio files, AVI video files. This work can be further extended in the aspect of security as well as efficiency of algorithms.

ACKNOWLEDGEMENT

We express our sincere and profound gratitude to our principal Dr. V.V.Rama Reddy, management members our chairman Sri P.Madhusudhana Rao, Vice-chairman Sri P.Srinivasa Rao and Secretary Sri K.Siva Rama Krishnan for their valuable support and guidance.

We also thank Prof. A. Rama Rao, Dr. M. Rajan Babu, and Prof. Hari Babu Thammineni for their continuous support.

REFERENCES

[1]. Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[2]. Mohammad Ahmad Alia, Abdelfatah A. Yahya, "Public–Key Steganography Based on Matching Method", European Journal of Scientific Research ISSN 1450-216X Vol.40 No.2 (2010), pp.223-231,© EuroJournals Publishing, Inc. 2010.

[3]. Balaji, R. ,Naveen, G.,"Secure data transmission using video Steganography" , Electro/Information Technology (EIT), 2011 IEEE International Conference on 15-17 May 2011.

[4]. E. Cole and R.D. Krutz," Hiding in Plain Sight: Steganography and the Art of Covert Communication",Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.

[5]. H.B.Kekre, Archana Athawale, and Pallavi N.Halarnkar, "Increased Capacity of Information Hiding in LSB's Method for Text and Image",World Academy of Science, Engineering and Technology 2008.

[6]. Poonam V Bodhak, Baisa L Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.
[7]. Gabriel Macharia Kamau, Stephen Kimani2 Waweru Mwangi2, "An enhanced Least Significant Bit Steganographic Method forInformation Hiding", Journal of Information Engineering and Applications www.iiste.org ISSN 2224-5782 (print) ISSN 2225-0506 (online),Vol 2, No.9, 2012.
[8]. Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi , "PUBLIC-KEY STEGANOGRAPHY BASED ON MODIFIED LSB METHOD", Volume 3, No. 4, April 2012 Journal of Global Research in Computer Science.
[9]. Djebbar, Fatiha ,Univ. de Bretagne Occidentale, Brest, France Ayad, B.; Hamam, H.; Abed-Meraim, Karim ,"A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011 International Conference on 25-27 April 2011.
[10]. K.P.Adhiya, Swati A. Patil , **"**Hiding Text in Audio Using LSB Based Steganography", Information and Knowledge Management www.iiste.org, ISSN 2224-5758, Vol 2, No.3, 2012.
[11]. Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125.
[12]. Jayaram P, Ranganatha H R, Anupama H S, "INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.
[13]. D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, "Embedding Data in Video Stream using Steganography", in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.
[14]. Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.pp 173-178,2007.
[15]. Vismita Nagrale, Mr. Ganesh Zambre and Mr. Aamir Agwani, "Image Stegano-Cryptography Based on LSB Insertion & Symmetric Key Encryption" International journal of Electronics and Communication Engineering &Technology (IJECET), Volume 2, Issue 1, 2011, pp. 35 - 42, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472, Published by IAEME.