INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DATA ENCRYPTION TECHNIQUE IN VIDEO USING AES ALGORITHMS FOR SHARING DATA SECRETLY

PROF. D.S.MAIND, SHILPA R. JADHAV

1. Department of Information Technology, IBSS College of Engg, Amravati.
2. Asst Professor, Department of Electronics & Telecommunication, IBSS College of Engg, Amravati.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Data Encryption;

Advance encryption standard;

Security;

Data hiding;

Data hiding

Corresponding Author

Prof. D. S. Maind

Abstract

The main objective of this paper is to develop a secret data sharing by using data hiding and extraction procedure for audio but by using uncompressed AVI videos. The videos are large so it can be transmitted from sender to receiver side over the network after processing the source video by using these Data Hiding and Extraction procedure securely. There are two different procedures, which are used here at the sender's end and receiver's end respectively. Secret communication is the main objective of this paper, so here we proposed some technique for sending data securely through Video.

I. INTRODUCTION

Video Steganogaphy deals with hiding secret data or information within a video. In this project, a based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A function is used to select the position of insertion in LSB bits. The proposed method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic video file. The proposed technique is compared with existing LSB based steganography and the results are found to be encouraging. An estimate of the embedding capacity of the technique in the test video file along with an application of the proposed method has also been presented.

II. LITERATURE REVIEW

Several steganographic methods have been proposed in literature and most of which are performed in pixel domain. However major contribution is in the domain of Image Steganography. The existing methods are mainly based on LSB where LSBs of the cover file are directly changed with message bits. In [1] a robust image steganography technique based on LSB insertion and RSA encryption technique has been used. Masud et.al has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. Other Examples of LSB schemes can be found in . Whereas EzStego developed by Machado embed information into an image in the GIF format. It sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable. Tseng and Pan presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Proposes bit plane complexity segmentation (BPCS) method to embed information into the noisy areas of the image. These techniques are not limited to the LSB. Existing steganographic software, such as

Steganos, S-tools and Hide4PGP, are based on LSB.

Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exists, where proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. Whereas in selected LSB steganography algorithm is proposed. Other steganography techniques in uncompressed raw video, is illustrated [2], [3] and [7]. Steganography techniques for compressed video stream can be found in [5]. Another video steganography scheme based on motion vectors and linear block codes has been proposed in [6].

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). The origin of steganography is biological and physiological. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia". A short overview in this field can be divided into three parts and they are Past, Present and Future [4].

2.1 Past

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [8, 9].

Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information [8, 10].

2.2 Present

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication [11]. In modern approach, depending on the nature of cover object, steganography can be divided into five types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

Information can be hidden inside a multimedia object using many suitable techniques. As a cover object, we can select image, audio or video file. Depending on the type of the cover object, definite and appropriate technique is followed in order to obtain security. In this section, we will discuss different techniques or methods which are often used in image, audio and video steganography.

- *Text Steganography*

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways [8]. Many techniques involve the modification of the layout of a text, rules like using every n^{th} character or the altering of the amount of white space after lines or between words [12]. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key.

- *Image Steganography*

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

III. METHODOLOGY

The technique is a Least Significant Bit (LSB) technique for Video Steganogaphy has been proposed. The flow diagram of the same is given in Figure 4.1.

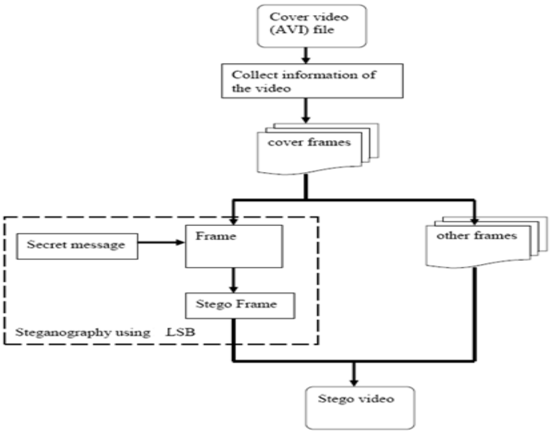


Figure 4.1: A) Block diagram of LSB Video Steganogaphy technique Encoding

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

The proposed technique takes sixteen bits of secret data at a time and conceals them in LSB.

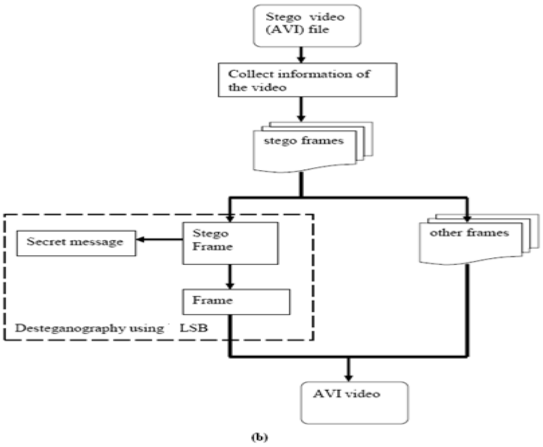


Figure 4.1: B) Block diagram of LSB Video Steganogaphy technique Decoding

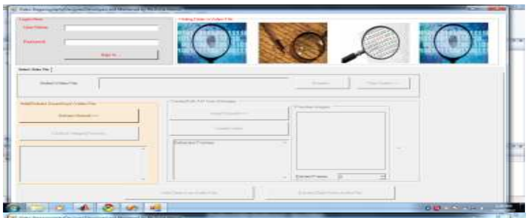
The embedding positions of the 16 bits of LSB is obtained using a LSB function of the form,

$$k= p \% n..... \quad (1)$$

where, k is LSB bit position within the pixel, p represents the position of each frames and n is number of bits of LSB.

IV. SYSTEM IMPLEMENTATION

In this section the various forma that are used for the system implementation



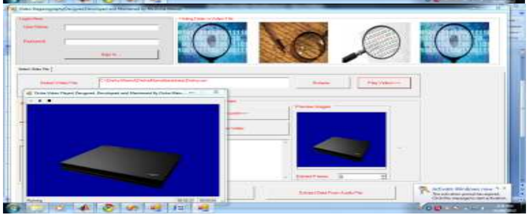


Figure 5.1 Login Form

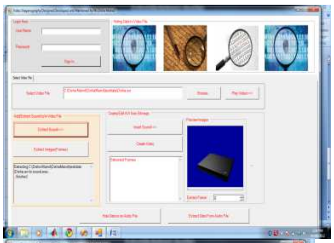
Figure 5.2 Selection of Input Video

Figure 5.1 shows the login form. It contains the username and password field. After login successfully the system started working. After successful login the rest of the buttons present on the forms become enabled, otherwise buttons are disabled. If the username and password is incorrect then it displays the message.

From the above figure it is observed that there are various buttons such as extract sound, Extract images, insert sound etc. The working of various buttons can be explained accordingly they can be used during the project running state.

After succefully login we move towards the next form. Figure 5.2 shows the form which shows the selection of the input video.

- The video can be selected with the help of select video field.
- Browse button is useful to show the path for the selection of the video.
- Play video button is useful to play the video. The window in the above figure shows the playing video and preview image field is useful to show the image.
- Extract Frame field is useful to represent the number of frames present inside the video because every video is developed by combining the number of frames.



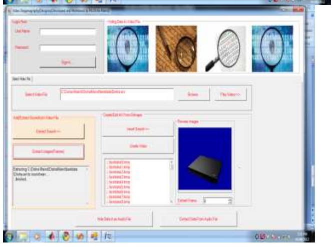


Figure 5.3 Extraction of Sound

Figure 5.4 Extractions of Frames

After the selection of the video we want to extract the sound as well as the number of frames present inside the video. The sound will be extracted with the help of extract sound button. By using this button we can separate the sound present inside the video. The field present below the extract image is useful to show the message that the sound is extracted.

The sound which is extracted is stored inside the sound.wav file. The stored sound file is used later during the process of stegnography. The detailed working of the extraction of the sound from the selected video is shown in figure 5.3. After successfully extract the sound from the video in the previous figure now we have to extract the frames from the video. The frames can be extracted from the video by using extract frame button. These frames are nothing but images that are present inside the video. The number of frames that are extracted from the video is shown by using extract frames field. The field below the create video represents the frames that are present inside the video. The frames are stored in .bmp format. The detailed working of the extraction of the frames is shown in figure 5.4.

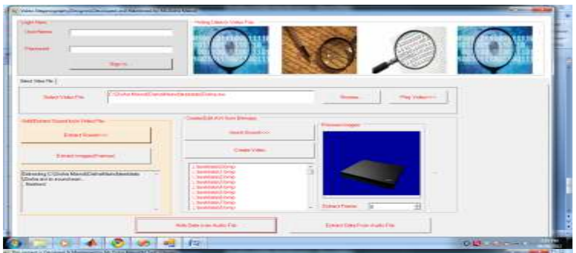


Figure 5.5 Data Hiding

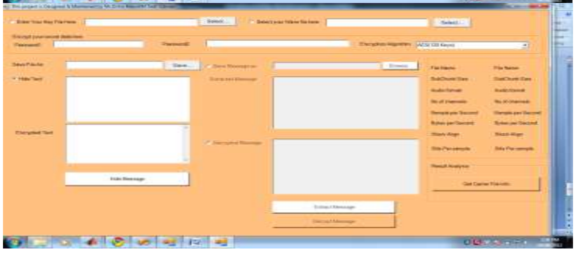


Figure 5.6 Audio Steganography

After extracting the frames and the sound from the video we have to hide the data inside the video. To hide the data inside the video we first extract the sound and frame. The data can be hiding inside the video by using hide data in audio file. This button is useful to hide data inside the audio we use the hide the data inside the sound. In our system we hide the data in the audio file by using hide data button. For hiding the data inside the audio file we used encryption algorithm. The working of hiding the data inside is shown in figure 5.5. Figure 5.6 show the form which is useful for audio steganography. For audio steganography we require two key files. These key files can be including by using Enter your key file. After selecting the key files the data can be encrypted by using AES algorithm.

This algorithm is worked for the 128 keys. After performing the encryption the data can be protected by using two passwords. This password is inserted by using two password fields. After protecting the data with the help of password the file can be saved at the proper location. Save button is used to save the data. Hide text field is useful to hide the text and the encrypted text field is useful to show the data in the encrypted format this data is encrypted by using AES algorithm. Extract Message and Decrypt message button is useful to extract the message and decrypt the data.

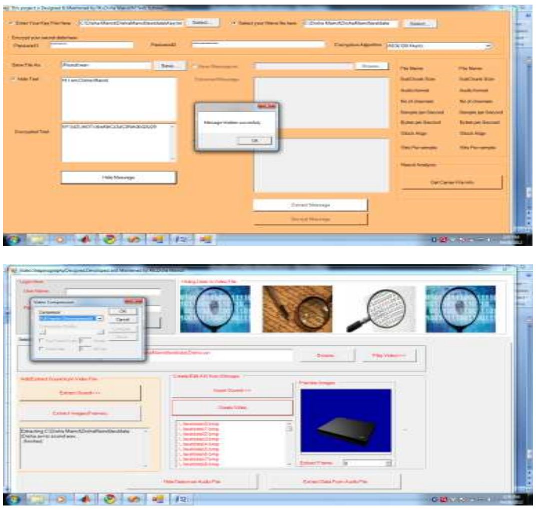


Figure 5.7 Data Hiding in Extracted Audio File, Figure 5.8 Create video from Extracted Images

The process of hiding the data inside the audio file is shown in figure 5.7. The above figure shows the use of key files. The password is inserted inside the Passwords field. There is one criterion while entering the password the length of password is greater than or equal to eight. The working of hide text and the encrypted text is shown in the above figure. After successfully hiding the data inside the audio file it display the message that hiding data successfully.Figure 5.8 shows the working of creation of the video from the extracted images.

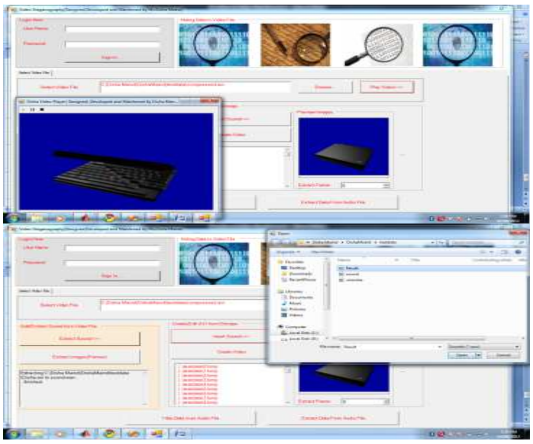


Figure 5.9 Video Created from Extracted frames, Figure 5.10 Sound Insertions in Video

When we extract the sound and the frames from the video. After that with the help of AES algorithm we hide the data inside the audio filed. Then we create the video. The video in which we hide the data is shown in figure 5.9. After hiding the data inside the audio file with the help of encryption algorithm. Then we have to add that file inside the audio. The need to add the sound is require because we create the video. The detailed working of adding the sound is shown in figure 5.10. The small window shows the path from where we have to add the sound. The sound is inserted by using insert sound button.

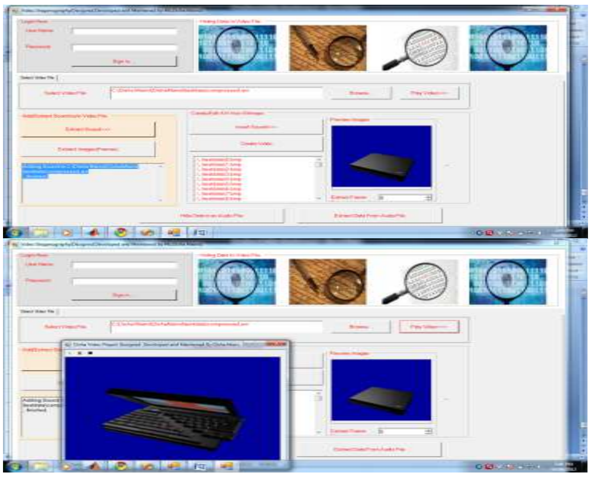


Figure 5.11 Sound Added Status,

Figure 5.12 Steg Video

Figure 5.11 show the working of form after adding the sound successfully. When we add the sound successfully it displays the message in the message field. After performing each procedure properly related with adding the sound, encrypt the data; apply the algorithm, reunion of the sound and frames for the creation of their video in which we hide the data. After performing all operations we play the video. The video play is shown in figure 5.12.

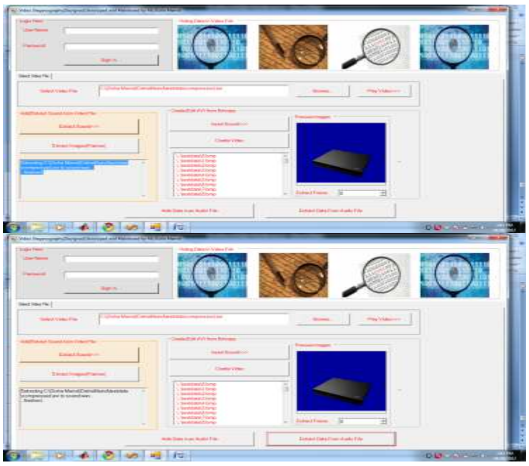
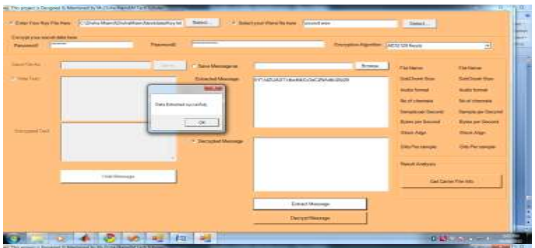


Figure 5.13 Sound Extracted from Stego Video , Figure 5.14 Extract Data from Audio file

After hiding the data inside the video we want to find the related information that is stored inside the video in encrypted format. To find the information from the encrypted video we have to first extract the sound from the stego video. The sound that is extracted from the stego video is shown in figure 5.13.Once we extract the sound from the stego video it display the message with the elated information.

Once we extract the audio from the stego video we have to extract the data from the audio file. The data can be extracted by double clicking on the Extract data from the audio file button. After clicking on this button we get the data from the audio file. Figure 5.14 show the procedure of extracting the data from the audio file.



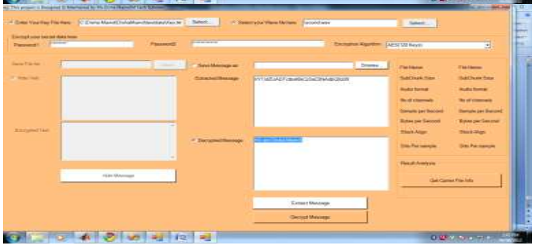


Figure 5.15 Extracted Data

Figure 5.16 Decrypted Data

Figure 5.15 shows the successful extraction of data from the video. Figure 5.16 shows the decrypted data from the video

V. RESULT ANALYSIS

Figure 6.1 shows the analysis of LSB bit method by performing the test on the bits

Sr No	Original Sample in Binary	Original Sample in Decimal	Data Bit (1)	Data Bit (0)	Resultant Bit in Binary	Resultant Bit in Decimal	Q Error
1	00011100 01011100	7276	Nil	0	00011100 01011100	7276	0
2	00011100 01011100	7276	1	Nil	00011100 01011101	7277	1
3	00011100 01011110	7278	Nil	0	00011100 01011110	7278	0
4	00011100 01011110	7278	1	Nil	00011100 01011111	7279	1
5	00011100 01010100	7268	Nil	0	00011100 01010100	7268	0
6	00011100 01010100	7268	1	Nil	00011100 01010101	7269	1
7	00011100 01010000	7264	Nil	0	00011100 01010000	7264	0
8	00011100 01010000	7264	1	Nil	00011100 01010001	7265	1
9	00001100 01011100	3180	Nil	0	00001100 01011100	3180	0
10	00001100 01011100	3180	1	Nil	00001100 01011101	3181	1
11	00001100 01011000	3176	Nil	0	00001100 01011000	3176	0
12	00001100 01011000	3176	1	Nil	00001100 01011001	3177	1
13	00001100 01010000	3168	Nil	0	00001100 01010000	3168	0
14	00001100 01010000	3168	1	Nil	00001100 01010001	3169	1

Figure 6.1 Test by using LSB Method

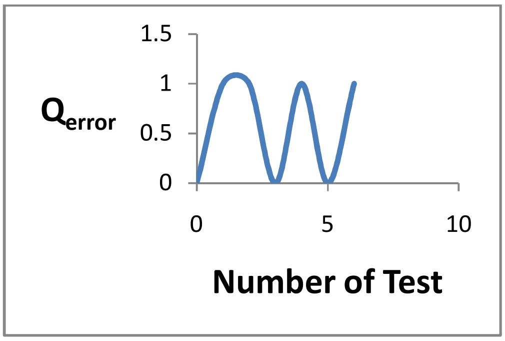


Figure 6.2 Graph between Q_{error} and the Number of test performed using LSB method

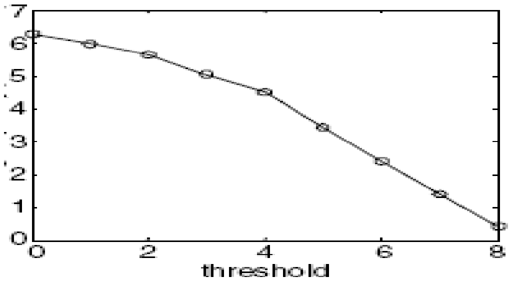


Figure 6.3 Graph given by Tao and Ping

When we compare the figure 6.2 and 6.3 we come to know that LSB method is useful for video steganography because it gives proportionate graph. While the graph plot by Tao and Ping is invariant. After analyzing both the graph we conclude that our graph provide better results as compare to Tao and Ping. Our results are god because we get proportionate graph.

Figure 6.4 shows the signals phase after encoding. The left signal represent the original signal and the right show the encoded signal.

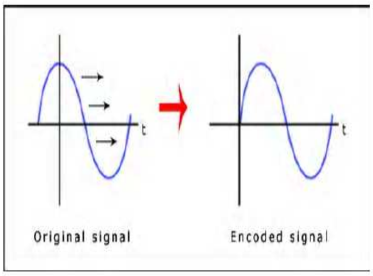


Figure 6.4 Signals Before and After Phase Coding

Figure 6.6 shows the general example of spectrogram in which we show the wave before and after implementing the LSB method

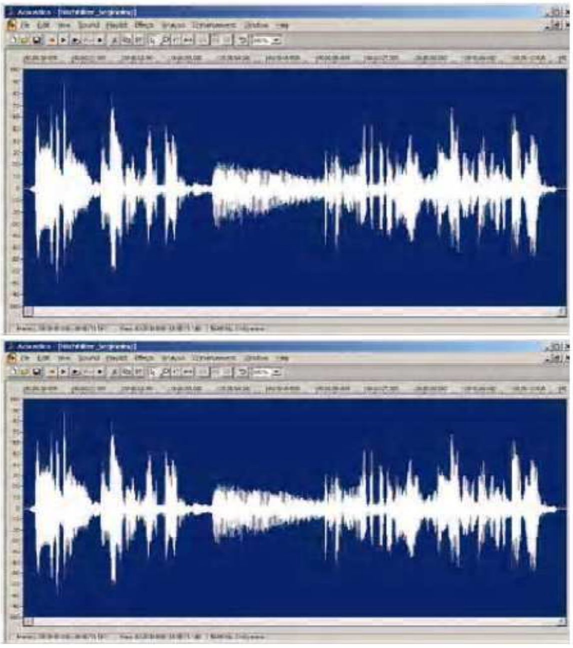


Figure 6.5 Signal Comparison between a WAV File (above) and after (below) the LSB Coding

VI. CONCLUSION

A secured LSB technique for video steganography has been presented in this project. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Performance analysis of the proposed technique after comparison is quite encouraging. The proposed technique is applied to video files; however it can work with any other formats with minor procedural modification. For compressed video files like MPEG the video needs to first decompress then the technique can be applied to the uncompressed video. Whereas for Flash Video FLV files the technique can be applied without modification. Software based Steganographic Engine for video steganography is the future scope of the technique.

I have described how to split uncompressed video so that I can embedded encrypted data in to it, Efficient Data Encryption Technique in Video for Secret Sharing for encrypted data and able to embed data in video and then to decrypt the data and to rebuild the original video by removing the hidden Encrypted data.

Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. Since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating steganography, to minimize the chances of hidden communication taking place. Even then, perfect steganography, where the secret key will merely point out parts of a cover source which form the message, will pass undetected, because the cover source contains no information about the secret message at all. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. More restrictions on the use of privacy-protecting technologies are not very unlikely, especially in this period of time with great anxiety of terrorist and other attacks.

VII. FUTURE SCOPE

As video steganography continues on its evolutionary path researchers have unearthed new platforms where steganographic techniques could be employed to hide information seamlessly. Such research efforts have rekindled the research and development efforts oriented towards steganography platforms and steganalysis and a number of researchers are working towards discovering new platforms that miscreants could potentially use to hide information. For instance, researchers have shown that voice over Internet protocol (VoIP) could emerge into a popular platform for steganography owing to its ubiquity and the difficulty in detecting hidden information in VoIP streams. In addition to VoIP, platforms such as images and other multimedia content are expected to be widely used for concealing information.

Current research in video steganography is focused on identifying various platforms through which one can hide information,' notes the analyst of this research service. 'Apart from the traditional platforms such as audio, video, and images, researchers are looking for additional platforms through which information can be hidden.' An interesting idea under consideration is to have a separate steganographic channel in a network to send messages. Although each mode has many benefits, it is very difficult to ascertain the single best platform to send hidden messages. Steganography is capable of mitigating piracy by aiding copyright marking.

In the future, digital camera manufacturers could implement steganographic features as a part of camera firmware to annotate pictures with the photographer's copyright information. Camcorder manufacturers could also follow suit and implement steganography and watermarking techniques for protecting video content captured on camcorders and video cameras. Going forward, legitimate applications such as tagging of multimedia content with hidden information could become an important application area for steganography. There is a distinct lack of awareness about video steganography, particularly among the business community. A major challenge associated with the field is convincing organizations to deploy tools to detect insider use of steganography, which requires complete awareness of the way data could be embedded and various approaches toward detecting this activity.

REFRENCES

1. Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing, Volume 60, Issue:2, pp. 556-569, Feb, 2012

2. A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas, Data Hiding in Video in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

3. J. J. Chae, B. S. Manjunath, Data Hiding in Video, Proceedings of the 6th IEEE International Conference on Image Processing, pp.311-315, 1999.

4. Stefan Katzenbeisser and Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 1999.

5. A. Giannoula, D. Hatzinakos, “Compressive Data Hiding for Video Signals”, in Proceedings of International Conference on Image Processing, pp. I529- I532, 2003.

6. Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video steganography using motion vector and linear block codes, in Proceedings of IEEE International Conference on Software Engineering and Service Sciences (ICSESS-20100), pp. 592-595, 2010.

7. Melih Pazarci, Vadi Dipcin, Data Embedding in Scrambled Digital Video, in Proceedings of the 8th IEEE International Symposium on Computers and Communication, pp. 498-503, 2003.

8. Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.

9. Juan Jose Roque and Jesus Maria Minguet, SLSB: Improving the Steganographic Algorithm LSB, in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, pp.1-11, 2009.

10. A. Westfield, and A. Pfitzmann, Attacks on Steganographic Systems, in Proceedings of 3rd Info.Hiding Workshop, Dresden, Germany, Sept. 28–Oct. 1, pp. 61-75, 1999.

11. 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.

12. N. F. Johnson and S. Jajodia, Steganalysis of Images Created using Current Steganography Software, in Lecture Notes in Computer Science, vol. 1525, pp. 32 – 47, Springer Verlag, 1998.