Secured information through digital watermarking and steganography using least significant bit algorithm

[1]Seema S. Girare, [2]Malvika U. Saraf
[1]Research scholar, [2]Assistant Professor
Department of Electronics, Wainganga College of Engineering and Management, Nagpur, India

***Abstract*—Over the last two years it is very essential to protect the confidential data from hackers due to the fast developments of internet. In this paper an efficient algorithm LSB is described to hide the information /logo inside the audio and video file. In the proposed system 4th and 5th bit of LSB is used to do it. This algorithm method provide robustness, imperticibility and easy to implements. A lot of works has been done on digital watermarking of various media such as image and text file, but this particular work will focus on digital watermarking of audio file and video file. Experiments output clearly shows that the message is transmitted via digital watermarking and steganography technique using LSB algorithm without affecting the original file.**

***IndexTerms*—Steganography, Watermarking, Embedding and Retrieving data, Software metrics, PSNR, SNR.**

I. INTRODUCTION

Now a day's network security is important issue due to the swift advancement of technology. People use steganography to transmit secret information to one another without other users acknowledge. Generally data can be embedded using watermarking and steganography technique. Watermarking is the best way for sending data and it is somehow depend /based on steganography method which is very safe technique for copyright protection. There are various types of watermarking content such as image, audio, text file and video file. Therefore there are more option are now available to use. But in previous paper more work has been done on image steganography and watermarking as compared to video and audio steganography. Now in this paper audio file and video file has been used instead of image file. Audio file and video file acts as a cover file which contains the real information. Watermark is used to insert information into cover file, so that users can properly access to it. Hiding some important message/information with the help of steganography and watermarking which is the need of today management and also illegal misuse of information. Therefore digital watermarking is very essential step toward day to day security system. Cover file is defined as the audio file, video file, image file in which information will be embedded is called as cover file.

In this paper describes digital watermarking and steganography method using LSB algorithm for hiding text in audio and video file such that information can reach at receiver in a safe manner without modifying the original audio file/video file and the receiver extract data assigned to him. Section II gives the details of work done and working, section III describes the literature review, section IV describe the proposed algorithm, output result presented in section V, conclusion and future scope finally discuss in section VI.

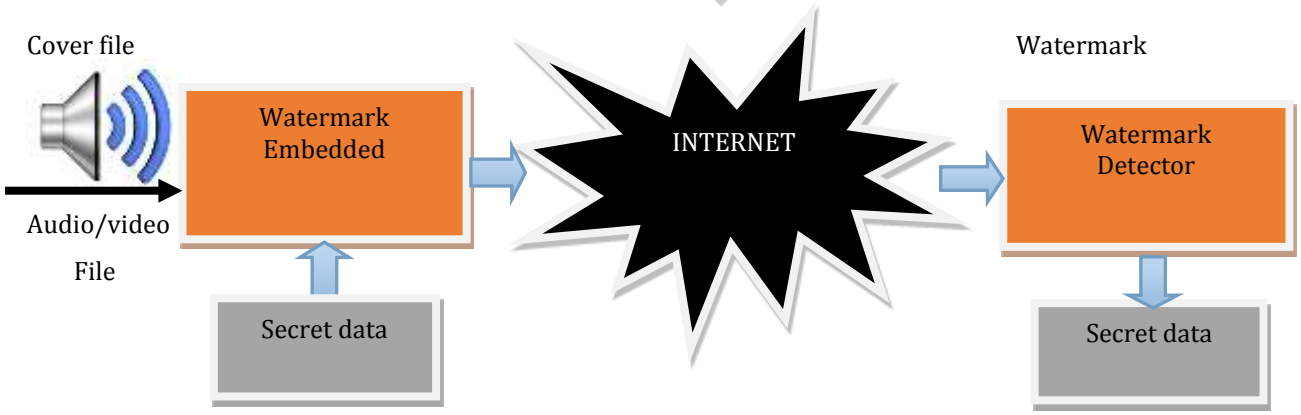

Figure- 1: Process of watermarking

II. PROPOSED METHODOLOGY SYSTEM

The process of audio or video steganography and digital watermarking begin when encoder embedded watermark into cover file .Fig- 2.1 and 2.2 represent the working of audio and video steganography. There are variety of option are available that can be used as a cover files such as text file, image file, video file and audio file.

SENDER

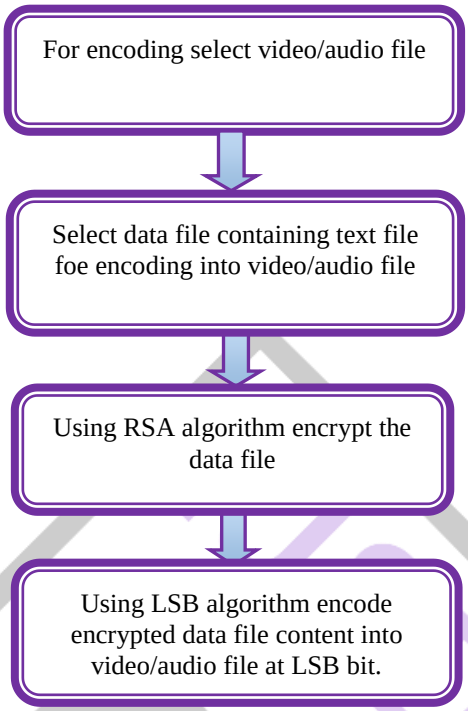

Figure- 2.1: Sender

In this proposed system video and audio file will be used as cover file. In the sender side first select the mp3 audio file format and mp4 video file format .Then the data file are inserted into the cover file using RSA algorithm. The text file is then encoded in LSB bit. Audio /video file size are compared with text file size before embedding and after embedding. If text file size is greater than video file size then process will repeat again. Encoding system is need for inserting data into both file such as video and audio file. In the proposed system 4th and 5th bit of LSB are used to do it, after encoding the text quality of original audio and video file remain unaffected. For embedding the data into video /audio file an encoding mechanism is used.

RECEIVER

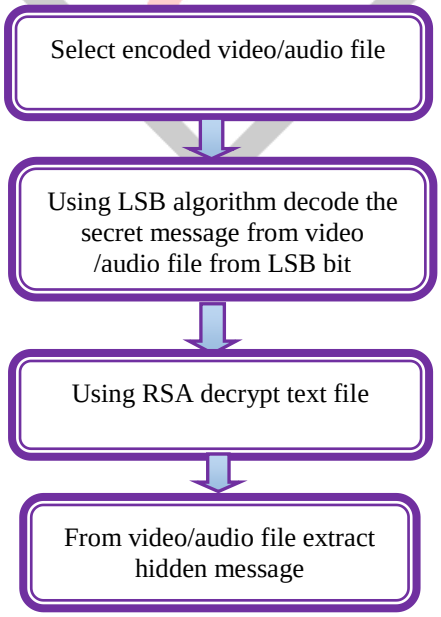

Figure-2.2: Receiver

On receiver side the embedded audio file and video file are selected to decrypt the secret data. Decoding system is necessary to verify or to check whether the text file contains specified watermark or not and it will separate the message from audio and video

file. For security reason least significant bit and RSA algorithm are used. Finally decoder compare the original audio file or video file and embedded audio or video file and compute the result. The resultant audio and video file obtained the secret information. With the help of RSA and LSB algorithm secret data is decoded.

III. LITERATURE SYSTEM

There are different technique are available for video /audio steganography and watermarking. Some of types are as follows:

1. LSB Coding
2. Parity Coding
3. Phase Coding
4. Spread Spectrum

Now in this proposed system least significant bit (LSB) has been used for embedding data into cover file.

The least significant bit (LSB) method is used for simple operation to insert data into an audio and video file. Figure 3 shows the working of proposed technique. In most of the paper used 1st and 3rd LSB bit but in this proposed system, hide the data at 4th and 5th bit of LSB instead of 1st and 3rd least significant bit. And the main reason for hiding data in 4^{th} and 5th bit is due to hackers will not get an idea that data will be hidden at such bit, so data will be more secure at this bit because of other user knowledge.

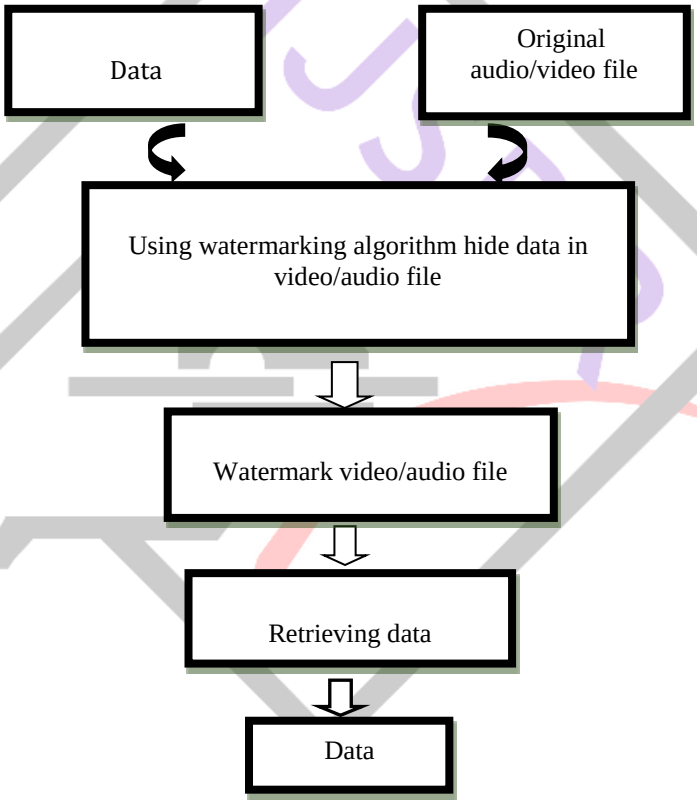

Figure- 3: Framework of LSB proposed system

The working of system start when sender select a cover file, the cover file is very important for any security purpose. The cover file may be text file, video file, image or audio file. First select the cover file which sender want to use for hiding the data inside it.Next it will select the data which it want to hide in cover file. Due to security purpose the text will embedded in cover file. Now in this proposed method audio and video file is used as a cover file. Therefore hide the data in audio file/ or video file by using LSB algorithm and data will be passed to users. At the decoder it will first select the audio file which has been sent by sender .After selecting the audio file or video file it will check the audio and video file that any message is hidden in the video / audio file or not. The receiver will retrieve the data back.

III. PROPOSED ALGORITHM

A) Algorithm for encoding data into audio/video file at the publisher side.

Algorithm used at publisher side for inserting data into audio/video file

In step 1: It will select the audio file/video file for embedding hidden data.

In step2: Then audio file and video file should play to the end of file. So that any noise will not attract the hackers.

In step 3: Now take a text file which contain the secret information.

In step 4: Encrypt data file content

In step 5: Now comparing audio/video file size with text file size

If data file size >video/audio file size

Indicating error and does not encoding the secret data

Else

Encode secret information in audio/video file in least significant bit.

In step 6: After encoding secret data display a message for users indicating a new audio and video file which contains the secret information.

B) Algorithm used at user side for decoding

Algorithm used at receiver side for decoding data from audio/video file

Step 1: Decoding the secret information from new audio file.

Step 2: Decode the secret information from new audio and video file from least significant bit.

Step 3: In audio file and video file if secret information /data present

Then

Message display to receiver after decoding message

Else

Message display that no information is hidden in cover file.

Step4: Decrypt the hidden data

Step5: Finally after decoding, display information to the receiver and receiver extract data assigned to him.

V. RESULT

Different experiments were conducted to check and verify that the above system is successfully work. The tools used for the execution of this algorithm was ASP.NET. Experiments output clearly shows that the message is transmitted via digital watermarking and steganography technique using LSB algorithm without affecting the original file. The above experiment were performed in the audio and video file;

1. Different size of text file are embedded into same audio file.
2. Same text file are embedded into different audio file.
3. Different size of text file are embedded into same video file.
4. Same text file are embedded into different video file.

The proposed idea is implemented using ASP.NET. Web pages are implemented using ASP.NET.ASP.NET framework allow users to developed web pages form, web application and services. Above tables has been drawn with the help of structured Query language (SQL).The resultant output shown in table 5 using SQL new database are created and it also allow to delete previous stored data from a database.

5.1 Implementation of Proposed Methodology for Embedding Text File Content into Audio File:

The following are the steps that are used for this project work:

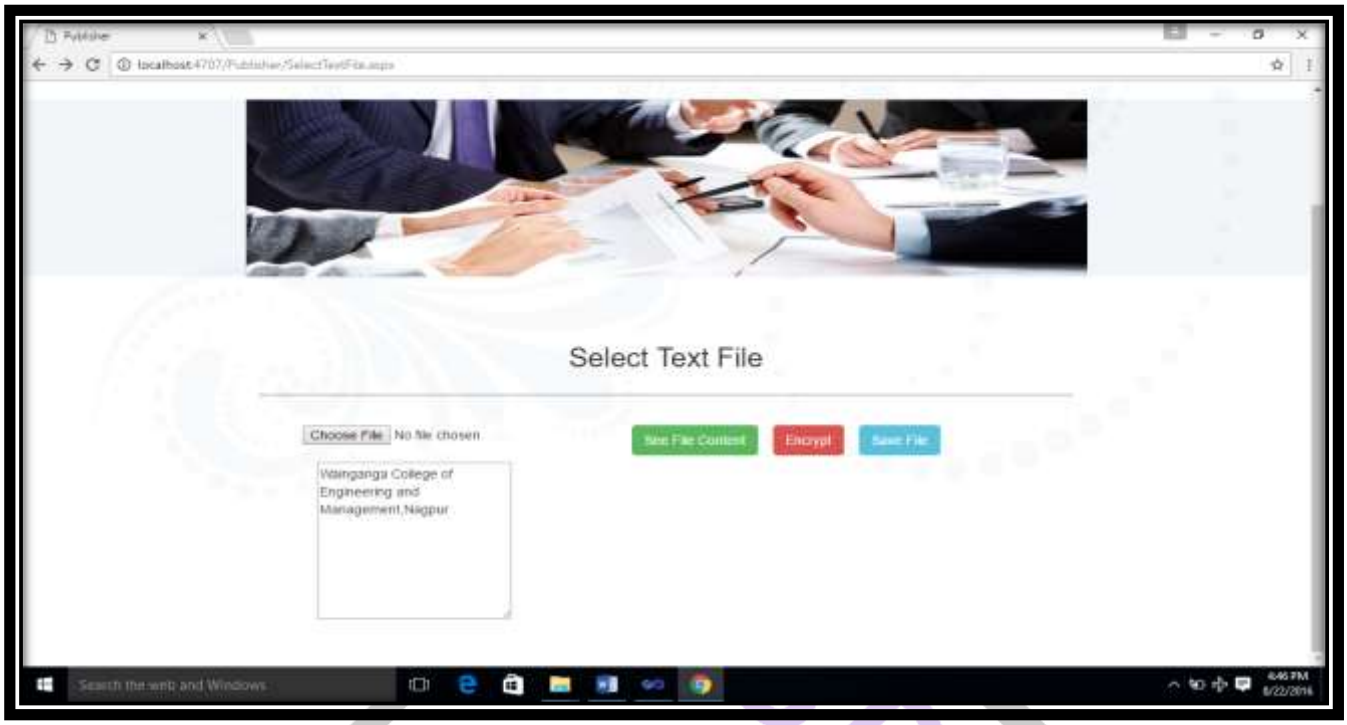

Figure- 5.1: Select the text file containing the secret message

5.2 Implementation of Extracting the Embedded Text from Audio File at the Receiver Side

Figure- 5.2.: Decrypt the secret message from audio file successfully

5.3 Implementation of Proposed Methodology for Embedding Text File Content into video File:

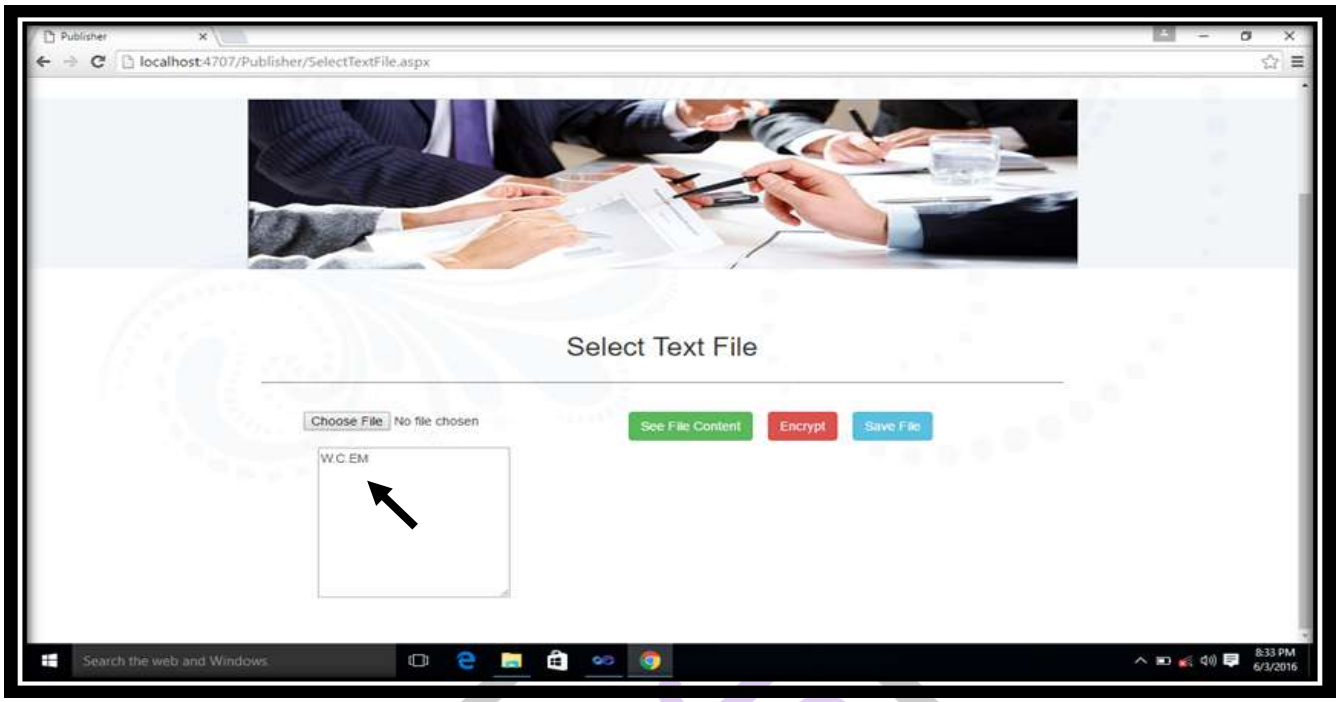

Figure- 5.3: Select the text file containing the secret message

5.4 Implementation of Extracting the Embedded Text from video File at the Receiver Side :

Figure- 5.3.1: Decrypt the secret message from video file successfully.

Final Parameter which includes parameter like PSNR and SNR:

SR.NO	AUDIO FILE	VIDEO FILE	TEXT FILE NAME	SNR VALUE	PSNR VALUE	WATERMARK EXTRACTED SUCCESSFULLY
1	Audio Sample_1		Text 1	38.00	52.03	YES
2		Video sample_1	Text 2	39.00	62.36	YES
3	Audio Sample_2		Text 3	40.00	61.61	YES
4		Video sample_2	Text 4	28.00	63.69	YES

Table no-5: The results are shown in Tabular form

Experimental output clearly shows that the proposed system provides better security not only to audio file but also to video files and successfully watermark. Audio and video watermark files quality are examine in term of 2 parameters: signal to noise ratio (SNR) and peak signal to noise ratio(PSNR).

VI.CONCLUSION

In this proposed system provides an efficient technique for embedding hidden message into audio or video file such that information can reach to receiver securely. Using algorithm RSA and LSB data will be more securely transmitted. This is the main advantages of this algorithm. In this paper describes digital watermarking and steganography method using LSB algorithm for hiding text in audio and video file such that information can reach at receiver in a safe manner without modifying the original audio file/video file and the receiver extract data assigned to him. Experimental output clearly shows that the proposed system provides better security not only to audio file but also to video files and successfully watermark.

FUTURE SCOPE

Secret information can be embedded using various method of watermarking and steganography using proposed system. This paper mainly focus on mp3 format of audio files and mp4 format of video files. It can also be used for various types of audio files like au, uma format and video format like avi,mpeg.

VII. ACKNOWLEDGMENT

The author is thankful to Professor Malvika U.Saraf, faculty of Electronics /Electronics and telecommunication for providing necessary guidance to prepare this paper.

REFERENCES

[1]Bender, W., Gruhl, D., Morimoto, N. and Lu, A (1996).: Techniques for data hiding. IBM Systems Journal, vol. 35, nos. 3&4.

[2] I.J. Cox, M.L. Miller, J.A. Bloom, Digital watermarking, Morgan Kaufmann, 2001.

[3] Puneet Kr Sharma and Rajni "analysis of Image Watermarking using least significant bit algorithm", International Journal of Information Sciences and Techniques (IJIST), Vol.2, No.4, July 2012.

[4] Rajni Goyal1, Naresh Kumar2" LSB Based Digital Watermarking Technique", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 9, September 2014.

[5] N. Cvejic, T. Seppanen "Algorithms for Audio Watermarking and Steganography", PHD thesis, Oulu University of technology, June 2004

[6] Methods of Audio Steganography, Internet publication on www.Snotmonkey.com.

[7] ManishaRana, RohitTanwar, 'Genetic Algorithm in Audio Steganography", International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 1 – Jul 2014.

[8] StutiGoel,ArunRana,Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography" IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) , Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48 www.iosrjournals.org

[9] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", Proceedings of International Journal of Engineering and Innovative Technology (IJEIT), March 2013Volume 2, Issue 9.

[10]Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", Proceedings of International Conference on Intelligent Computation Technology and Automation, 2010.

[11]Manpreet Kaur, Sonia Jindal, Sunny behal, " A Study of Digital image watermarking" , Proceedings of Volume2, Issue 2, Feb 2012.

[12] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[13] Abdullah Bamatraf, Rosziati Ibrahim Mohd. Najib B. MohdSalleh" Digital Watermarking Algorithm Using LSB"International Conference on Computer Application and Industrial Electronics (ICCAIE), December 5-7, 2014 kualu Lumpur, Malaysia.

[14] Frank Hartung, Martin Kutter (July 1999), "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[15] R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced", Journal of Theoretical and Applied Information Technology.

BIOGRAPHIES

Seema S.Girare is aM.tech students of Electronics branch at Wainganga college of Engineering and Management, Nagpur, Maharashtra, India. She completed B.E in Electronics and Telecommunication branch from G.H. Raisoni Institute of Engineering and Technology for Women, from RashtrasantTukadojiMaharaj Nagpur University, Maharashtra in 2014. She completed diploma in Electronics and Telecommunication (ETC) from G.H. Raisoni Polytechnic in 2011. Her areas of interest are communication, Digital Design and image processing.

Prof.Malvika U.Saraf is the Head of Electronics/Electronics and Telecommunication at Wainganga college of Engineering and Management, Nagpur, Maharashtra, India.She completed M.tech from G.H. Raisoni Institute of Engineering and Technology for Women, from RashtrasantTukadojiMaharaj Nagpur University, Maharashtra. She has an experience of about 6 year in teaching field .She has 2 year of industrial experience. Her areas of interest are digital image processing, Digital Design.