Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 7, July-2016

IMPLEMENTATION OF DATA HIDING TECHNIQUE USING LSB SUBSTITUTION AND HDL

Prof. Ashwini Desai[1], Priyanka U.Shirodkar[2]

[1,2]*Electrnoics & Communication Engg., KLEs Dr.M.S.Sheshgiri College Of Engineering and Technology, Belgaum, Karnataka, India*

Abstract *—**The Security of the information while it is being transmitted through various sources has become a major issue of concern. The basic task of information hiding can be achieved by applying the approach of steganography. The secret information which needs to be transmitted through a carrier first undergoes compression and then is encrypted into the carrier object to minimize the amount of information being transmitted and also ensures double protection. This paper aims to describes the concept of steganography and develop a data embedding and extraction technique that enables us to secretly embed data into a cover object which mainly include any form of digital media.***

Keywords-Data Hiding, Steganography, LSB coding, cover object, key file, Xilinx, MATLAB

I. INTRODUCTION

The growth of the internet technology has been enormous and depicting fast improvement thus causing a great revolution in the field of digital communication. The enormous development of variety of software and declining cost of digital devices [1] is becoming a very adaptable and feasible way for anyone globally to access and exchange the multimedia form of data. But there is always a risk involved while sending any sort of confidential data over the internet because the main concern is to protect the data from the attack of intruders and disabling them from acquiring any information unethically.

The term steganography derives its origin from the two Greek terms namely “steganos” which means “covered” and “graphy” which means “writing or drawing”. Hence steganography details methodology to camouflage the private information into other digital forms [6]. History of steganography dates back to ancient Greece where selected messengers were asked to shave their head, write a message, re-grow their hair and finally sent to convey the secret. At the recipient’s end they were supposed to shave off the re-grown hair from the head of the messengers to retrieve the secrete message. Another method was where message were written on wax covered tablets. During 1939-1945 the period of “WWII”, the method of using invisible ink to write information was used. The concept of steganography [2] is embedding private information into a digital form of media, like image, audio, or video and later transmitting it to the recipient without the knowledge of the illegal attackers and hence providing the recipient with the highly confidential information in a secretive manner.

Steganography is a process which basically involves concealing of any source of information which may be in any of the digital format such as an image, video, text or audio file into a carrier “cover” file which could also be of the similar or different digital form. Data embedding is carried out through various techniques among which LSB technique is one of the simplest of all.

The diagram shown below describes the stegaonaraghy process in a brief manner. The message object is the information which needs to be hidden is first embedded inside a cover such as an audio, text, video or an image file using various steganography methods, thus creating an embedded object called as stego object.

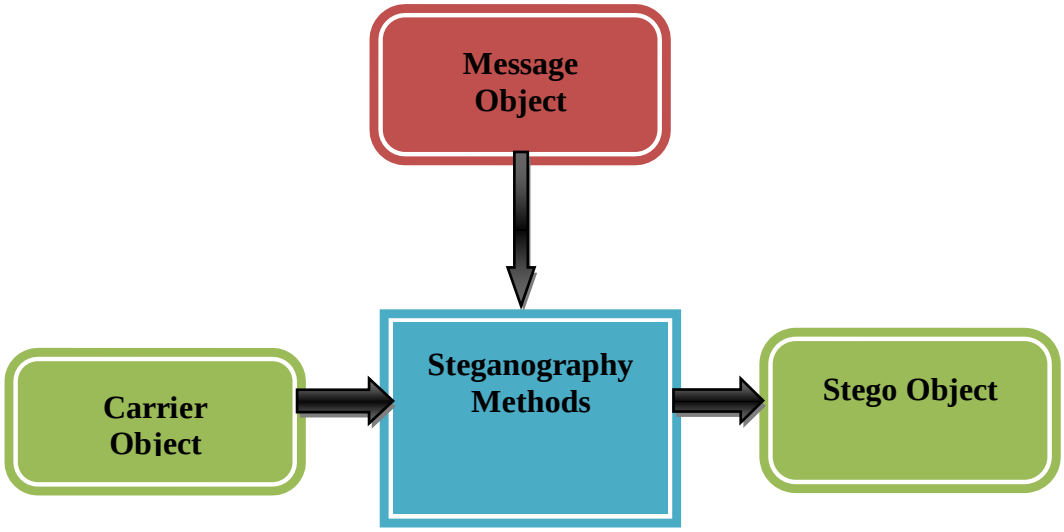

Fig 1.1 Principle of Steganography

II. LITERATURE SURVEY

Shivani et.al [2015]. "A Novel Approach of Bulk Data Hiding using Text Steganography",describes how the technique of Steganography enables the individual to maintain privacy and develop an efficient technique for it. The paper describes the art of text steganography mainly intended to camouflage information within text [1].

Venkatraman.S et al [2014] "Significance of Steganography on Data Security" describes the importance of the steganography and also enlightens the techniques that are employed. It also enlightens the problems that appear during the implementation of various steganographic algorithms [2].

Gunjan Nehru et.al [2012] "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" proposes two implementations for audio steganography i.e "genetic algorithm approach and LSB approach" is described and enlightens the area of audio steganography of embedding data within a cover which is an audio file [3].

Nithya A, Gnanasekar A K [2011] "Data Hiding in Multimedia Audio using VLSI technology"enlightens the implementation of VLSI technology which is intended here for the purpose of high data security. The paper also demonstrates how information of the textual form can be easily encrypted within an audio file by the LSB substitution method of coding and is encrypted and decrypted by Steganography algorithm [5].

III METHODOLOGY

The proposed design of steganography intends to hide a textual form of data into an audio, image and video file. The design is implemented using both MATLAB tool and a hardware description language. The diagram below shows the embedding and extraction process of the secret data. First the decoding of the digital cover which may be an audio or an image or video file is performed. Next these decoded values are stored in a format such that it is compatible with the design tools. For instance the decoded file is a .list file that is generated by running the preprocessing.m file in the MATLAB tool. This generates a testing.emb file which is the digital cover or the stego object. Next the tool allows us to extract the data from the stego object, hence differentiating it into an original and text file.

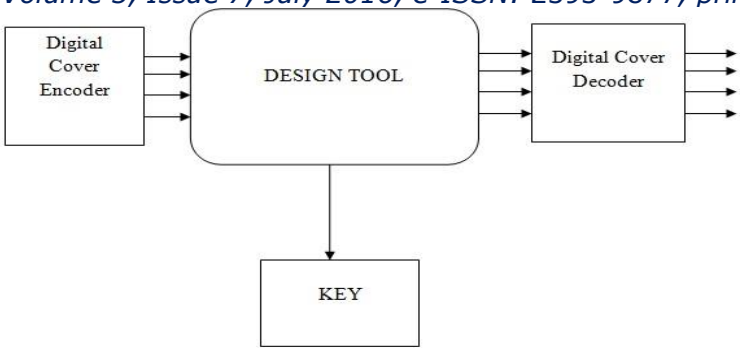

Fig 3.1Embedding process

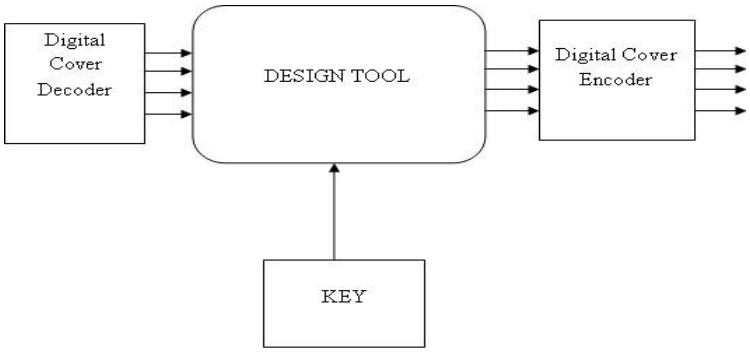

Fig 3.2 Extraction Process

The design tools used are MATLAB and Xilinx. Both the tools are used to generate a stego object also called as cover into which an input text file is embedded into and also is extracted from. Hence the proposed design thus performs the steganography technique using both MATLAB as well as the HDL.

IV RESULTS AND DISCUSSION

The below figures display the results of the proposed design. Figure 6.1(a) and Figure 6.1(b) show the audio embedding and extraction using VHDL. The hex values of the audio output and the key file are displayed. The binary values of the encoded audio input file are shown. We can observe that after embedding the key file into the audio input there is a slight alteration in the audio output due to this embedding process.

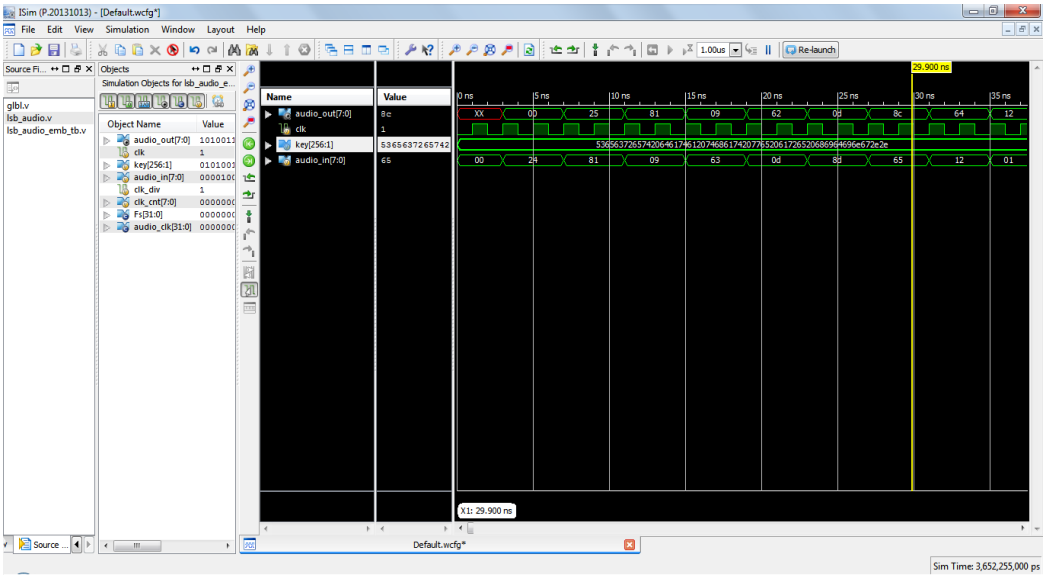

Fig 4.1Output of audio embedding

The two waveforms display the result of the audio embedding and audio extraction process. In the former result the audio input file encodes the key file which is a text document into it and thus producing an embedded object which is the audio output. In the later image, the result of extraction displays how this audio output obtained from the previous file is decoded and hence the extracted key file is shown.

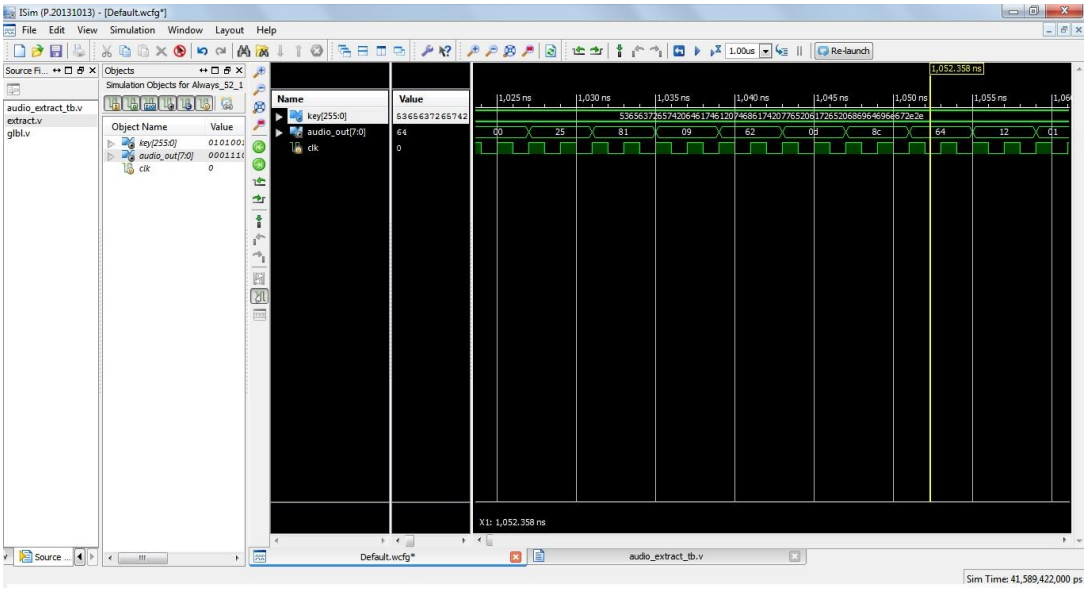

Fig 4.2 Output of audio extraction

The images below depict the simulation results obtained by image embedding and extraction.

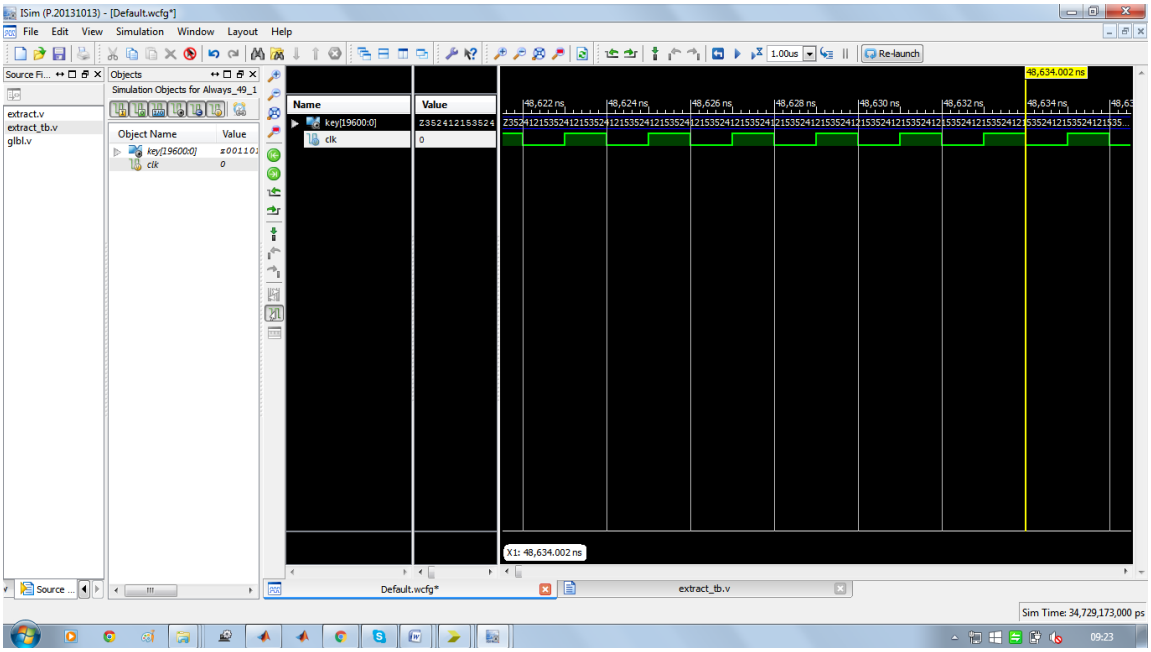

Fig 4.3 (c) Output of image embedding

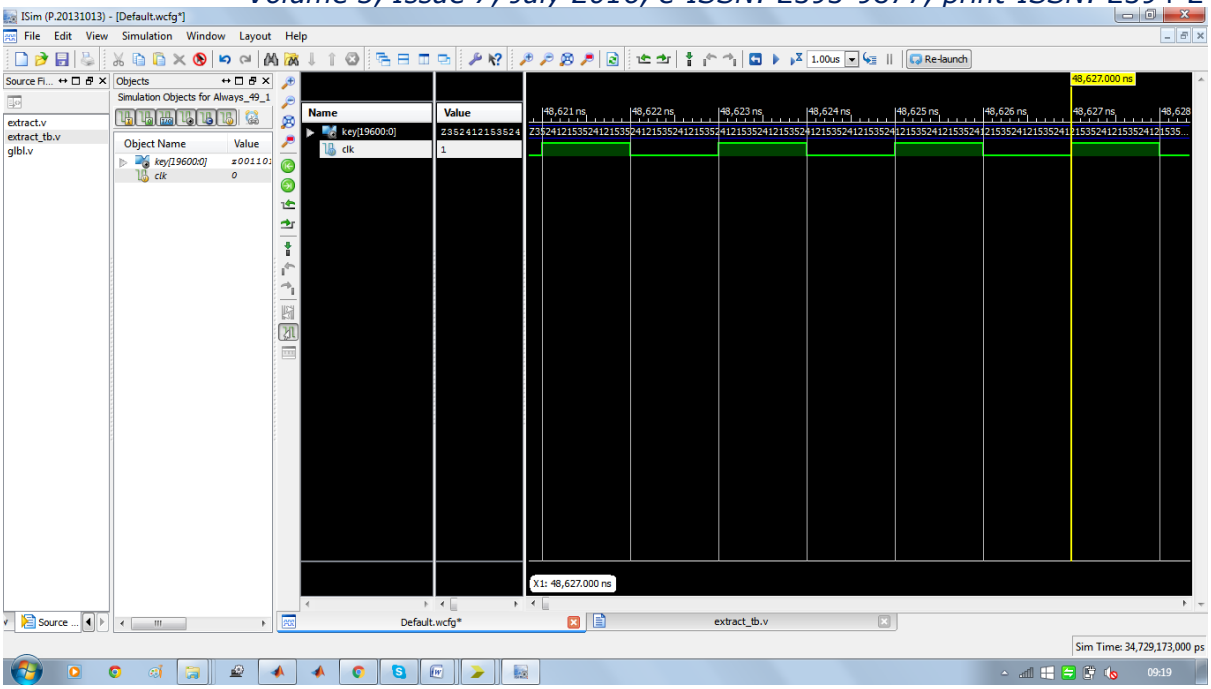

Fig 4.4 (d) Output of image extraction

V CONCLUSIONS & FUTURE SCOPE

Steganography, also known as data hiding facilitates for an efficient technique to easily embed any form of digital input file into a textual, audio, image or a video cover, thus creating a stego object which would be difficult to detect when being transmitted. The various algorithms available, makes it easier to embed and extract the data only to the authorized personnel and hence makes the transmission of highly confidential information very secure. It also helps to transmit any sort of highly confidential data through apparently undetectable cover object and hence achieves the task of concealing the existence of any secret file. Due to the advancement of easily accessible technological tools techniques such cryptography and strong encryption are also falling short. Hence this has given rise to continuous battle between the experts of data security and hackers. Steganography has gained high applications in fields like hiding data on the network private communications between peer to peer network, etc [7].

The proposed design thus enables us to implement steganography for various multimedia technologies such as audio, image and video successfully using the popular LSB technique on a Xilinx ISE platform using the Verilog Description Language. This technique is mainly intended to provide lossless embedding & extraction of the data. It also intends to reduce the overall power consumption and quantum cost of the overall implementation if implemented on a hardware platform. Now the project only intends to provide simulation results of the implemented design.

As of now the project has been designed only to hide a textual information using audio, image & video cover. However in the future attempts can be done to encrypt different kinds of multimedia information into the various multimedia forms of cover thus providing various choice ranges for the user.

REFERENCES

[1] "A Novel Approach of Bulk Data Hiding using Text Steganography", Shivania,Virendra Kumar YadavaSaumya Bathamb,3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

[2] Shouchao Song, Jie Zhang, Xin Liao, Jiao Du, Qiaoyan Wen. "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Procedia Engineering, 2011

[3] Venkatraman.S, Ajith Abraham, Marcin Paprzycki, "Significance of Steganography on Data Security", IEEE, May 2004

[4] Gunjan Nehru, Puja Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, ISSN (Online): 1694-0814

[5] Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012, ISSN : 2278 – 1021

[6] Nithya A, Gnanasekar A K, "Data Hiding in Multimedia Audio using VLSI technology", International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011, Proceedings published by International Journal of Computer Applications® (IJCA)

[7] Alan Siper, Roger Farley, Craig Lombardo, "The Rise of Steganography", Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005

[8] Xilinx, ISE In-Depth Tutorial, UG695 (v14.1) April 24, 2012

[9] "A brief introduction to MATLAB", Linear Algebra with Application to CME200, Engineering Computations M. Gerritsen, Autumn 2006, Handout 3