Hardware Efficient Image Stegnography

[1]Somshekhar R Puranmath, [2]Vishwas Patil, [3]shivaraj S T
[1]Asst.Professor, [2]Asst.Professor, [3]Programmer
[1]Electronics and communication (K.L.E Institute of Technology,Hubballi),
[2] Electronics and communication (K.L.E Institute of Technology,Hubballi)
[3] VSK University Ballari

***Abstract*—in recent years, communication has become a booming field, where each day new developments are made and security is of utmost priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Stenography is defined as the study of invisible communication. In image stenography, secret communication is achieved by embedding a message into cover image and generates a stegno image. The existing implementations have consumed more hardware and hence the area. Stenography is a branch of information hiding and its main goal is to communicate or transit the data securely in a completely undetectable manner. Literally meaning writing in a cover is the practice of hiding messages within other messages in order to conceal the existence of the original. Stenography refers to data or a file that has been concealed inside a digital image, video or audio file. Examples of its use can be found throughout history, dating as far back as ancient Greece. However, with the digital media formats in use for data exchange and communication today providing abundant hosts for Stenography communication, interest in this practice has increased. Couple this fact with the multitude of freely available, easy to use stenography software tools on the internet, the ability to exchange secret information without detection is available to virtually anyone who desires to do so, and provides unique challenges and opportunities for the security professional. This algorithm is compatible for hardware implementation on FPGA.**

***Index Terms*— stenography ,FPGA**

I. INTRODUCTION

In this modern era, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel. The security in the field of communication remains as a serious concern whenever new developments occur. Secure data transfer is the need of every time. Data hiding is a popularly used technique for secure communication. Data hiding is the technique of embedding information into digital content without causing perceptual degradation. A number of hardware and software solutions have been proposed and implemented for information security, which restrict the unauthorized access, disclosure and malicious use of personal and classified information etc. Watermarking, cryptography and Stegnography[1] are three famous techniques used in data hiding. Watermarking is the process of hiding digital information in a carrier signal, where hidden information does not need to contain a relation to the carrier signal. Digital watermarks can be used to verify the authenticity or integrity of the carrier signal and also to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Cryptography is a popularly used technique for secure communication in the presence of third parties. Cryptography was synonymous with encryption, which involve the conversion of information from a readable form to apparent nonsense. A particular decoding technique will be required to decrypt or recover the original information from an encrypted message. The source of an encrypted message shares the decoding technique only with intended recipients; thereby avoid the unauthorized or unintended third party access to the secret information. Stegnography is defined as the study of invisible communication. Stegnography is a branch of information hiding and its main goal is to communicate or transmit the data securely in a completely undetectable manner. Literally meaning writing in a cover is the practice of hiding messages within other messages in order to conceal the existence of the original. The main Hardware Efficient Image Stegnography motive of stegnography technique is to prevent detection of hidden information and thereby ensure secure information transfer. In Greek, stegnography is defined as covered writing. Stegnography technique have been employed in ancient Greek times, there exist the practice of tattooing secret message on shaved head of a messenger, and letting his hair grow before sending him through the enemy territory. However majority of the stegnography techniques have been developed and computerized stegnography usage have been started only by 2000. Batch stegnography, permutation Stegnography, least significant bit(LSB), bit plane complexity segmentation(BPCS)[2] and chaos based spread spectrum image stegnography(CSSIS) are some of the stegnography techniques used for data hiding. In image stegnography, secret communications is achieved by embedding a message into cover image and generate a stegoimage. Examples of its use can be found throughout history, dating as far back as ancient Greece. Stegnography provide priority to offer imperceptibility to human senses, whereas digital watermarking tries to control the robustness as top priority. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness.Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. However, with the digital media formats in use for data exchange and communication today, providing abundant hosts for stegnography communication, interest in

this practice has increased. Couple this fact with the multitude of freely available, easy to use stegnography software tools on the internet, the ability to exchange secret information without detection is available to virtually anyone who desires to do so, and provides unique challenges and opportunities for the security professional.

II. SYSTEM ARCHITECTURE

This chapter describes the block diagram and also various modules used in the design.

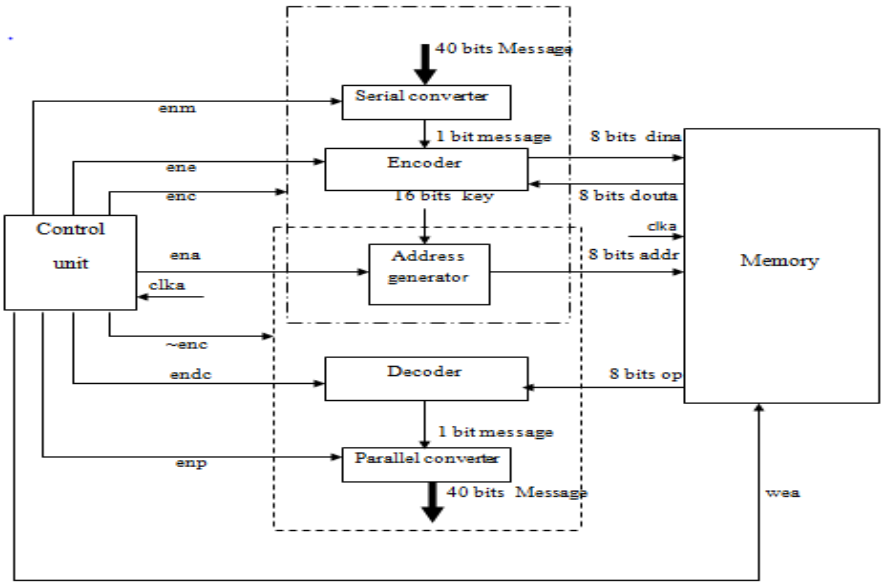

Figure2.1 Block diagram of the proposed model Hardware Efficient Image Steganography

Address Generator

This block is activated by the enable address signal (ena) by the FSM. It generates the pixel address according to the logic of random number generator. These addresses are written into the memory. The last bit of each pixel has to be embedded with the message bit.

Serial Converter

The serial converter has a 5 character message (here din) as input .In order to enable the loading of message into the converter there is a load signal .Whenever load signal is high, the message loads into the converter and when load signal is low, the 5 character message flows out of converter in bits. Also, the FSM has complete control over the serial converter. Whenever, the enable message signal is high (enm), the converter is activated.

Encoder

The bit stream from serial converter is fed as an input to encoder. Whenever the read signal (rd) is high, the pixels from the memory are fed in to the encoder. Here each bit of message is embedded into the last bit of pixel .The pixel into which the message has to be embedded is decided by the address generator. The FSM has enable encoder signal (ene) which activates the encoder. The embedded pixels are written into the memory, when write signal (wr) is high.

Decoder

Decoder is used at the receiver side to extract the secret message bits from the stego image. Encoded pixel values of the image are stored in the memory block. When the read signal is high, these pixel values are sent to the decoder. The least significant bit of each pixel is sent to the Serial to Parallel converter to combine the message bits.

Finite State Machine

In order to control entire system, a finite state machine is designed. FSM consists of eight states to embed the secret message bits into the cover image and to extract the same from the stego image. When enc signal is high, it encodes the message bits into the pixel and when enc signal is low, it decodes back and the message is retrieved back from the pixels. Encoding consists of four Hardware Efficient Image Steganography states which include address generation, parallel to serial conversion, read from memory, encode, and write in to memory. Decoding consists of three states which includes address generation, read from memory, decode and serial to parallel conversion. When reset signal is high, it will go back to initial state.

Serial to Parallel Converter

Serial to parallel converter is used at the receiver side to combine all the message bits which are extracted from the encoded pixels. The decoder extracts the message bits from the pixels and sends them to the parallel converter. When a control signal from FSM, i.e, enable parallel converter (enp) is high, parallel converter is activated and it combines the message bits one by one.

Memory Block

It is a storage block. It has pixel values with respect to the addresses. The pixel values whose last bit has to be embedded with message bits are present in memory block and the respective pixel addresses are given to memory block by the address generator. The memory block gives the pixel values to the encoder which embeds the message into pixel and the output from the encoder is again given back to the memory block. Further, the 8-bit pixel values which is embedded with message bits is given to decoder block for decoding.

III. HARDWARE IMPLEMENTATION DESIGN

Steganography means hiding the message .Our designed system represents a steganography tool which encrypts a text message in an image using a stego-key. The basic elements of an image are the pixels. Each pixel is of size 8 bits .For example 0d, ae, etc.... The pixels of the image are obtained using the MATLAB tool where only the grayscale image is used. The values of pixels obtained from the MATLAB are in the hexadecimal form. These are stored in the memory block. The message to be encrypted is of size 5 characters, each of size 8 bits. Hence, total size of the message is 40 bits. A stego-key is used to have enhanced security and thus avoid the hacking of message by the unauthorized user. This stego key is known only to the sender and the receiver. According to the block diagram figure, the system is controlled by a control unit called FSM. When enc signal is high, the message to be encrypted must be embedded inside the picture, where the message hidden is invisible to the naked eyes. The algorithm used to embed is LSB-embedding algorithm i.e., the single least bit of the pixel is replaced with the message bit. The pixel to be modified is decided by the address generator. The pixel value of the address Hardware Efficient Image Steganography.

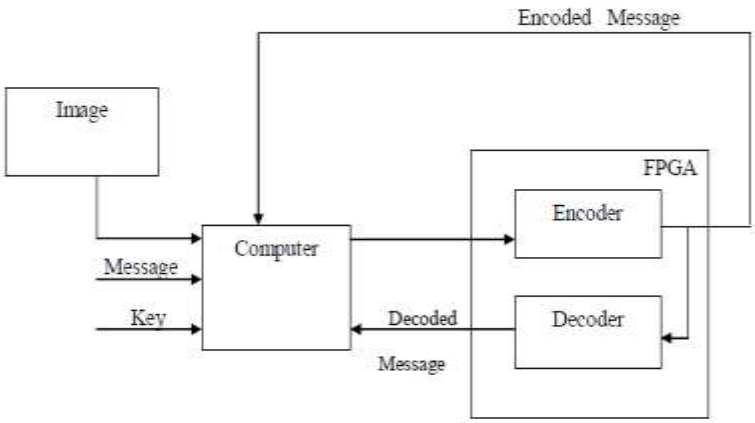

Fig3.1 working of proposed design

generated is embedded with the message bit & restored in the same address. As only one bit of pixel is getting changed, the disturbance to the image is hardly visible to the naked eyes. In order to retrieve back the message that is transmitted, a decoder is used at the receiving end from the stego image. Along with the decoder, parallel converter is also used. Encoded pixel values of the image are stored in the memory block. The control signal from the FSM, enc is set to binary 0. When the read signal is high, these pixel values are sent to the decoder. The embedded pixels are obtained from the memory and fed as an input to the decoder. The decoder takes only the last bit of pixel and transmits it to the parallel converter. Whenever the enable signal of parallel converter is high, the parallel converter is activated and takes these message bits, combines and provides a parallel output. In order to get pixels values from the image, a MATLAB code is written, where an image is converted to pixel matrix. The pixel matrix has Red, Green, Blue(RGB) values and red values are considered which are stored in co-efficient(coe) file. This file is loaded in BRAM on FPGA. Figure 3.4 depicts the pixel values obtained by considering the image in figure 3.2.

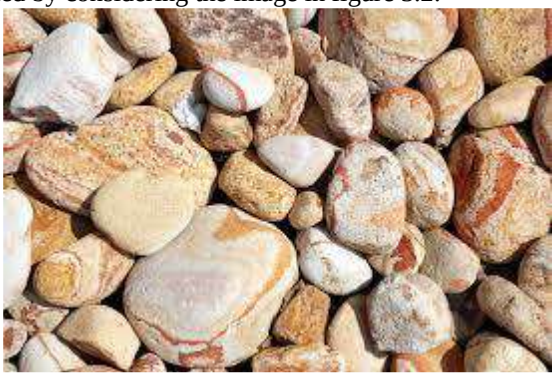

Figure 3.2: Sample image to obtain pixel values

img	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	255	158	155	171	143	255	135	191	156	180	231	146	97	171	219	233	206	145	218	188
2	217	174	172	209	139	247	135	168	180	161	186	160	98	149	237	243	183	143	209	200
3	176	192	203	236	153	223	142	140	212	161	146	187	111	133	244	242	170	151	194	208
4	187	198	246	252	218	170	168	133	237	229	172	174	156	156	205	198	208	184	178	193
5	147	200	255	255	223	167	199	129	214	255	208	142	191	198	165	169	227	201	183	190
6	104	194	240	253	185	162	223	131	171	242	235	111	198	234	137	165	221	198	199	187
7	165	164	168	220	189	200	214	152	162	172	210	113	138	210	141	209	177	162	208	158
8	202	161	162	190	182	215	223	161	141	135	203	175	123	196	145	219	145	125	204	142
9	203	176	205	180	201	232	240	169	118	139	211	255	146	198	154	206	137	100	192	146
10	156	156	209	241	215	229	216	221	132	183	202	226	150	221	198	234	175	113	188	184
11	174	151	185	227	224	233	221	244	137	197	194	175	158	244	227	227	194	120	182	225
12	254	169	146	138	223	245	255	231	136	178	189	130	173	255	231	184	183	118	175	255
13	255	215	154	119	201	236	244	228	200	201	172	140	178	223	217	174	147	137	194	246
14	255	228	178	157	186	219	233	218	237	230	184	168	205	208	194	170	145	162	185	186
15	255	193	205	239	186	198	233	201	226	254	230	197	252	204	168	169	189	182	136	90
16	255	159	190	244	153	170	238	218	240	255	233	181	207	157	169	202	193	143	129	125
17	233	143	173	220	143	163	235	234	249	248	214	162	160	122	177	231	196	90	119	179
18	179	158	172	185	185	187	217	230	240	221	183	164	157	132	182	236	217	46	89	201
19	156	187	187	157	227	193	185	209	224	217	149	172	197	175	159	219	193	64	118	190
20	148	210	201	140	255	193	160	189	210	220	127	180	236	212	137	201	164	92	151	173

Figure 3.3: Pixel values obtained from the sample image.

IV. RESULT AND ANALYSIS

The proposed system is analysed using several test cases.

Test Case 1: Here the message "abcde", is embedded in the image shown in figure 5.1.The key used to embed the message is 1254.The simulation of embedded message is as shown in figure 4.2

Figure 4.1: Image considered for test case 1

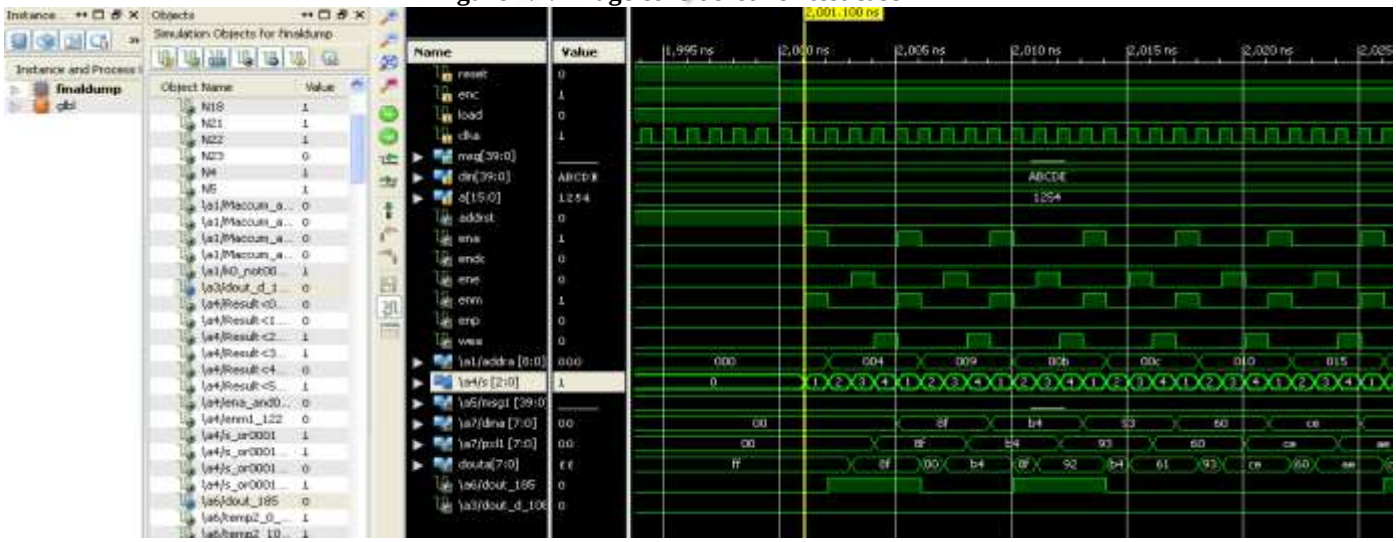

Figure 4.2: Embedding of message1

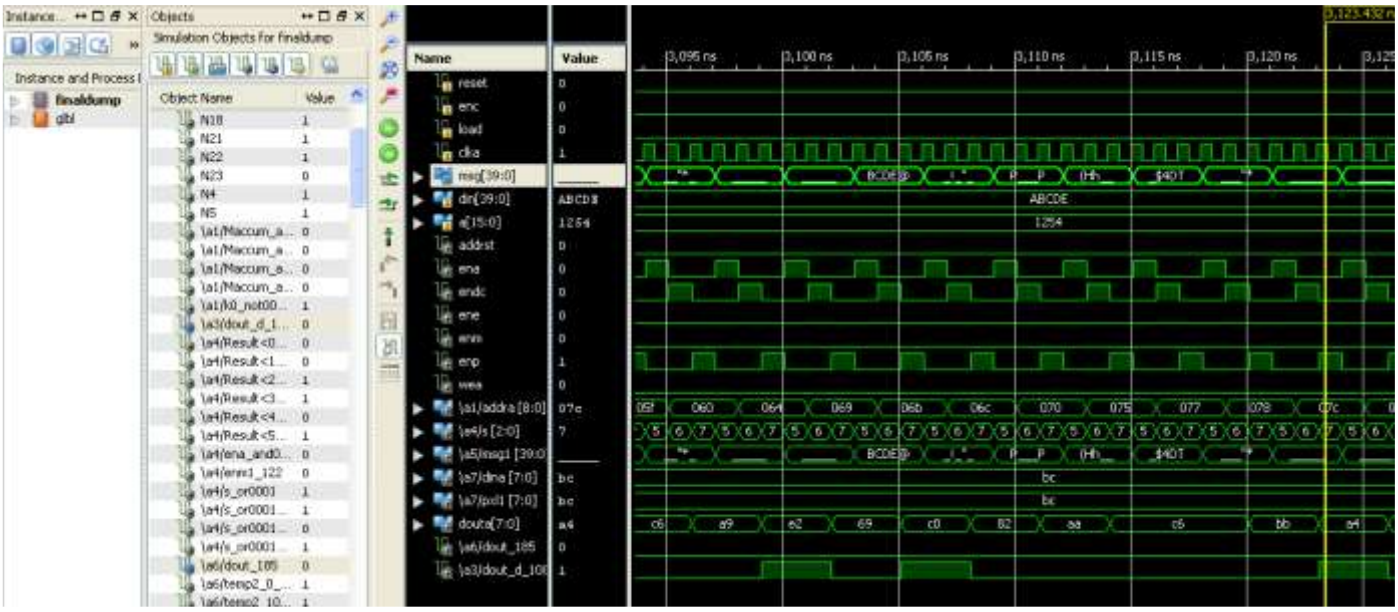

Figure 4.3: Extraction of message1

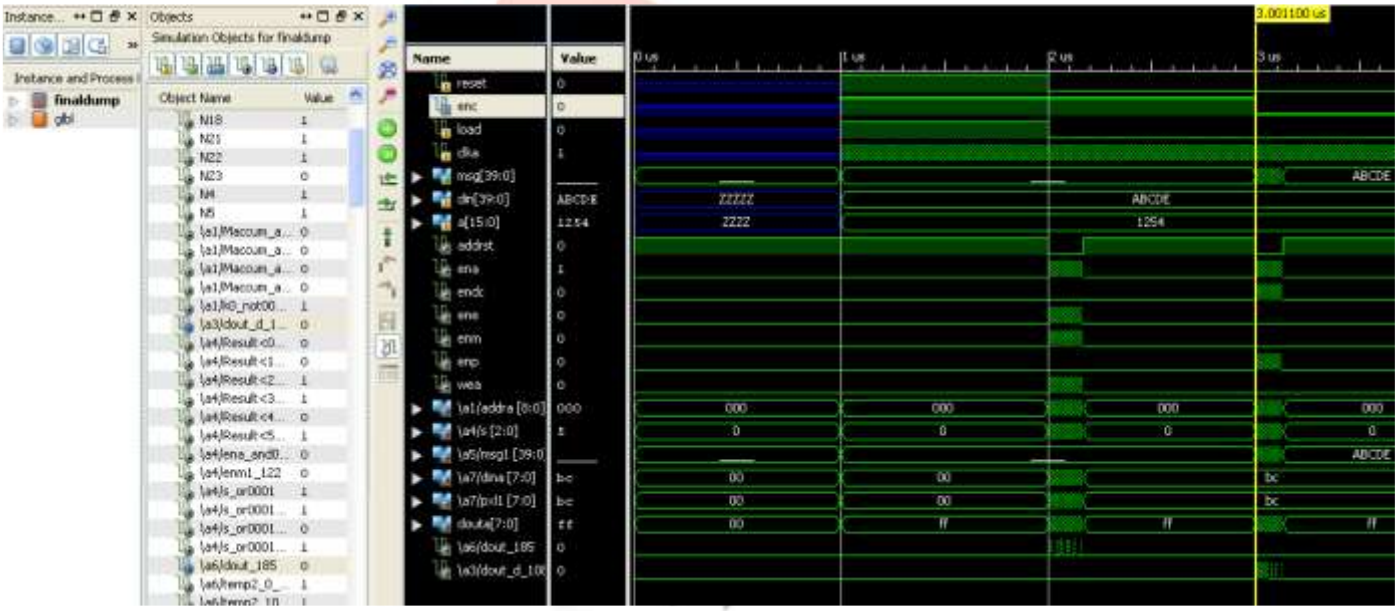

Figure 4.4: Embedding and extraction of message1

Test Case 4: Here the message "LIGHT", is embedded in the image shown in figure 5.9.The key used to embed the message is 5164. While retrieving the message a distinct key is used, i.e., 2134.Since the key to embed and retrieve is different the same message is not retrieved. The entire simulation of test case4 is shown in figure 4.6

Figure 4.5: Image considered for test case 2

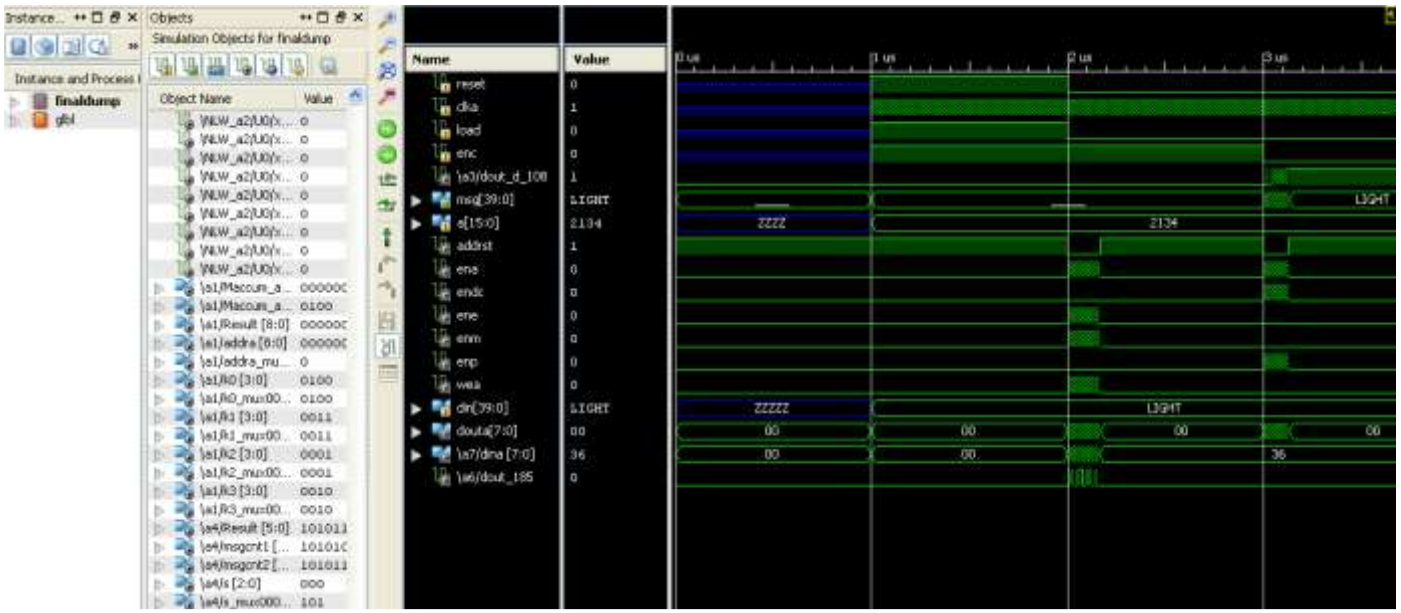

Figure 4.6: Embedding and extraction of message 2

The security in the field of communication remains as a serious concern whenever new developments occur. Secure data transfer is the need of every time. Data hiding is a popularly used technique for secure communication. Though steganography is not implemented in wider ways but it can be the best security tool. The main problem of today's world is to secure their data confidentially; the techniques used currently are not considered the best which can only be replaced by steganography.

.

REFERENCES

[1] E. A. Elshazly, Safey A. S. Abdelwahab , R. M. Fikry, S. M. Elaraby , O. Zahran, M. El-Kordy ,"FPGA Implementation of Robust Image Steganography Technique based on Least Significant Bit (LSB) in Spatial Domain", International Journal of Computer Applications (0975 – 8887) *Volume 145 – No.12*, July 2016.

[2]. Amritpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015., pp 1-4

[3]. Mrs.Manjula.Y, Mr.Jagadeesha.D.H, Dr. K.B ShivaKumar,"FPGA Implementation for Image Steganography Technique Using X-Box Mapping" , International Journal of Computer & Organization Trends –*Volume 3 Issue 6* – June 2013.

[4]. Dr. Ahlam Fadhil Mahmood, Nada Abdul Kanai, Sana Sami Mohmmad," An FPGA Implementation of Secured Steganography Communication System", Tikrit Journal of Engineering Sciences/*Vol.19/No.4*/December 2012, (14-23) .

[5]. Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar, A. M. Bagul, "Online Payment System using Steganography and Visual Cryptography" , International Journal of Computer Engineering In Research Trends, *Volume 3, Issue* 4, April-2016.

[6]. Mohammed J. Khami, Lemya G. Shehab and Zeynab M. Jawar have designed "Matlab coding for Text Steganography system by using LSB insertion method with key", *Vol.33(2),37-51, 2015*.

[7] Manoj Kumar Meena, Shiv Kumar, Neetesh Gupta have designed "Image Steganography tool using Adaptive Encoding approach to maximize Image hiding capacity", International Journal of Soft Computing and Engineering (IJSCE) *ISSN: 2231-2307,Volume-1,Issue-2*,May2011.