Arm Implementation of LSB Algorithm of Steganography

Pallavi Hemant Dixit, Uttam L. Bombale

Abstract*— Network security and protection of data have been of great concern and a subject of research over the years There are many different forms of steganography mechanisms like LSB, Masking and filtering and Transform techniques. All of them have respective strong and weak points. The Least Significant Bit (LSB) embedding Technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format. This paper explains the LSB embedding technique and Presents the evaluation for various file Formats. In a network, the success of the algorithm depends on hiding technique used to store information into the image. This paper is based on the study of steganography with its LSB algorithm. Human biometrics like iris, fingerprint, and face are the unique things for human. That's why we propose a unique authentication and encryption technique using IRIS biometric pattern of a person. Text message encrypted by cryptographic key which is generated by iris image. Then using LSB algorithm this encrypted text message hide into the iris image. LSB algorithm is implemented in ARM7 LPC2148.

***Index Terms*— iris image, steganography, LSB.**

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. it is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keep in the contents of a message secret, steganography focuses on keeping the existence of a message secret [2]. This paper intends to offer a state of the art overview of the LSB algorithms used for image steganography to illustrate the security potential of steganography for business and personal use. After the overview it briefly reflects on the introduction to embedded system used in this paper i.e. ARM. This reflection is based on a set of criteria, i.e. memory capacity. The remainder of the paper is structured as follows: Section 3 gives the reader most popular algorithm for image steganography LSB algorithm and implantation and results in section 4 and 5, In Section 6 conclusion is reached.

II. LITERATURE SURVEY

For "ARM implementation of LSB algorithm of steganography" we have gone though the following IEEE papers .

"Iris Biometric Cryptography For Identity Document"**,** this paper present an approach to generate a unique and more secure cryptographic key from iris template. The iris images are processed to produce iris template or code to be utilized for the encryption and decryption tasks. AES cryptography algorithm is employed to encrypt and decrypt the identity data. [12].

Secondly 'Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions" This paper give information about Cryptography & Steganography, This paper introduces two new methods wherein cryptography and Steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed.[13]

Next paper is "A New Image Steganography Technique" it includes various image Steganography techniques like

Text-Based Steganography, Audio Steganography, Steganography in OSI Network Model, Image Steganography etc. [14]

"Designing Of Robust Image Steganography Technique Based On LSB Insertion And Encryption" This paper discusses the design of a robust image Steganography technique based on LSB (Least Significant Bit) insertion and RSA encryption technique. Steganography is the term used to describe the hiding of data in images to avoid detection by attackers. [15]

"Multilevel Network Security Based on Iris Biometric", In this paper A novel security Mechanism is developed here for high security networks by combining IRIS biometric techniques with cryptographic and Steganography mechanisms.[16]

Manuscript published on 28 February 2013.

* Correspondence Author (s)

Ms. Pallavi Hemant Dixit*, M-Tech in Electronics, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India.

Dr. Uttam L. Bombale, PHD in, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India.

Hiding information in images is an primeval method and with the advancement digital technology paving way to many types of steganographic techniques [13].

III. OVERVIEW OF LSB ALGORITHM

A. *Image Definition*

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [3]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its color [4]. These pixels are displayed horizontally row by row. The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel [5]. The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [5]. Monochrome and grayscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey.

B. *List Significant Bit Algorithm*

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [3]. The least significant bit in other words, the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [7]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**0** 0110001**1**)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [7]. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [3].

In the above example, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key [6]. In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image.

IV. PROPOSED WORK

For security, only encryption may not be enough, hence proposed project include combination of both cryptography and Steganography. The encrypted data hide into the image and then image is transmitted in the network.

There is some weakness in hiding information in images; that is adversary could easily detect the confidential message, by noticing the noise and clarity of the image's pixels, also by observing the difference between the embedded image and the original one if it is known to him.

In the proposed project, We are using an Iris images instead of images that contain faces or natural scenes, because the only feature or data of a person that hackers cannot hack is their biometric features.

A. *Need of ARM implementation:*

- A software implementation of an Steganography scheme provides the benefits of **flexibility, speed of implementation, and lower cost** over time
- Also having Stegnography in software provides the ability to **modify product design and/or product security** without the need to make expensive changes in hardware and the potential resulting changes to the manufacturing process.
- More importantly, the NXP ARM microcontrollers feature **In Application Programming (IAP)** and the popular LPC2300 and LPC2400 series also feature Ethernet, USB and CANIAP allows customers to periodically change the security algorithm in the field whether or not the product has been comprised.
- Competitive hardware encryption cannot be updated without replacing the microcontroller, which is costly and complicated [8].

B. *Hardware Description:*

ARM7 is the leading provider of 32-bit embedded RISC microprocessors with almost 75% of the market. ARM offers a wide range of processor cores based on a common architecture, delivering high performance together with low power consumption and system cost [10][11]. ARM processors implement Load/store architecture. Depending on the processor mode, 15 general purpose registers are visible at a time. Almost all ARM instructions can be executed conditionally on the value of the ALU status flags. Load and store instructions can load or store a 32-bit word or an 8-bit unsigned byte from memory to a register or from a register to memory. The ARM arithmetic logic unit has a 32-bit barrel shifter that is capable of shift and rotates operations. The second operand to all ARM data-processing and single register data transfer instructions can be shifted before data processing or data transfer is executed, as part of the instruction.

When the shift amount is specified in the instruction, it may take any value from 0 to 31, without incurring any penalty in the instruction cycle time. LPC2148 contain 32K of RAM, so We divide 16k for Image storage and 16K for text and key.

For wireless transmission between two ARM kit, the ZigBee protocol is used. ZigBee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless M2M networks. The ZigBee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz[9].

C. Choice of development environment:

The obvious choice for an integrated development environment was Keil's mVision4 IDE, because of its excellent debugger and the availability of a free evaluation version. For making GUI, we used visual basic 6.0 software.

D. Experimental Block Diagram

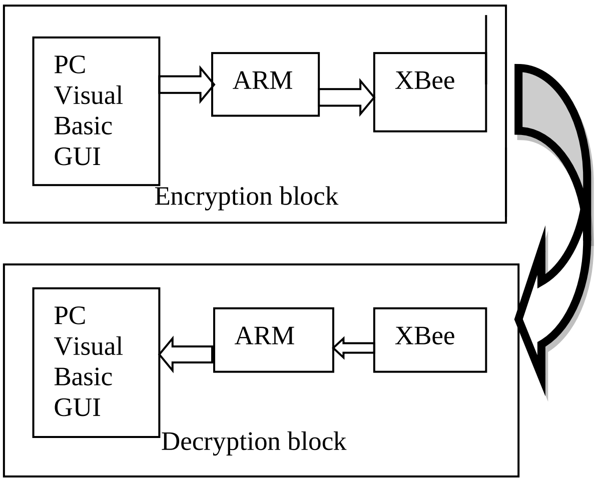


Figure 2: Blocks and internal connection

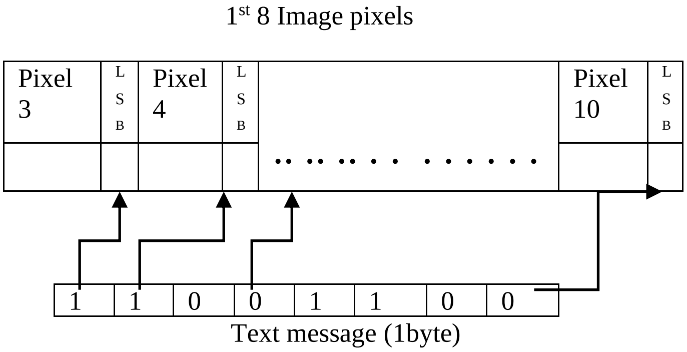
Step involving in transmission of document

1. Generate a Secrete key from the Iris image of user using Steganography
2. Use this generated key, and encrypt document as a cipher text, this process of encryption is called cryptography. Generated Key + Document or private file = Encrypted Document (Cryptography)
3. Then, the encrypted document hides in image of user using Steganography algorithm LSB.
   Image + Encrypted document = Image (Steganography)
4. Send this image to its destination though the network using zigbee.
5. Reverse process takes place at the receiver side.

V. DESIGN METHODOLOGY

LPC2148 contain 32k RAM, we use 16k for image storage and 16K for text. Here image storage take place in such a way that last pixel is stored in 1st memory location in ARM, then second last pixel in 2nd memory location and so on. We consider sequence of pixel from a pixel stored in 1st memory location. So first two pixels include text size. We start encoding of text from pixel stored in 3rd memory location.

In figure shown below contain iris image pixels from 3 to 10 Pixel 1 and 2 are used to store text size to be encoded. One byte of text is stored in LSB of pixels 3 to 10.



Algorithm Step:

1. Made image buffer and text buffer
2. Consider first 8 bit of text buffer and 8 pixels from image buffer.
3. Used shift operator to select LSB of Single Pixel then performed following logic.

```
If (Pixel_LSB_bit == text_bit)
  Pixel_LSB_bit = (Pixel_LSB_bit) OR (text_bit)
Else
  Pixel_LSB_bit = (Pixel_LSB_bit) AND (text_bit)
End
```

VI. EXPERIMENTAL RESULT

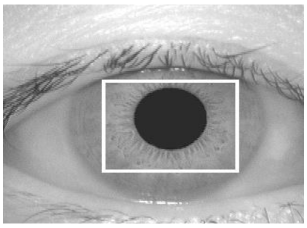


Figure 2. Eye Image

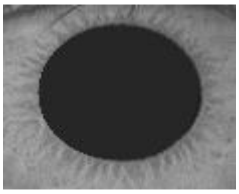
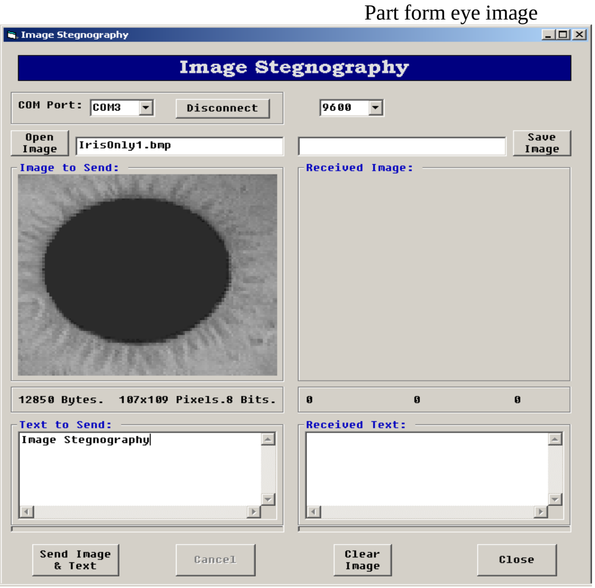


Figure 3. Taking Iris Part form eye image



COM Port: COM3
9600
IrisOnly1.bmp
12850 Bytes. 107x109 Pixels.8 Bits.
0 0 0
Text to Send: Image Stegnography

Figure 4 GUI for image steganography

In Figure 4 and 5, we design GUI for image Steganography. This GUI design take place in Visual Basic 6.0 which is very simple and user friendly software to design GUI. In this GUI, we can take an image file which you want to use in communication. We can also see the size of image. Then we can write text which is encoded in image.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

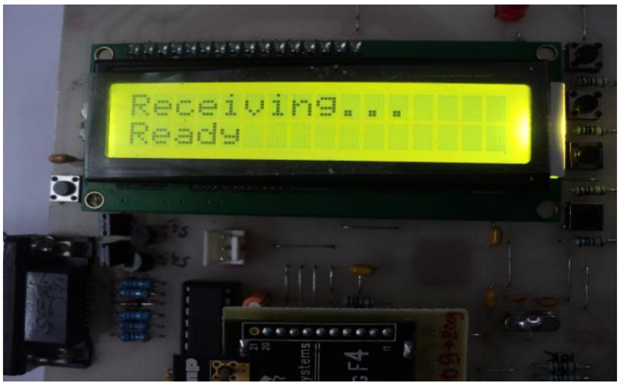
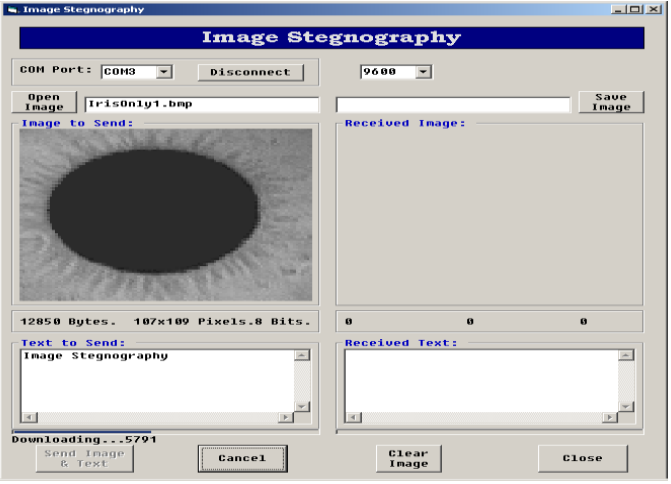


Figure 5: Data from PC to ARM. “Receiving status”



COM Port: COM3 9600

IrisOnly1.bmp

12850 Bytes. 107x109 Pixels.8 Bits.

0 0 0

Text to Send: Image Stegnography

Downloading...5791

Figure 6. Encoding status

This GUI made in Visual basic 6, Iris image of 16kb consider for stego image. Text massage “Image steganography” encoded into image and this image send to receiver.

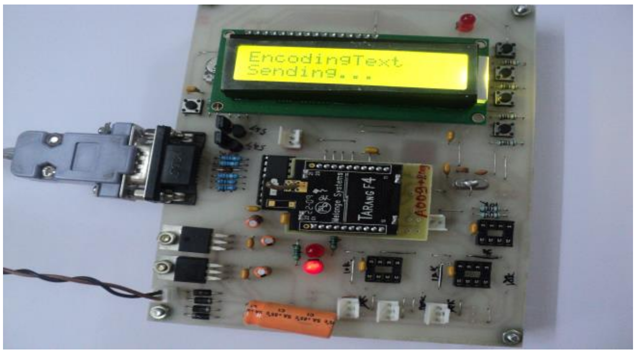


Figure 7: encoding text sends to Zigbee

As in figure, this Kit includes LPC2148 ARM Controller. LCD having 16*2 character interfaced to controller. UART0 and UART1 used for serial communication. Here we use UART0 for PC Communication and UART1 for ZigBee interfacing. All Programming is done in Keil uVersion 4. We send Text + Iris Image from Pc to Controller. In this Diagram, it means it receive frame of text and image from PC. When Controller receives all date send by PC then he start sending to next receiver through ZigBee. Similarly decoding process take place at receiver side. Stego image received by Zigbee, then it send to controller, then controller decode text from iris image and transmit to PC.

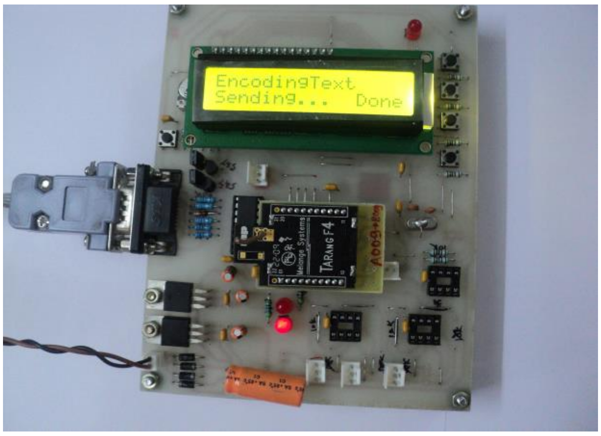


Figure 8: sending is done

VII. CONCLUSION

From above result it is possible to send text message from iris image using LSB algorithm. It can be used to send data on network secure. A software implementation of a Steganography scheme provides the benefits of **flexibility, speed of implementation, and lower cost** over time.

Also having Steganography in software provides the ability to **modify product design and/or product security** without the need to make expensive changes in hardware and the potential resulting changes to the manufacturing process.

REFERENCES

[1] Moerland, T., “Steganography and Steganalysis”, Leiden *Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf.,

[2] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM*, 47:10, October 2004

[3] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, *Computer Journal*,February 1998

[4] Owens, M., “A discussion of covert channels and steganography”, *SANS Institute*, 2002

[5] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, *IEEE Journal of selected Areas in Communications*, May 1998

[6] Krenn, R., “Steganography and Steganalysis”, http://www.krenn.nl/univ/cry/steg/article.pdf

[7] NXP & Security Innovation Encryption for ARM MCUs ppt,

[8] ‘UM10139 LPC214x User manual’ pdf.

[9] B. Gladman. A Speci cation for Rijndael, the AES Algorithm. Available at http://fp.gladman.plus.com, May 2002

[10] G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti and S.Marchesin, “Efficient Software Implementation of AES on 32-bit Platforms,” *CHES 2002, LNCS 2523*, pp. 159–171, 2003.

[11] Intel Strong ARM SA-1110 Microprocessor. Developer's Manual 278240-003, Intel Corporation, Jun 2000.

[12] Sim Hiew Moi, Nazeema Binti Abdul Rahim,Puteh Saad, Pang Li Sim, Zalmiyah Zakaria,Subariah Ibrahim,“Iris Biometric Cryptography for Identity Document”, 2009 International Conference of Soft Computing and Pattern Recognition.

[13] Sujay Narayana1and Gaurav Prasad” Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions” Signal & Image Processing: An International Journal (SIPIJ) Vol.1, No.2, December 2010

[14] Hassan Mathkour , Batool Al-Sadoon, Ameur Touir ” A New Image Steganography Technique”

[15] Mamta Juneja 1, Parvinder Singh Sandhu2 “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption” 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[16] V.V.Satyanrayanarayana Tallapragada , Dr. E.G.Rajan, “Multilevel Network Security Based on Iris Biometric” 2010 International Conference on Advances in Computer Engineering.

[17] http://www.casia.com/iresdatabase

Ms. Pallavi Hemant Dixit did her B.E (E&TC) from Shivaji University, Kolhapur in the year 2008. She is pursuing her M-TECH (Electronics) from Department of Technology, Shivaji University, and Kolhapur. She has a total of 04 years of experience in teaching. She has presented 2 papers in National Conferences. She has attended number of workshops on various subjects.

Prof. Dr. U.L Bombale Has received PhD from Dhirubhai Ambani Institute of Information & Communication Technology, (DA-IICT) Gandhinagar, Gujarat, India, under the guidance of Dr. Sanjeev gupta. M.E in Electronics & Telecommunication in 1994 from COE, Pune, and Currently he is working as a Professor in Dept. of Technology ,Shivaji university, Kolhapur (India). Ph.No-+919049274380