ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

ARM Controller Based Image Steganography Using LSB Algorithm

Pallavi Sunil Narule[1], Neha Dnyandev Patil[2], Priyanka Subhash Kurade[3], P.D.Patil[4], J.M.Waykule[5]

Electronics and Telecommunication Department, Sanjay Ghodawat Institutes, Atigre[1,2,3]

Assistant Professor, Electronics and Telecommunication Department, Sanjay Ghodawat Institutes, Atigre[5]

Abstract: Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopted. Embedding secret information inside images requires intensive computations and therefore designing Steganography in hardware speeds up Steganography. This is implemented using ARM7TDMI processor. 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. 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. The Least Significant Bit 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.

Keywords: Steganography, LSB Algorithm.

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. Steganography 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. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1] defining it as "covered writing". In image steganography the information is hidden exclusively in images.

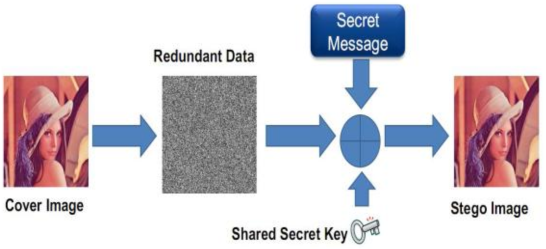


Fig.1

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

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.

II. LITERATURE SURVEY

For "ARM implementation of LSB algorithm of steganography we have gone through the following ieee paper "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. [3].

"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. [4]

DOI 10.17148/IJARCCE.2015.4431

III. OVERVIEW OF STEGANOGRAPHY

To provide an overview of steganography, terms and concepts should first be explained. An overview of the different kinds of steganography is given at a later stage.

3.1 Steganography concepts

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [5], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [6].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [7].

3.2 Types of key

- PURE
- PUBLIC
- PRIVATE

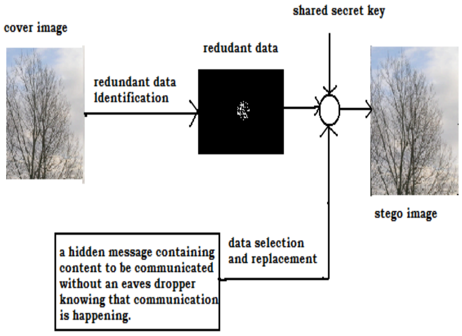


Fig. 2

IV. IMAGE STEGANOGRAPHY

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

4.1 Image definition

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [12]. 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 colour [13]. 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 [14]. The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [14]. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour [14]. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits [12]. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours [14]. Not surprisingly the larger amount of colours that can be displayed, the larger the file size [13].

V. TYPES OF ALGORITHM

- There are two trends to implement steganographic algorithms:

1. Transform domain:

Steganography in the transform domain involves the manipulation of algorithms and image transforms.

2. Image domain**:-**

In image domain technique the bits of the pixels of images are modified according to the data to be inserted.

The algorithms that work in the spatial domain are simpler and faster. Here the algorithms are more robust, that is, more resistant to attacks.

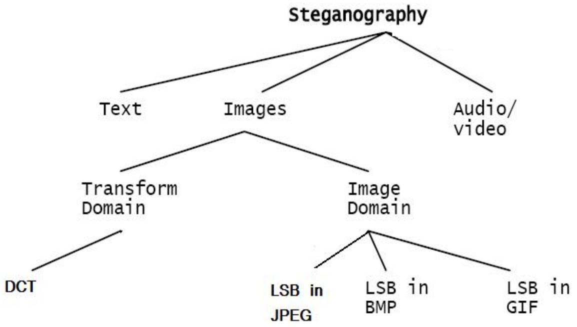


Fig.3

5.1 Least significant bit algorithm

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [12]. 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 [16]. 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)

DOI 10.17148/IJARCCE.2015.4431

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:
(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

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 [16]. 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 [12].

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 [15].

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.

5.2 ALGORITHM OF PROPOSED METHOD

5.2.1 Algorithm to embed message

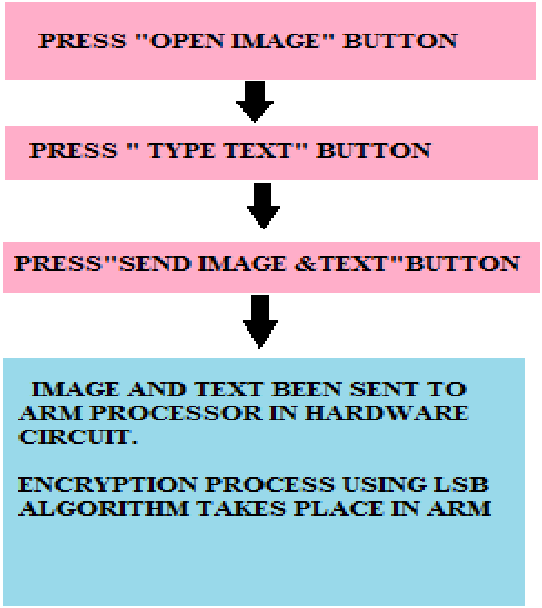

PRESS "OPEN IMAGE" BUTTON
PRESS " TYPE TEXT" BUTTON
PRESS"SEND IMAGE &TEXT"BUTTON
IMAGE AND TEXT BEEN SENT TO ARM PROCESSOR IN HARDWARE CIRCUIT.
ENCRYPTION PROCESS USING LSB ALGORITHM TAKES PLACE IN ARM

Fig.4

5.1.2 Algorithm to retrieve message

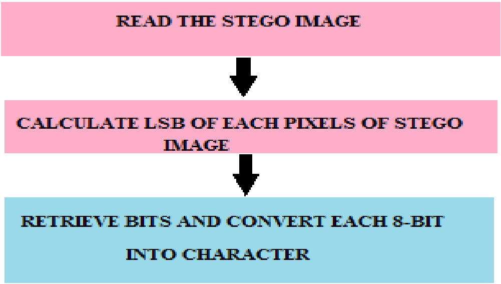

READ THE STEGO IMAGE
CALCULATE LSB OF EACH PIXELS OF STEGO IMAGE
RETRIEVE BITS AND CONVERT EACH 8-BIT INTO CHARACTER

Fig.5

VI. IMPLEMENTATION DETAILS

6.1 Hardware Implementation

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].

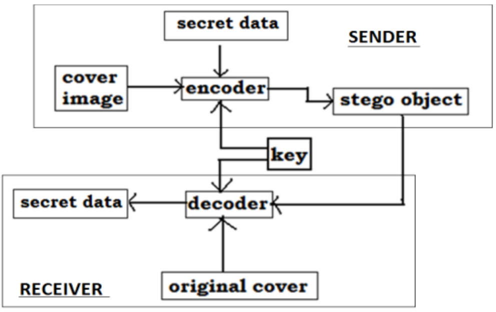


Fig. 6. Block diagram of the system

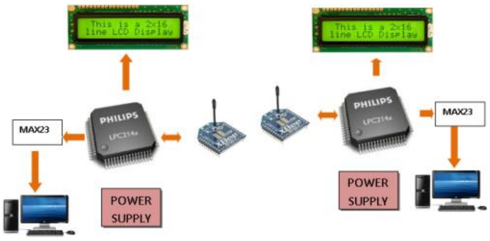
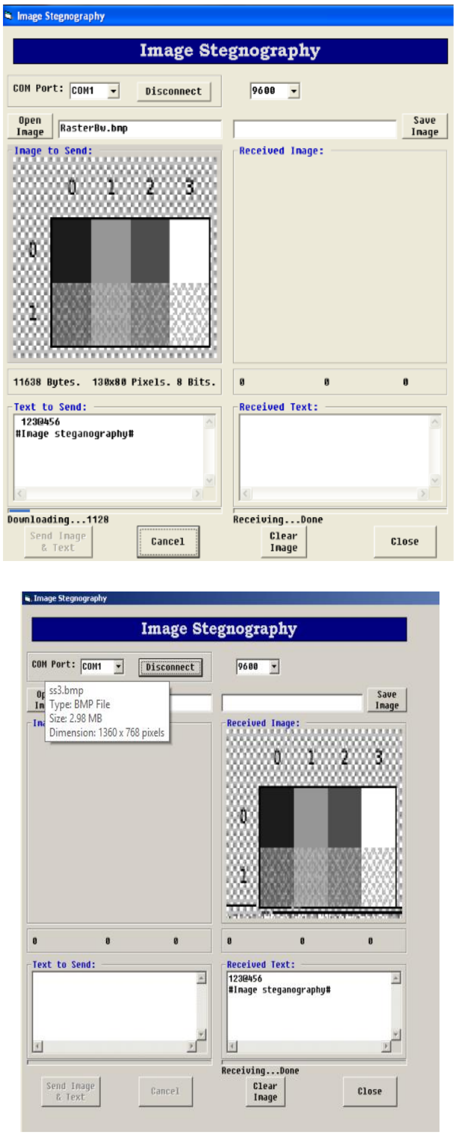

This is a 2x16 line LCD Display
This is a 2x16 line LCD Display
PHILIPS
PHILIPS
MAX23
MAX23
POWER SUPPLY
POWER SUPPLY

Fig. 7. EXPERIMENTAL SETUP

VII. RESULTS

The designed system is a half duplex circuitry which can be used for transmission of secret message. To keep the data intact we have made use of lsb algorithm. Experimental results shows by using Zigbee for wireless transmission the maximum coverage area is restricted to about 100m.Since it is a half duplex system, only one machine can send the data at one time. The other machine i.e receiver has to wait until transmitter has completed its sending process, same is applicable for vice-versa. Below are some snapshot taken during run-time process of the system.



COM Port: COM1 9600

RasterBw.bmp

11638 Bytes. 130x80 Pixels. 8 Bits.

0 0 0

1230456
#Image steganography#

Downloading...1128

Receiving...Done

COM Port: COM1 9600

ss3.bmp
Type: BMP File
Size: 2.98 MB
Dimension: 1360 x 768 pixels

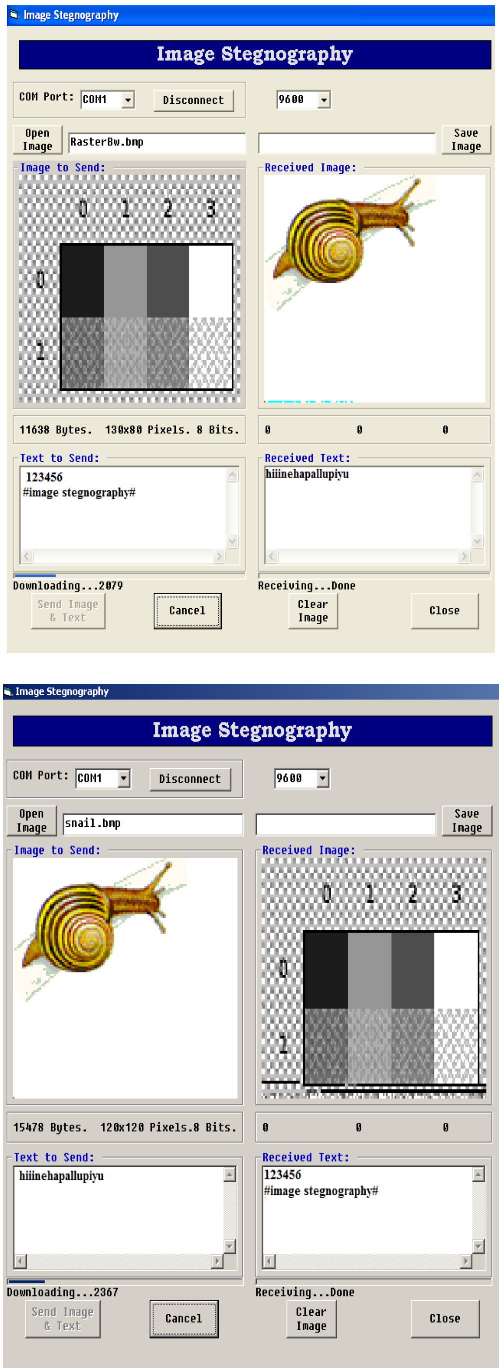
0 0 0

0 0 0

123@456
#Image steganography#

Receiving...Done

Fig.8 Sending and Receiving of stego image



COM Port: COM1 9600

RasterBw.bmp

11638 Bytes. 130x80 Pixels. 8 Bits.

0 0 0

123456
#image stegnography#

hiiinehapallupiyu

Downloading...2079

Receiving...Done

COM Port: COM1 9600

snail.bmp

15478 Bytes. 120x120 Pixels.8 Bits.

0 0 0

hiiinehapallupiyu

123456
#image stegnography#

Downloading...2367

Receiving...Done

Fig.9 Half-duplex operation sending and receiving

VIII. CONCLUSION

E-mailing is not completely secret communication method because sending and receiving action can be noticed by third party. Also in communication there are hacking problems which reduced confidentiality of communication to overcome such problems steganography technique is advantageous.

Attaching a ‘stego’ file to an e-mail message is simplest example in hiding the existence of confidential data, the data can be image or audio file. In our project we have successfully done the secret communication by attaching a stego file to an E-mail message.

DOI 10.17148/IJARCCE.2015.4431

REFERENCES

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

[2]. Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001

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

[4]. 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.

[5]. Simmons, G., “The prisoners problem and the subliminal channel”, CRYPTO, 1983

[6]. Chandramouli, R., Kharrazi, M. & Memon, N., “Image steganography and steganalysis: Concepts and Practice”, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

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

[8]. Currie, D.L. & Irvine, C.E. ,“Surmounting the effects of lossy compression on Steganography”,19th National Information SystemsSecurityConference,1996

[9]. Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001

[10]. Handel, T. & Sandford, M., “Hiding data in the OSI network model”, Proceedings of the 1 st International Workshop on Information Hiding, June 1996

[11]. Ahsan, K. & Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002

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

[13]. “Reference guide: Graphics Technical Options and Decisions”, http://www.devx.com/projectcool/Article/19997

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

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

[16]. NXP & Security Innovation Encryption for ARM MCUs ppt.

DOI 10.17148/IJARCCE.2015.4431