Proceedings of 1st Shri Chhatrapati Shivaji Maharaj QIP Conference on Engineering Innovations
Organized by Shri. Chhatrapati Shivaji Maharaj College of Engineering, Nepti, Ahmednagar
In Association with JournalNX - A Multidisciplinary Peer Reviewed Journal, ISSN No: 2581-4230
21st - 22nd February, 2018

STEGANOGRAPHY BASED ON EMBEDDED SYSTEM

Chaudhari Pallavi,

Dhadge Snehal,

Rajale Aishwarya

Abstract—Steganography is method dealing with writing hidden messages in a specific path that only the sender and the receiver are able to decrypt. Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices. This project work mainly focuses on the implementation of a steganographic algorithm on embedded devices like ARM, PIC or any equivalent embedded device.

The advantage of FPGA for steganography is speed, a FPGA being able to execute steganographic algorithms more faster than other devices. The disadvantage in using an FPGA is cost, making them impossible to be used in small devices like mobile phones etc. The objective of our project work is to implement steganographic algorithms like the LSB algorithm on embedded system like using ARM, PIC or any equivalent mobile or embedded devices without significantly raising their price.

The main purpose of implementing such an algorithm on a microcontroller is to bring steganography and its advantages on low and medium cost mobile and dedicated devices.

Keywords — steganography, concealing, embedded, mobility.

1. INTRODUCTION

Steganography is a method of concealing a file, message, image, or video within another file, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected," and graphein meaning "writing". The first recorded use of the steganography was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message will be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a sharedsecret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoff's principle. incriminating in themselves in countries in which encryption is illegal. In cryptography their is preventing the contents of a message only, steganography is interested with concealing the fact that a secret message is being sent as well as concealing the contents of the message. Steganography include keeping secrete information within computer files. Steganographic coding inside of a transport layer, such as a document file, image file, program or protocol may include in digital steganography of electronic communication. Ideally, media files are steganographic transmission because of their large size. For example, a sender may be start with an undamaging image file and adjust the colour of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

2. RELATED WORK

As shown below significant steps have been made in bringing steganography on dedicated devices using FPGAs. The major advantage of using a FPGA for steganography is speed, a FPGA being able to execute steganographic algorithms much faster than other devices. The disadvantage in using an FPGA is cost, making them impossible to be used in mobile phones for example. This paper tries to enlarge the possibilities of using steganographic algorithms. The main concern of this paper is to bring steganographic algorithms like the LSB algorithm on mobile and embedded devices without significantly rising their price. One possible solution presented here is using microcontrollers for hosting and executing a steganographic algorithm. The hardware used consists of the Olimex LPC-H2294 development board. The board's main components that were used in the implementation are: an ARM7 based microcontroller unit (NXP Phillips LPC-2294), 1 MB (256 K x 32 bit) 12 ns 71V416 SRAM.

The main advantage of steganography over cryptography is that the encrypt message does not focus to itself as an object. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may be

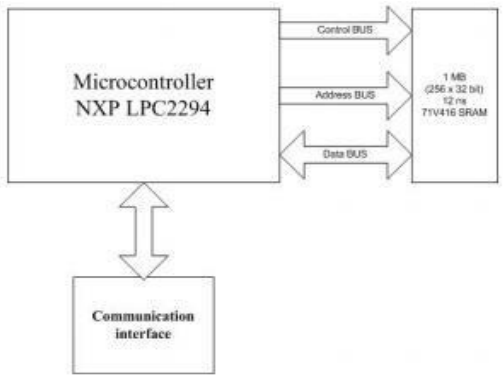

Figure 1. Brief system schematic

ARM7TDMI-S based microcontroller has 256 KB of embedded high speed flash memory having more variety of peripheral interfaces. The ARM architecture is based on Reduced Instruction Sets Computer (RISC) principles. Microprocessor or microcontroller has characteristics that ARM architecture is simplicity resulting in high speed and has high instruction throughput. Also pipeline techniques are present within the architecture making sure that all parts of the processing and memory systems can operate continuously. The Phillips LPC-2294 microcontroller also has an EMC module (external memory controller) allowing it to be connected with external memory through a dedicated address and data busses. The EMC unit has an important feature that to allow the external memory to be transparent for the embedded programmer. The Olimex LPC-H2294 development board also consists of a JTAG debugging interface.

3. IMPLEMENTATION DETAILS

The algorithm of embedded devices on steganography implementation was mainly focused on the procedures regarding the decoding an encrypted image within a carrier image. The first step in the implementation of the decoding steganography algorithms was designing a proper memory organization. The size of the images that needed to be stored and processed is the main aspects that were considered during the memory organization process were influenced by The Phillips LPC-H2294 microcontroller disposes of internal RAM memory containing only 16 KB of memory. For storing the image needed to be decoded the amount of RAM memory contained is insufficient. Another memory is contained within the microcontroller is 256 KB of internal FLASH memory, that insufficient for storing the image, most part of the memory being used by the code and, being a FLASH memory, it is low on speed, making decoding a large time consuming process.

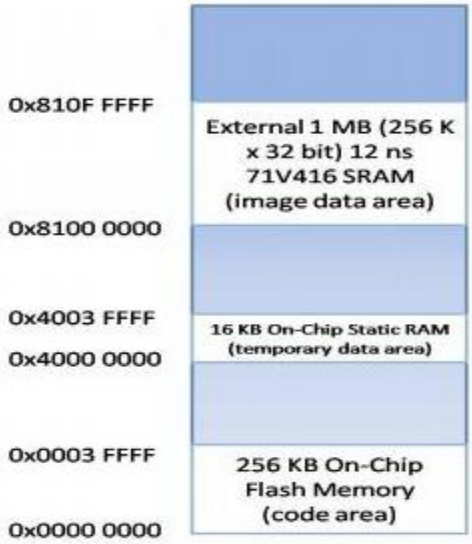

Figure2.Embedded system memory map

The steganographic algorithm that was implemented on the device is the LSB algorithm. The process of adjusting the least significant bit pixels of the carrier image is the LSB (Least Significant Bit) substitution. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. The 8 bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. The compression in BMP is lossless therefore LSB is an effective in using BMP images. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats. The problem can be avoided by only using for GIF formats, but problem with the GIF image is whenever the least significant bit is changed the whole colour palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect. For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images. For hiding the data within an image there are many approaches available: least significant bit submission approache is “Optimum Pixel Adjustment Procedure. The simple algorithm for OPA explains the procedure of hiding the sample text in an image.

Step1: A few least significant bits (LSB) are substituted with in data to be hidden.

Step2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.

Step3: Let n LSBs be substituted in each pixel.

Step4: Let d= decimal value of the pixel after the substitution.d1 = decimal value of last n bits of the pixel.d2
= decimal value of n bits hidden in that pixel.

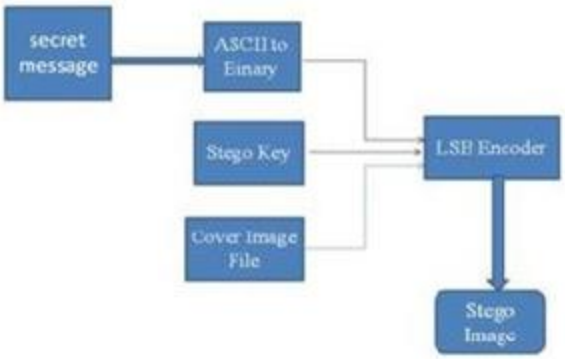

Figure3:LSB insertion mechanism

Step5: If (d1~d2)<=(2^n)/2then no adjustment is made in that pixel else.

Step6: If (d1<d2)d =

d-2n. If (d1>d2)d = d
+ 2^n.

This "d" is converted to binary and written back to pixel. This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.

Figure 5. Stego Image

The images shown above in Fig. 4 represent the payload (Fig b) to be hidden within the carrier image in Fig4.a. After the encrypting, when algorithm was applied on the two images then above third image was generated, that image containing the payload hidden within the carrier ,i.e."stego image".

A)

B)

FIGURE 4. A) CARRIER IMAGE
B) PAYLOAD IMAGE

4. CONCLUSION:

The proposed project work focuses on using microcontrollers or microprocessors for executing the steganographic algorithms instead of using Field Programmable Gate Arrays to achieve the cost benefits. First result shows how the steganography works for analysis using LSB method. As we have stated earlier that the LSB steganolysis is done by changing the least significant bits of image pixel.

5. REFERENCES:

1) Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "a secure and high capacity image Steganography technique" Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013. [2]DipeshAgrawal, SamidhaDiwedi Sharma, "Analysis of Random Bit Image Steganography Techniques" International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology – 2013.
2) GowthamDhanarasi and Dr .A. Mallikarjuna Prasad," image steganography using block complexity analysis" , International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.07 July 2012.
3) Siddharth Singh and Tanveer J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for DataHiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
4) Rahul Jain and Nareshkumar, "Efficient data hiding scheme using lossless data compression and image steganography ", International Journal of Engineering Science and Technology (IJEST) , Vol. 4 No.08 August 2012.
5) Neeta, D.; Snehal, K.; Jacobs, D., "Implementation of LSBSteganography and Its Evaluation for Various Bits", DigitalInformation Management, 2006 1st International Conference onVolume, Issue, 6-6 Dec. 2006 Page(s): 173 – 178Digital Object Identifier 10.1109/ICDIM.2007.369349.
6) Phillips Semiconductors, "LPC2119 /2129/ 2194/2292/2294 UserManual", May 2004.
7) JózsefLenti, "Steganographic methods", Department of Control Engineering and Information Technology, Budapest University of Technology and Economics, H-1521, Budapest, Hungary, June 2000, pp. 249-258.
8) H.A. Farouk and M. Saeb, "Design and implementation of a secretkeysteganographic micro-architecture employing FPGA,"Proceedings of the 2004 conference on Asia South Pacific designautomation: electronic design and solution fair, Yokohama,Japan: IEEE Press, 2004, pp. 577-578.
9) Neil F. Johnson, SushilJajodia, "Exploring Steganography: Seeing the Unseen", IEEE COMPUTER, vol. 31, 1998, pp. 26—34.
10) D. Gruhl, W. Bender, A. Lu, "Echo hiding", in Information hiding: First International Workshop, R.J. Anderson, Ed. Vol.1174 of Lecture Notes in Computer Science, Isaac Newton.
11) ARM ARM7TDMI-S (Rev 4), "Technical Reference Manual".
12) J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," Selected Areas in Communications, IEEE Journal on, vol. 13, 1995, pp. 1495- 1504.