Steganographic Secure Data Communication – A Hardware Approach

[1]Mrs.A.N.Naik-
Lecturer SIT, Polytechnic

[2]Prof.R.T.Patil
(Associate Professor,R.I.T Sakhrale)

[3] N.B.Naik
Lecturer SIT, Polytechnic

Abstract-Steganography is a science dealing with writing hidden messages in a particular way that only the sender & the intended recipient are able to decipher so as to provide security in open environment like internet. Steganography attempts to hide the very existence of the message and make communication undetectable. Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices. This paper focuses on the implementation of a steganographic algorithm on embedded devices –microcontrollers. Furthermore, this article presents experimental results obtained from testing a steganographic algorithm on embedded devices. The main purpose of implementing such an algorithm on a microcontroller is to provide security on low and medium cost mobile and other dedicated devices [1].

1. Introduction

Nowadays, an important aspect of the modern way of life is *communication*. Many devices present today have the ability to transmit various information between themselves using different ways of communication, like insecure public networks, different types of wireless networks and the most used: the Internet. In some cases it is needed to keep the information travelling through different kinds of channels secret.
Mainly there are two ways of concealing information: cryptography and steganography.
Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an *encryption key* also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is an encrypted, secret information.[2]
On the other hand steganography is able even to hide this aspect making sure that even the fact that there is secret information, is concealed. Steganography's main aspect is that it is embedding the secret message into another message [3].
Mainly, steganography can be used for concealing important information within computer files such as documents or image files in such a way that only so called authorized users know and can extract the information. The advantage over classic cryptography is that messages hidden using steganography techniques do not attract attention on themselves. Before continuing this discussion additional terminology needs to be added. In general, steganography terminology is analogous to more conventional radio and communication technologies. The most important terms in steganography are the following:

- *The payload* – is the data that is needed to be transported, the data needed to be hidden
- *The carrier* – is the signal, data file or stream into which the valid data, the payload is hidden
- *Channel* – is a term used to refer to the type of input
- *The package, stego file* or *covert message* – is usually the resulting signal, stream or data file

2. RELATED WORK

Significant results have been obtained hiding information into text. The main goal was to discourage illegal document copying by making documents with line shift encoding, the lines of text

being shifted up or down thereby encoding a serial number. [4]

Steganography was also used to embed data into an audio signal by manipulating characteristics of the audio signal below the level of perceptibility. These techniques were useful in applications such as annotation, captioning and the automatic monitoring of radio advertisements. [5]

Important steps have been made hiding information using digital watermarking using improved techniques based on the decorrelation property of the Karhunen- Loeve Transform [6] as well as a method of hiding messages in digital images based on YUV format and its derivatives [7]. These techniques were used especially against a current common issue like illicit copying and distribution of copyright material.

Studies and tests were made for elaborating different techniques and algorithms to embed large amount of data into a picture as well as the requirements needed.

Other steps have been taken towards eliminating detection of steganography and counteracting attacks meant to extract the hidden information. New and more complex algorithm have been developed to avoid the detection of hidden data as well as embedding hidden information in preprocessed images and in images where
compression was applied. [8]

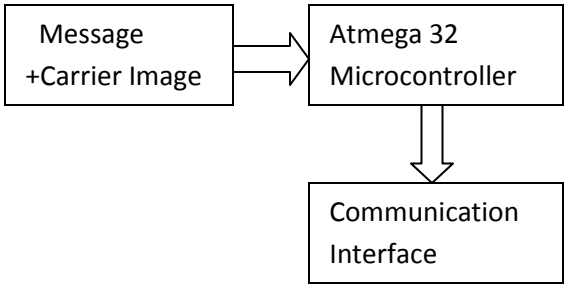
Other related work on the subject is about using steganography to insert a video or audio message in the cover in real time, using a secret key steganographic micro-architecture employing Field Programmable Gate Arrays [9]. Furthermore, devices such as Field Programmable Gate Arrays (FPGA) also hosted steganalysis (the reverse process of steganography) algorithms.

3. Brief description of Embedded hardware used for Implementing Steganography

This paper focuses on the steganographic technique used for hiding information in communication between various mobile or embedded devices.

As shown above 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 implement the steganographic algorithms on embedded devices. The main focus 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 executing the steganographic algorithm.



The hardware used consists of the AtMega 32 development board. The board's main components that were used in the implementation are: High-performance, Low-power Atmel AVR 8-bit Microcontroller.

The main processor is an AVR -8 bit microcontroller with 32Kbytes of In-System Self-programmable Flash program memory of embedded high speed flash memory having a large variety of peripheral interfaces.

The Atmel ®AVR® ATmega32 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega32 achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.

The ATmega32 provides 32Kbytes of In-System Programmable Flash Program memory with Read-While-Write capabilities, 1024bytes EEPROM, 2Kbyte SRAM.

4. Implementation Details

The steganography algorithm can be implemented on embedded devices based on how to decode an encrypted message within a carrier image.

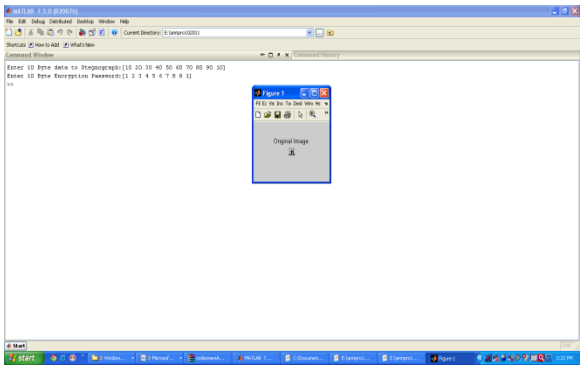
In an implementation two main aspects are considered i.e size of memory needed to store the image & process. Atmega 32 has 32KB of internal flash memory which is insufficient for storing large images because most of the part of memory is being used by code. So the image used in this work is 16×16 bitmap image.

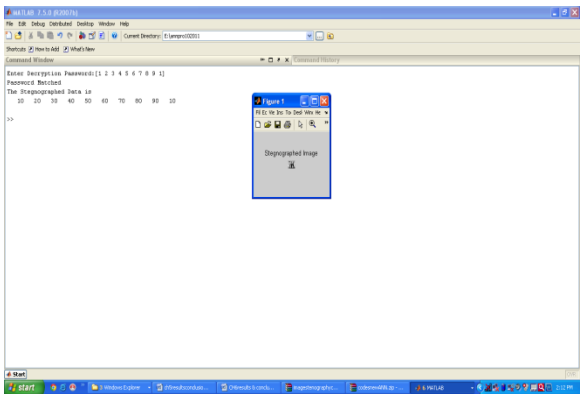
Steganography algorithm implemented on microcontroller can perform the effective hiding of information in such a way that it is very difficult to a casual person to detect that image contains some

information. It can't attract the attention of any user except the intended recipient.
This can hide or retrieve the data by using the various options present in the software these options can be:
1. Hide Message: -Hide the Text message into the Bitmap file.
2. Retrieve Message:-Retrieve the Text message from the Bitmap file.

The Data and Image are applied from PC and transferred to microcontroller through MAX232, where the encryption process is performed on data. In encryption process the encryption algorithm with password is applied. This data and cover image are hide by steganography algorithm. This is called stego image This stego image is then transmitted through channel via Zigbee. At receiver side the stego image is received via Zigbee receiver. The exactly reverse operations are performed at this stage. The decryption password and steganography algorithm are applied to stego image to extract the message from it. Then decrypted message is sent to pc with the help of MAX232.

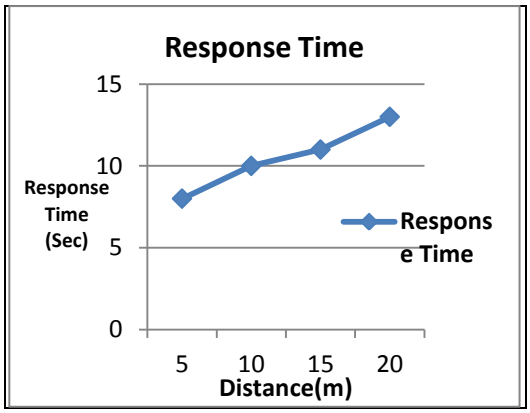
5. Results





Response time from Encoder to Decoder:

Distance	Response Time from Encoder to Decoder
5m	8sec
10m	10sec
15m	11sec
20m	13sec



Original Image

Stegnographed Image

PSNR Calculation:

$$PSNR_{worst} = 10 \times \log_{10} \frac{255^2}{WMSE}$$

$$= 10 \times \log_{10} \frac{255^2}{(2^k - 1)^2} \text{ dB.}$$

$$= 48.13 \quad \text{for k=1}$$

6. Conclusion

This paper presents a possible implementation of steganography algorithms on an embedded platform as well the analysis regarding the amount of time needed by the embedded microprocessor to extract the payload or data/message from the carrier. The main benefit of

this implementation is that it brings steganography on a level very common nowadays, the mobility. Using steganography on mobile devices may improve security on data transfers without additional significant cost. Furthermore, this work focuses on using microcontrollers or microprocessors for executing the steganographic algorithms instead of using Field Programmable Gate Arrays. This way, when adding steganography capabilities on an embedded device the cost is not mainly influenced as it could be if a FPGA module is added to the device. Steganography may also help hiding secret information in communication lines, for example embedded modules with steganographic encrypting and decrypting capabilities connected between two systems. An embedded device with steganography implemented on it can be used in secret communication. The technique used in this work is LSB algorithm, processing the images on the pixel level.

7. References

[1] Daniela Stanescu, Valentin Stangaciu, Ioana Ghergulescu, Mircea Stratulat "Steganography on embedded devices" 5th International Symposium on Applied Computational Intelligence and Informatics • *Timişoara, Romania*

[2] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE COMPUTER, vol. 31, 1998, pp. 26--34*

[3] József Lenti, "Steganographic methods", *Department of Control Engineering and Information Technology, Budapest University of Technology and Economics, H-1521, Budapest, Hungary, June 2000, pp. 249-258*

[4] 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.*

[5] 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 Institute, Cambridge, England, May 1996, pp. 295 – 315*

[6] D. Stanescu, M. Stratulat, B. Ciubotaru, D. Chiciudean, R. Cioarga, and D. Borca, "Digital Watermarking using Karhunen- Loeve transform," *Applied Computational Intelligence and Informatics, 2007. SACI '07. 4th International Symposium on, 2007, pp. 187-190*

[7] Stanescu, D.; Stratulat, M.; Groza, V.; Ghergulescu, I.; Borca, D."Steganography in YUV color space", *Robotic and Sensors Environments, 2007. ROSE 2007. International Workshop on Volume , Issue , 12-13 Oct. 2007*

[8] Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy, "Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics", *Communications and Multimedia Security, 2005, Volume 3677/2005, ISB*978-3-540-28791-9, *pp. 273-274*

[9] H.A. Farouk and M. Saeb, "Design and implementation of a secret key steganographic micro-architecture employing FPGA," *Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair, Yokohama, Japan: IEEE Press, 2004, pp. 577-578.*

[2] Mr. P.D.Khandait **"**LSB Technique for Secure Data Communication" [01] Eric Cole ,"Hiding in Plain Sight: Steganography andthe Art of Covert Communication" [02] Karen

Bailey & Kevin Curran Steganography
[03] Gregory Kipper,"Investigator's Guide to Steganography "
[04] Stefan Katzenbeisser and Fabien, A.P. Petitcolas ," Information Hiding Techniques for Steganography and Digital Watermarking " [05] Hiding secrets in computer files: steganography is the new invisible ink, as codes stow away on images-An article from: The Futurist by Patrick Tucker
[06] R.J. Anderson and F.A.P. Petitcolas, "On the Limits ofSteganography," IEEE Journal of Selected Areas inComm., vol. 16, no. 4, 1998, pp.474-481.
[07] Ismail Avcıbas¸, Member, IEEE, Nasir Memon, Member, IEEE, and Bülent Sankur, Member, "Steganalysis Using Image Quality

Metrics," IEEE Transactions on Image Processing, Vol 12, No. 2, February 2003. [08] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE,1998.
[09] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to Steganography" IEEE Computer Society IEEE Security & Privacy. [10] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.