IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 2, February 2016

A Hardware Approach to Digital Image Steganography using Black fin ADSP BF-532

M. Selvam[1]

Assistant Professor, Department of Electronics and Communication Systems,

Karpagam Academy of Higher Education, Coimbatore, India[1]

Abstract: Securing the Data over the wireless transmissions is the urgent need in the Data Communication field. The Protection of information over the wireless networks by encrypts the information but due to advancements in the computing techniques the cipher texts can easily detected and decrypted. So avoiding the attacks from the unintended users the presence of secret information must masked. It helps the recipient to protect the message from the hackers. In this regard a technique is developed to hide the Secret information over the wireless networks a cover digital image is used and that is called digital Image steganography. Digital Image Steganography is hiding data within image more securely and confidentially for the communication. This paper emphasis the Hardware based digital image Steganography using blackfin BF532 ADSP processor.

Keywords: steganography, blackfin, secure communication.

I. INTRODUCTION

Since, from the first written communication secrecy is the ultimate goal for men to maintain their integrity and confidentiality. In the past, messages could easily be intercepted and there were no secrecy devices, so the third party was able to read the message. During the time of the Greeks, around 500 B.C., when Demaratus first used the technique of steganography. The word **Steganography** derived from two Greek words **steganos,** meaning **"covered,"** and **graphein,** meaning **"to write."**

As the name says steganography has a cover medium to hold the secret message without showing it's explicit it passes the message from one end to another end. The goal of Steganography is to avoid drawing suspicion to the transmission of a hidden message.

Steganography encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages.

Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. This project Emphasis the implementation of Digital Image Steganography using LSB Embedding Technique by Blackfin ADSP Processor BF532. A 24 bit color image is used as cover image and secret information is written into that by LSB embedding technique using BF 532 Visual DSP Coding.

II. STEGANOGRAPHY MODEL

There are various methods of Steganography models are available in the field. It is called as Steganography algorithm. The process of steganography is shown in fig.

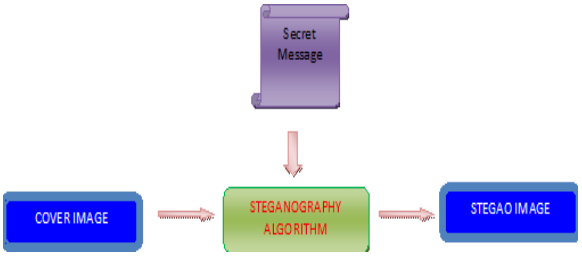


Fig1.Steganography model

From the Figure the process of steganography have unsuspicious cover to pass the information it is called a cover medium it can be audio, video and images or texts. In this paper we took it is a 24bit digital image.

Once the secret information i.e text, audio or video is embedded with a cover image then the image call called as stego image. This steganography methods can compared with other data securing methods such as Cryptography

CRYPTOGRAPHY VS STEGANOGRAPHY

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the Information is hidden

III. STEGANOGRAPHY METHODS

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

LSB REPLACEMENT TECHNIQUE

In Image Steganography almost all data hiding techniques try to alter in significant information in the cover image. Least significant bit (LSB) insertion is a common, simple

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 2, February 2016

approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc.

MSB REPLACEMENT TECHNIQUE:
The moderate significant bits of each pixel in the cover image can be used to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image.

TRANSFORMATION METHOD:
Another steganography method is to hide data in mathematical functions that are in compression algorithms. Two functions are Discrete Cosine Transformation (DCT) and Wavelet Transformation. The DCT and wavelet functions transform data from one domain into another. The DCT function transforms that data from a spatial domain to a frequency domain.

IV. BLOCK DIAGRAM

The Block Diagram contains two modules
(i) Hiding Data
(ii) Extracting Data

HIDING DATA:

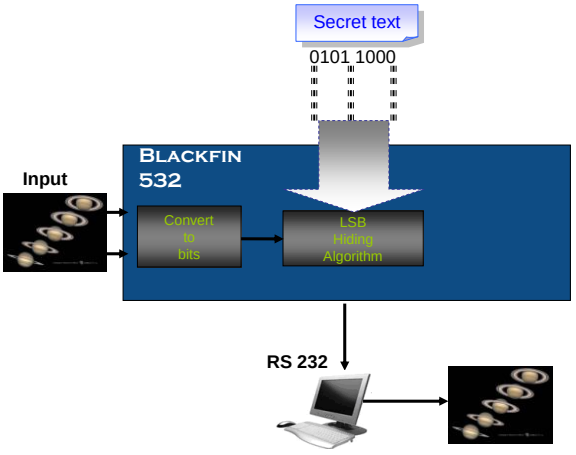


Fig 2: Hiding Data

This process is used to embed the secret text into the image by performing the following process.

- ❖ Checking the capable of Cover Image to carrying the message.
- ❖ RGB plane separation
- ❖ Masking the LSB of each byte
- ❖ Inserting the message into LSB.
- ❖ Obtain Stego-Image

EXTRACT DATA:
In this phase the stego image is steg analysed and separates the lsb bits in the colour plane patterns and combines to form the secret text.

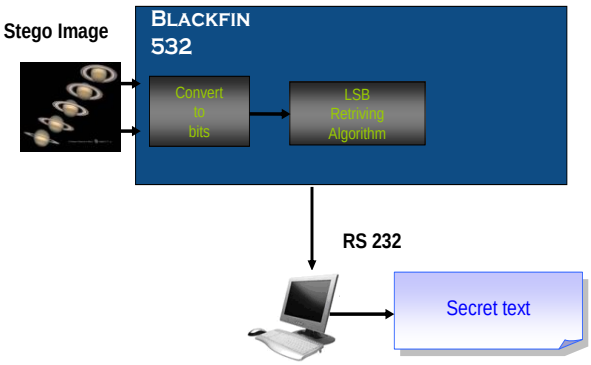
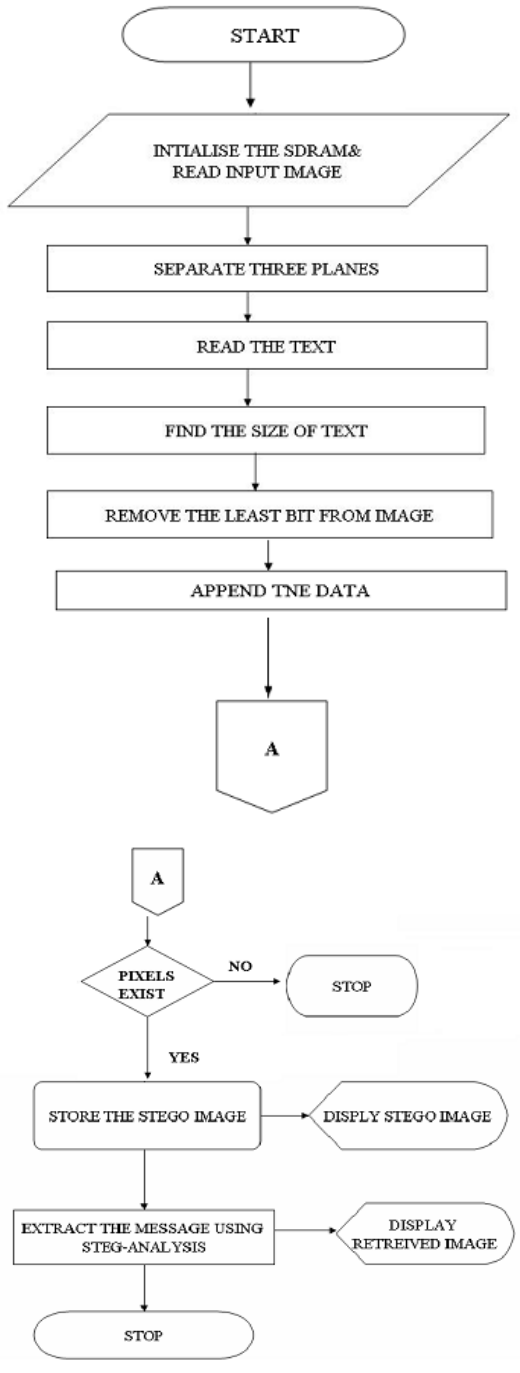


Fig 3: Extract Data

V. FLOW CHART



IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 2, February 2016

VI. WORKING PROCESS

In this stage the blackfin ADSP based digital image steganography has the following steps.

Step1: A 24 bit JPEG colour image is read by the user through a MATLAB GUI and given to the Blackfin BF 532 UART at 9600 baud rate. This is shown in the image

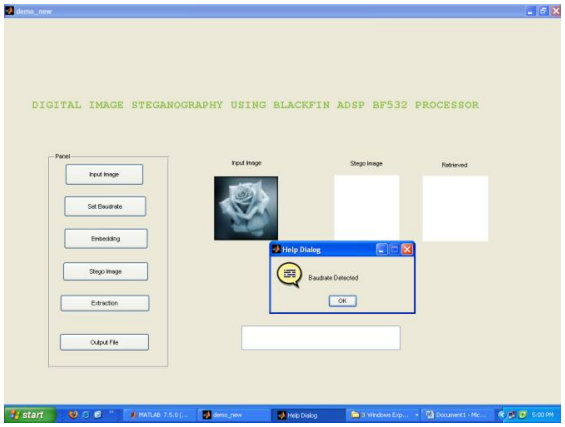


Fig 4: Selecting Baud Rate of BF532

Step2: The Input colour image will be separated into 3 colour planes as their primary colours such as Red, Green, blue by plane separation algorithm. Each plane 8 bit wide.

Step 3: The Lower 3 nibbles of Red and green and two of blue will embed by the secret message bits. This process is called as LSB insertion technique. It is shown in fig with an example

Assume the original three pixels are represented by the three 24-bit words below
(00100111 11101001 11001000) - Red
(00100111 11001000 11101001) - Green
(11001000 00100111 11101001) - blue

The binary value for the letter A is (10000001). Inserting the binary value of A into the three pixels, starting from the left byte, would result in:

A is (10000001). Original Pixel Value
R→ 00100111 G→ 11101001 B→ 11001001

Emptying LSB (3) Values in RGB bit streams
R→ 00100000 G→ 11101000 B→ 11001000

After Embedding the bitstream of 'A'
R→ 00100100 G→ 11101000 B→ 11001001

The graphical explanation of this technique is

INPUT PLANE SEPERATION:

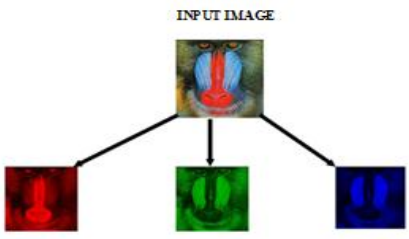


Fig 5: Colour Plane separation

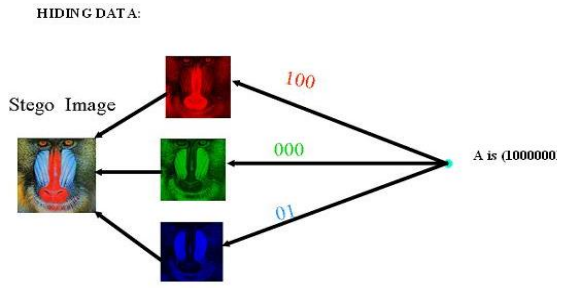


Fig 6: Hiding data into image

Step4: once the Data bits are embedded in the colour plane bits, the Steganography are completes and the secret information is buried into the image. Hence the image called as Stego image.

Step 5: once the stego image is achieved then the image gets into the data extraction phase to reverse the data readable. This Process is known is steganalysis.

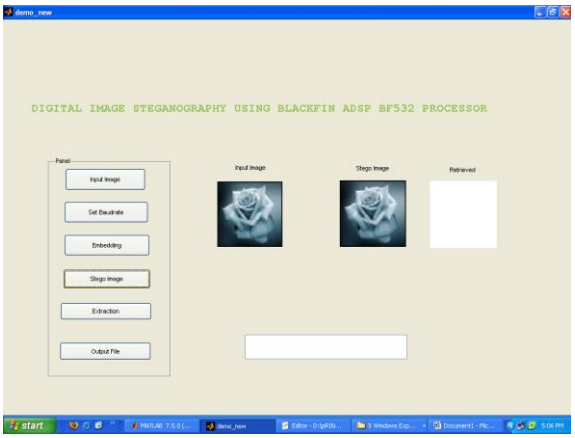


Fig 7: Obtaining Steg Image

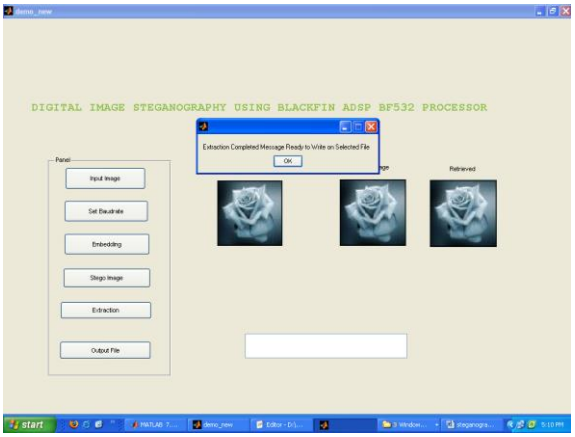


Fig 8: Data retrieval

VII. CONCLUSION

A Hardware approach to digital image steganography using black fin BF532 is user friendly approach can easily adopted an digital hardware to perform the secure data communication over wirelessly. A direct approach of hardware synthesis is accomplished and future multimedia gadgets can embed this algorithm to transfer information

REFERENCES

1. A. C. Rencher, Methods of Multivariate Analysis. New York: John Wiley, 1995, ch. 6, 10.
2. A. M. Eskicioglu, "Application of multidimensional quality measures to reconstructed medical images," Optical Engineering., vol. 35, pp. 778-785, Mar. 1996.
3. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673-1686, Dec, 1997.
4. B. Lambercht, Ed., "Special issue on image and video quality metrics," in Signal Process., Oct. 1998, vol. 70.
5. N. F. Johnson and S. Jajodia, "Steganalysis: The investigation of hidden information," in Proc. IEEE Inform. Technol. Conf., Syracuse, NY, 1998.
6. C. E. Halford, K. A. Krapels, R. G. Driggers, and E. E. Burroughs, "Developing operational performance metrics using image comparision metrics and the concept of degradation space," Opt. Eng., vol. 38, pp. 836-884, May 1999.
7. M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," in Proc. SPIE Conf. On Security and Watermarking of Multimedia Contents II, San Jose, CA, 2000, pp. 371-380.
8. J. Fridrich, R. Du, nad M. Long, "Steganalysis of LSB encoding in colour images," in Proc. ICME 2000, New York, 2000.
9. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," in Proc. ICME 2000, New York, 2000.
10. I. Averbas, B. Sankur, and K. Sayood, "Statistical analysis of image quality measures, "J. Electron. Imag., vol. 11, pp. 206-223, Apr, 2002.

BIOGRAPHY

The Author is working as an Assistant professor in deemed university and has 6.5 years of experience. He has completed Msc., M.Phil., M.E. in the Stream of Electronics and Communication. His Area of Research Interest is Embedded Systems and Image Processing. He has qualified in UGC NET.

DOI 10.17148/IJIREEICE.2016.4226