ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

A Review-FPGA Implementation of Different Steganographic Technique

K.N.Pansare, Dr. A.K.Kureshi

Asst.Professor, Dept. of E&Tc, P.D.V.V.P.COE, Pune, Ahmednagar, Maharashtra, India

Professor, Dept. of E&Tc, V.A.COE, Pune, Ahmednagar, Maharashtra, India

Abstract: Steganography is a method of hiding the information in a cover in such a way that only intended recipient can know that there is a hidden message. In Steganography for hiding information any embedding medium can be used, called as carriers. These carriers can be images, audio files, video files, and text files. In this paper we have focused on steganographic techniques for image files. Image steganography techniques now days developed with an alternative approach based on an embedded FPGA system for image processing. Due to its reconfigurable ability Various FPGA approaches are chosen and without requiring hardware change-out, the uses of FPGA type Devices expand the product life by updating data stream files.

Keywords: FPGA, Steganography, Steganalysis, Synthesis.

I. INTRODUCTION

Steganography is the method to hide data in a cover media such as text, audio, image, video, etc. In other words, steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Steganography will hide the message so there is no knowledge of the existence of the message in the place. The term Steganography is forked from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Generally, there are two types of data hiding techniques using images: spatial and frequency domain. The spatial domain is based on embedding message in the least significant bit (LSB) of image pixel. The basic LSB method is simple for implementation and it has high capacity. However it is weak versus some attacks such as low-pass filtering and compression.

The frequency domain embeds the messages in the frequency coefficients of images. These hiding methods overcome the problems found in the spatial domain. Steganalysis is nothing but the process of detecting hidden data which are crested using steganography. Steganalysis detects stego-images by analyzing various image features between stego-images and cover-images [1]. In recent researches, numerous steganography techniques based on genetic algorithms is released. Now a day the steganography techniques are developed on various FPGA hardware. Field programmable gate array i.e. FPGA, provides the reconfigurability as well as the robustness for the image processing.

Due to the use of FPGA we can develop an alternative approach based on an embedded FPGA system for image processing. Field Programmable Gate Array (FPGA) is widely used in embedded applications such as automotive, communications, industrial automation, motor control, medical imaging etc. And without requiring hardware change-out, the uses of FPGA type Devices can expand the product life by updating data stream files. FPGAs have capability to hold an entire system on a single chip also it allows in-Platform testing and debugging of the system. Furthermore, it offers the opportunity of utilizing hardware/software co-design to develop a high performance system for different applications by incorporating processors, on-chip busses, memory, and hardware accelerators for specific software functions [2].

Most of the work is now happening to create efficient FPGA hardware architectures for various steganographic techniques.

II.FPGA HARDWARE APPROCHES

The FPGA hardware was developed by (L. V. S Subbaraju, P. Praveen, U. Yedukondalu) for the detection of hidden bits in the Least Significant Bit (LSB) plane of a natural image. They have used mean level and the covariance matrix of the image, considered as a quantized Gaussian random matrix, is unknown. And they have designed adaptive

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

statistical test such that its probability distribution is always independent of the unknown image parameters, while ensuring a high probability of hidden bits detection.

This is based on the likelihood ratio test except that the unknown parameters are re-placed by estimates based on a local linear regression model. This test maximizes the probability of detection as the image size becomes arbitrarily large and the quantization step vanishes. This provides an asymptotic upper-bound for the detection of hidden bits based on the LSB replacement mechanism. System is developed on Xilinx Spartan3 Field Programmable Gate Array (FPGA) device using embedded development kit (EDK) tools from Xilinx [2].

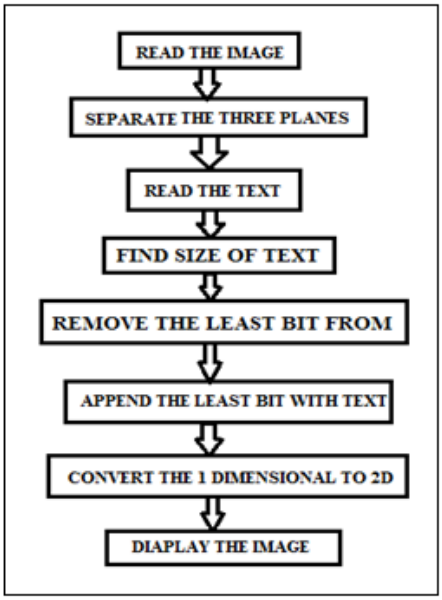

Fig. 1 Flow Chart of Adaptive Stegano Analysis Using LSB Technique [2]

They have processed as per the flow chart given in fig.no.1, and they have got the synthesis report as shown in table. 1 [2],

```
Selected Device : 3s200tq144-4

 Number of Slices:                    1880  out of   1920    97%
 Number of Slice Flip Flops:          2118  out of   3840    55%
 Number of 4 input LUTs:              2971  out of   3840    77%
    Number used as logic:             2418
    Number used as Shift registers:    297
    Number used as RAMs:               256
 Number of IOs:                         62
 Number of bonded IOBs:                 62  out of     97    63%
    IOB Flip Flops:                     64
 Number of BRAMs:                        4  out of     12    33%
 Number of MULT18X18s:                   3  out of     12    25%
 Number of GCLKs:                        4  out of      8    50%
 Number of DCMs:                         1  out of      4    25%
```

Table. 1 Synthesis report of Adaptive Stegano Analysis Using LSB Technique [2].

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

In the next work done by Hala Farouk, Magdy Saeb, in that they have proposed a video or audio steganographic model. In which the hidden message can be composed and inserted in the cover in real-time. This is realized by designing and implementing a secret key steganographic micro architecture employing FPGA. The architecture is divided into an embedder processor and an SDRAM controller. The embedder processor, issues read and write commands to the memory, which are processed and reformatted by the SDRAM control and waits for a confirmation from memory to ensure stabilized output.

The controller halts the process when hiding is complete. In the next sections we discuss the various building blocks of our proposed micro-architecture [3].

They have implemented the micro architecture on Xilinx Spartan-2 device and the respective synthesis report is as shown in Table 2 and Table 3 [3],

Implementation Results
Target Device: x2s100
Target Package: tq144
Target Speed: -6
Mapper Version: spartan2 -- C.22

Minimum period	48.811ns
Maximum frequency	20.487MHz
Maximum combinational path delay	49.783ns
Maximum net delay	11.980ns

Table. 2 Total Design Timing Summaries [3].

Number of External GCLKIOBs	2 out of 4(50%)
Number of External IOBs	43 out of 92 (46%)
Number of SLICEs	1195 out of 1200 (99%)

Table. 3 Device utilization summaries [3]

The FPGA Hardware for LSB Steganographic Technique which Based on the Lifting Scheme was developed by (Gorre Josh Kumar, U.N.Subhadra Devi), in which they have proposed LSB Information Hiding algorithm which can Lifting wavelet transform image. They have used LSB algorithm is to insert the bits of the hidden message into the LSB of the pixels. Due to such information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed.

It is observed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks. However, due to the limitation of capacity they have approached to programmable gate array (FPGA) board [5].

The synthesis report is as shown in Table.4 [5],

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

```
Design Summary:
Number of errors:      0
Number of warnings:    3
Logic Utilization:
  Number of Slice Flip Flops:          976 out of   3,840   25%
  Number of 4 input LUTs:            1,560 out of   3,840   40%
Logic Distribution:
  Number of occupied Slices:                        1,174 out of   1,920   61%
    Number of Slices containing only related logic:   1,174 out of   1,174  100%
    Number of Slices containing unrelated logic:          0 out of   1,174    0%
      *See NOTES below for an explanation of the effects of unrelated logic
Total Number 4 input LUTs:           1,953 out of   3,840   50%
  Number used as logic:               1,560
  Number used as a route-thru:            7
  Number used for Dual Port RAMs:       256
    (Two LUTs used per Dual Port RAM)
  Number used as Shift registers:       130
  Number of bonded IOBs:                 62 out of      97   63%
    IOB Flip Flops:                     122
  Number of Block RAMs:                   4 out of      12   33%
  Number of MULT18X18s:                   3 out of      12   25%
  Number of GCLKs:                        2 out of       8   25%
  Number of DCMs:                         1 out of       4   25%
  Number of BSCANs:                       1 out of       1  100%

   Number of RPM macros:             3
Total equivalent gate count for design:  325,662
```

Table.4 Synthesis report of LSB Steganographic Technique Based on the Lifting Scheme [5]

The SysGen Architecture for Visual Information Hiding Framework was developed by (Abhishek Basu, Tirtha Sankar Das, Subir Kumar Sarkar), in which they have focused on of rapid prototyping tools such as MATLAB-Simulink and Xilinx System Generator (SysGen). They have developed the decoding and encoding unit.

The decoding unit consists of three blocks, counter as address generator to access the ROM containing watermarked image following by information processing block which recover the watermark from the watermarked image. At the time of implementation of Encoder and Decoder, Xilinx blocks are used from Matlab Simulink browser [8]. The architecture is implemented using available Spartan-3A (XC3SD3400A-4FGG676C) DSP edition board. The Device Utilization Summary is as shown in table. 5 and table.6 [8],

For Encoder unit:

Logic Utilization	Used	Available	Utilization
Number of Slices	16	23872	0%
Number of Slice Flip Flops	31	47744	0%
Number of 4 input LUTs	31	47744	0%
Number of bonded IOBs	19	469	4%
Number of GCLKs	1	24	4%

Table. 5 Synthesis report of LSB encoder unit [8]

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

For Decoder unit:

Logic Utilization	Used	Available	Utilization
Number of Slices	6	23872	0%
Number of Slice Flip Flops	11	47744	0%
Number of 4 input LUTs	4	47744	0%
Number of bonded IOBs	11	469	2%
Number of GCLKs	1	24	4%

Table. 6 Synthesis report of LSB decoder unit [8]

III. CONCLUSION

This paper has discussed some steganographic techniques which are proposed on field programmable gate array. Mainly the spatial domain and transform domain techniques are taken into account. After going through the synthesis results for respective techniques, we have observed that FPGA is the best solution for the efficient image processing. Also by proper hardware architecture development we can improve the results for spatial domain i.e. LSB technique. Also future work can be done on optimisation of developed hardware architectures with respect to power, timing, and area.

REFERENCES

[1] Masoud Nosrati and Ronak Karimi, "Advanced frontal A Survey on Usage of Genetic Algorithmsin Recent Steganography Researches," presented *World Applied Programming, Vol. 2, No. 3, Mar. 2012. Page no. 206-210*.
[2] L. V. S Subbaraju, P. Praveen, U. Yedukondalu, "A Hardware FPGA Implementation of Adaptive Stegano Analysis Using LSB Technique," *Journal of Engineering Research and Application, ISSN: 2248-9622, Vol. 3, Issue 5, Sep-October 2013, pp.2010-2014*.
[3] *Hala Farouk, Magdy Saeb*, "Design and Implementation of a Secret Key Steganographic Micro-Architecture Employing FPGA" 1530-1591/04, 2004 IEEE.
[4] Mrs.Manjula.Y, Mr.Jagadeesha.D.H, Dr. K.B ShivaKumar, "FPGA Implementation for Image Steganography Technique Using X-Box Mapping," *International Journal of Computer & Organization Trends –Volume 3 Issue 6 – June 2013*.
[5] Gorre Josh Kumar, U.N.Subhadra Devi, "FPGA Hardware LSB Stegnography Technique Based on the Lifting Scheme," International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 8, August - 2013.
[6] Mustafa Osman Ali and Rameshwar Rao, "Determination Digital Image Watermarking Basics, and Hardware Implementation," *International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012*.
[7] Amit Joshi, Vivekanand Mishra and R. M. Patrikar, "Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application", Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7.
[8] Abhishek Basu, Tirtha Sankar Das, Subir Kumar Sarkar, "SysGen Architecture for Visual Information Hiding Framework," International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, Volume 2, Issue 3, Mar. 2012.

BIOGRAPHY

Pansare K.N. received the B.E. degree in Electronics Engineering, from Pune University in 2006. He is pursuing his M.E. in VLSI and Embedded system of Pune University from Vishwabharati College of engineering, Ahmednagar, under the guidance of Dr. A. K. Kureshi, Principal, Vishwabharati College of engineering, Ahmednagar, Maharashtra. He is currently working as Asst. Professor, Dept. Of Electronics and Telecommunication, P.D.V.V.P. college of engineering, Ahmednagar, Maharashtra. His current interests include VLSI and Steganography techniques.

Dr. A. K. Kureshi received the B.E. degree in Electronics Engineering, from B.A. Marathawada University, Aurangabad in 1994 and M.E. in Electronics from B.A. Marathawada University, Aurangabad in 2004. He received PhD from Aligarh Muslim University, Aligarh in 2010. He is currently the Principal of Vishwabharati College of engineering, Ahmednagar, Maharashtra. His current interests include VLSI and low power techniques and architectures of FPGA.