FPGA Prototyping of Image Watermarking SRAM

S.JAGADEESH[*1]

Associate Professor & HOD, Department of Electronics and Communication Engineering, Sri Sai Jyothi Engineering College, JNTUH, Gandipet, Hyderabad-75, (A. P.), India.

S. BHARGAV KUMAR[#2]

P.G. Student, M.Tech. (VLSI), Department of Electronics and Communication Engineering, Sri Sai Jyothi Engineering College, JNTUH, Gandipet, Hyderabad-75, (A. P.), India.

DR.M.ASHOK [#3]

Professor, Department of Computer Science and Engineering, Sri Sai Jyothi Engineering College, JNTUH, Gandipet, Hyderabad-75, (A. P.), India.

Abstract

In order to improve the security and authentication in an image transmission over any communication channel, watermarking techniques have been evolved. Watermarking techniques use a cover image, over which the bit based or transparency based watermarking image is watermarked. The watermarked image will be further processed to retrieve the original cover image at the receiver. If watermarking image is revealed, then security in cover image transmission through any communication channel fails. In order to protect the cover image we are proposing a new method of watermarking technique [1], which will increase the generation of watermark image as a non-repetitive sequence of bits. We are using Linear Feedback Shift Register (LFSR), which generates 8x8 watermark bits, which will be watermarked with (8x8) cover image and (8x8) address generator, where our watermarked bits will be stored. Advantage of LFSR is that, it won't generate the sequence of similar bits till it reaches the seed or initial value. The watermarked image bits which are stored in SRAM memory address location will be retrieved and reverse watermarking will be done. We simulated and synthesized all the modules using Matlab 7.5, Xilinx 9.1i and ModelSim XE III 6.4b. The layout and sketch design of our module for watermark and address generator was implemented using layout and SPICE tools. The complete layout is analyzed and presented in our paper. A comparative result between different images using our method of watermarking has been analyzed. The VLSI architecture of the functional units of our proposed watermarking technique is presented. The results of hardware implementation in SRAM design are also presented. The prototype chip carries both watermarking and addresses generation techniques in SRAM are also presented.

Keywords: watermarking techniques, LFSR, seed value, SRAM, layout.

1. Introduction

With enormous use of the data sharing through Internet and improvements in continuous digital media and data compression technology, digital audio files, digital images, streaming video, online readable books and plug-and-play games can be distributed widespread between the end-users through different computer networks. However, without protection and management of digital rights, digital content can be easily copied, altered, and distributed to a large number of recipients, which could cause revenue loss in data transfer between the legal parties. Digital rights management (DRM) refers to protecting ownership/copyright of electronic content by restricting what actions an authorized recipient may take in regard to that content. DRM control the use of that content and preventing unauthorized distribution. DRM consist of encryption and watermarking. Encryption can be used to prevent unauthorized access to digital content.

Digital watermarking is to protect the owner's copyright over that content. The watermark which is added to original image can be later be extracted from a watermarked image and be analyzed in order to identify the owner of the content. For an authenticated image transmission [8] over a communication channel scheme of watermarking consists of three parts: the watermark, the encoder, and the decoder. The watermarking technique incorporates the watermark in the content, whereas the verification technique authenticates the content by determining the presence of the watermark and its actual data bits.

Digital image watermarking will improve the security in the content of digital documents. Different types of watermarking techniques were developed with different types of implementation strategies. The main purposes of all these techniques are to transmit a digital content securely without losing its digital content.

In paper [1], the digital image watermarking was done using LFSR [2 and 3]. The size of original image bits are 16x16 matrix of size 256x256, watermarking image bits are 16x16 matrix of 256x256 and the resultant watermarked image bits are 16x16 matrix of size 256x256. These watermarked image bits are stored in SRAM memory address of 8x8 sizes. In our paper we are going to implement using 8x8 bit size for original image, watermarking image and address generation. These modules are simulated and synthesized in Xilinx and Model Sim.

In our paper, we are presenting a FPGA prototype [4] of digital image watermarking SRAM. Here we are using SRAM to store our watermarked image bits. The prototype of FPGA we had selected for our design is SPARTAN 3E family of xa3s1600e device of FGG400 package with speed -4. Our FPGA prototype was synthesized in XST VHDL tool and simulated in Model Sim XE VHDL. And the layout of our proposed prototype is implemented in Digital Schematic tool and high-end layout tool. The complete layout of our proposed method has been implemented on CMOS 0.12µm technology VSLI architecture. Simulated results of our proposed method of watermarking have shown best results in area utilization, power consumption and gate count.

The rest of the paper as follows, Section 2 will discuss about the related contribution of our proposed method. In section 3, the method selected for hardware architecture is discussed. In section 4, FPGA prototyping is presented. Section 5 will clearly explains the simulation and synthesis of our proposed method of watermarking and section 6 will conclude our paper.

2. Related Contribution

In paper [1], two LFSRs were implemented, one for digital image watermarking [3] of size axa and the other for address generator of size cxc. Here the first LFSR will generate the cover image of axa size bit array which will be watermarked with bxb size bit array. After watermarking, the watermarked bit array will be stored in the SRAM (Static Random Access Memory) address locations using another LFSR of cxc size bit array. LFSR's will generate random numbers, which will be hidden in the image. If these random numbers won't match at the extraction process, the original image won't be retrieved [7]. Bit wise operation is made between the LFSR generated axa size bit array and the original image bxb size bit array. In this technique, the size of watermarking LFSR as 16x16 and the original image size as 256x256. And for address generator LFSR, 8x8 size LFSR. Depending on the seed value of the LFSR we can implement watermarking technique for different sizes of images. LFSR based watermarking showed a secured authenticated copyright protection to the digital images.

In our technique of watermarking we are implementing on 8x8 bits of original image, cover image and watermarked image. This will make the extraction process simpler than the previous proposed technique.

3. Method Selected For Architectural Implementation

In this chapter, we present the algorithms used to implement the architecture of several units and modules of the watermarking.Two 8 bit LFSR's are used to implement our proposed method, one for watermark generation and the other for address generation.

We implemented our proposed method in five module, the tasks of each module is:

a. First module will perform 8 bit LFSR [6] watermark generation.

b. Second module will perform 8 bit watermarking process with 8 bit cover image.

c. Third module will perform generation of 8 bit address location in SRAM and storing the watermarked image bit (from task b) in to SRAM.

d. Fourth module will perform the retrieving of image bits from SRAM memory address location and perform revere watermarking which is an invisible [12].

e. Fifth module will calculate the PSNR between the transmitted image bits and received image.

And we grouped all the above modules in to three architectural design and implementations as:

A. Watermark Insertion algorithm: The watermark insertion can be done by implementing the AOI logic based watermarking on the cover image bits and LFSR generated bits. This is shown in the Fig: 3.1.

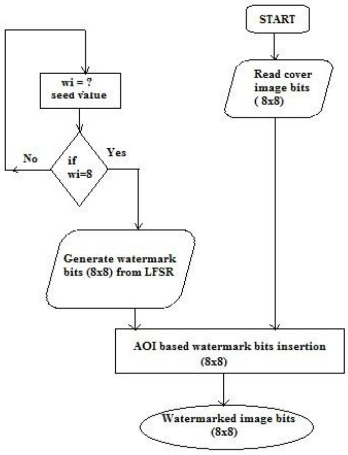
START
Read cover image bits (8x8)
wi = ? seed value
if wi=8
No
Yes
Generate watermark bits (8x8) from LFSR
AOI based watermark bits insertion (8x8)
Watermarked image bits (8x8)

Fig: 3.1 Watermark Insertion algorithm

B. Address generation Algorithm: In address generation process [11], we will generate polynomials using LFSR and these bits will be our memory address locations. This is shown in the Fig: 3.2.

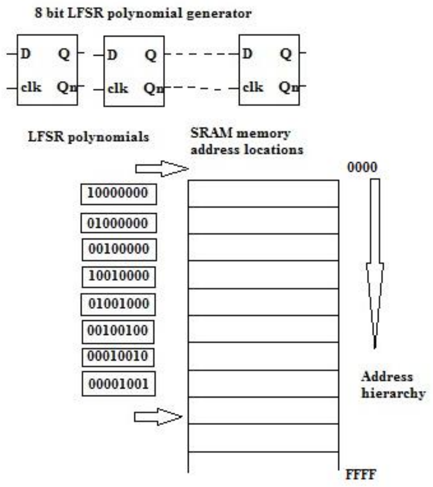

Fig: 3.2 Address generations algorithm

C. Watermark Extraction Algorithm: This step is divided in to two parts:

a. Watermarked bits will be stored in the SRAM memory locations, which are generated by address generation algorithm. This is shown in the Fig: 3.3.

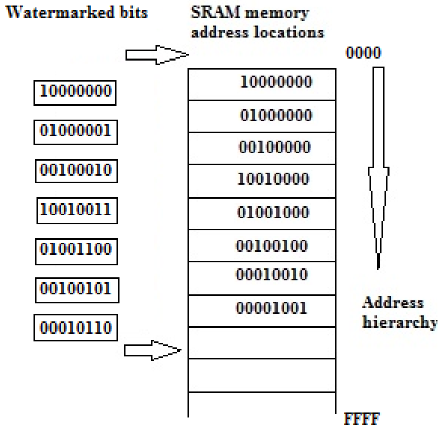

Fig: 3.3 Watermarked bits retrieved from memory location

b. And watermark extraction will be implemented. This is shown in the Fig: 3.4.

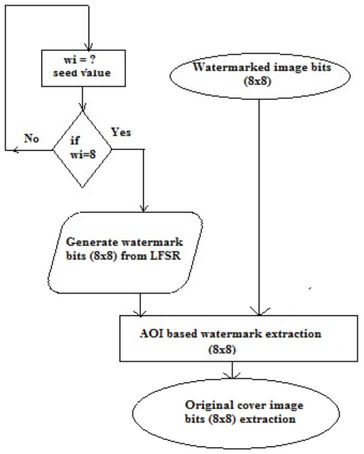
wi = ? seed value
Watermarked image bits (8x8)
if wi=8
No
Yes
Generate watermark bits (8x8) from LFSR
AOI based watermark extraction (8x8)
Original cover image bits (8x8) extraction

Fig: 3.4 Watermark extraction algorithm

4. FPGA Prototyping

In this chapter, we present the architecture [4 and 5] of several units and modules of the watermarking. We implemented our proposed method of watermarking on JPEG 2000 [9] color to gray converted image. The techniques and stages involved in the development of the architecture are described. In Fig: 4.1., we present the architecture of the digital image watermarking module. The architecture of the LFSR-based image watermarking module with its address generation is presented in Fig: 4.2. The modules of watermarking, address generation and watermark extraction process will be presented, the FPGA architecture of the watermark encryption and decryption unit [10] is also presented.

The high level architecture of the visible watermarking module is composed of several sub modules, such as watermark, insertion, row and column address generator and en-decoder, registers and controller. The watermark module calculates the watermark coefficients of host and watermark images before they are stored in the SRAM memory. The controller performs the operations of all the other modules and the data flow in the watermarking unit. Address decoders are used to decode the memory address where the image and watermark are stored.

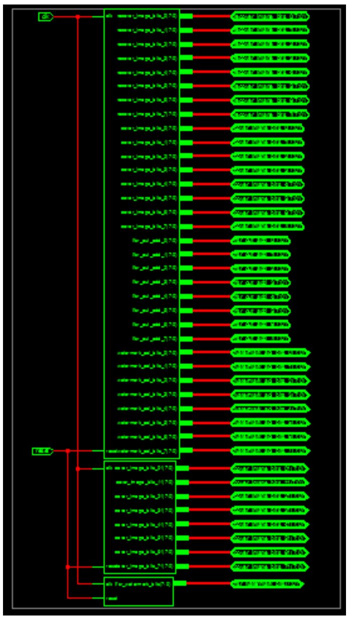

Fig : 4.1 Technology schematic of Image watermarking SRAM

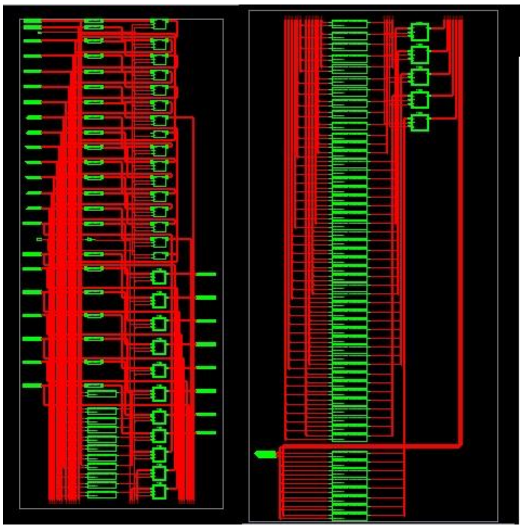

Fig: 4.2 Technology Schematic of Watermark insertion modules

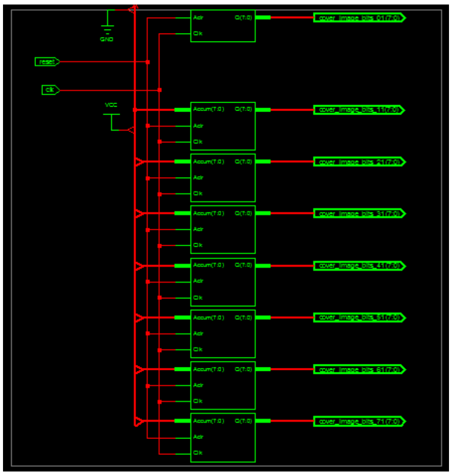

Fig: 4.3 Technology Schematic of Watermark extraction modules

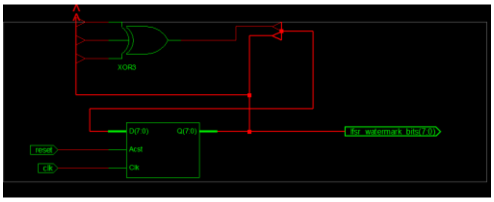

Fig: 4.4 Technology Schematic of Watermark extractions from memory

For the prototyping, the architecture was modeled using VHDL and the functional simulation was carried out using ModelSim XE III 6.4b tools. The VHDL code was compiled using Xilinx ISE 9.1i. The synthesis of the architectures was carried out using SPARTAN 3E technology with xa3s1600e target device. The address generator serves the purpose of address en-decoder by supplying the appropriate address needed for reading from the SRAM memory for watermarking and insertion. Two block RAMs is needed for our implementation; one block RAM is used as a memory for storing individual image and one RAM is used for storing data that has undergone watermarking processes.

For the implementation, input RAM was used to temporarily store data. The input RAM was also used for pipeline design so that data could be received while the processing of previous data is being carried out. To aid utilization of pipelining, we also extensively used registers in our watermarking module. Registers were used instead of RAM to increase the performance of our system. The use of parallelism in the implementation in our method of the insertion module of the watermarking unit gives the capability to watermark an image bits block in one clock cycle instead of two. For the insertion unit of the invisible watermark module, we employ the concept of resource sharing in our implementation.

This improves the performance of our system; however, there is a trade of between the performance and the area used. A watermark unit was shared between the address generator and watermark extractor by using two multiplexer. The Technology Schematic of the invisible watermarking modules and the address generation unit are shown in Fig. 4.1, Fig. 4.2, Fig. 4.3 and Fig. 4.4, respectively. The layout of AOI based watermarking module is shown in the Fig: 4.5. The cover image which we used in our proposed method is shown in the Fig: 4.6.

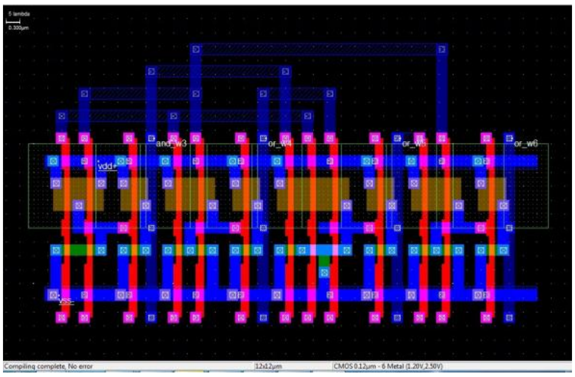
and_w3
or_w4
or_w5
or_w6
vdd
Compiling complete, No error
12x12μm
CMOS 0.12μm - 6 Metal (1.20V,2.50V)

Fig: 4.5 Layout of AOI based watermarking module.

Fig: 4.6. Cover image used in our proposed method of watermarking.

5. Simulation Results

The timing simulation results for the watermark insertion module are shown in Fig. 5.1 and Fig. 5.2 respectively. The simulation waveform of the watermark module used in the watermark and address generation module is shown in Fig. 5.1. The simulation waveform of the watermark extraction is shown in Fig. 5.2. All the values obtained from simulation are the same as the expected values. The synthesis result and timing report is presented in Table 5.1 The cell usage for the different modules and sub-modules are also presented in Table 5.1 which is all the logical cells that are basic elements of the technology. The minimum period is the timing path from a clock to another clock in the design.

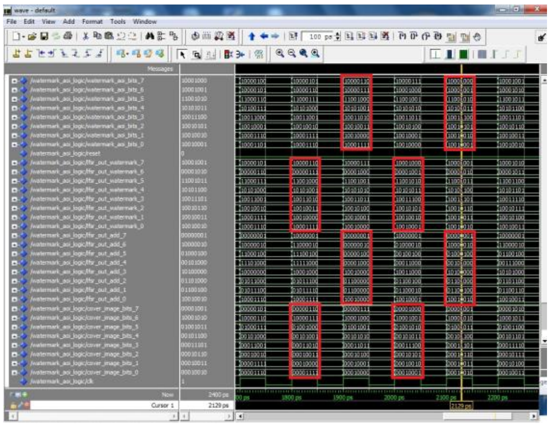

Fig: 5.1 Simulation waveform of Watermarking and Address generation modules

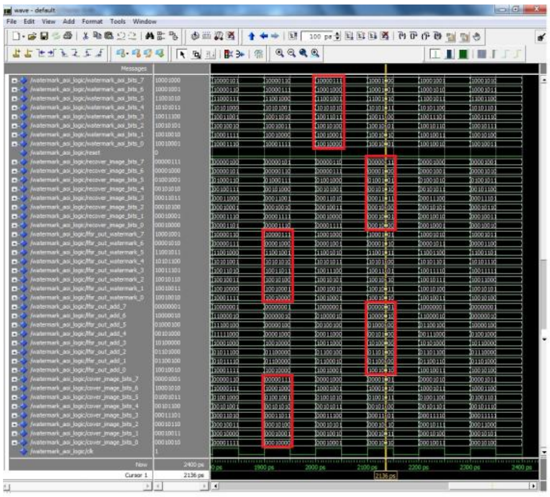

Fig: 5.2 Simulation waveform of watermarking extraction from address locations.

In Fig: 5.1, in first clock pulse the lfsr watermark bits, cover image bits and lfsr address were generated. In second clock pulse lfsr watermarked bits were generated and stored in the address locations of SRAM memory.

In Fig: 5.2, in first clock pulse the address bits from SRAM memory were retrieved and in second clock pulse the watermark retrieving has done.

The above simulation results shows that the performance of watermarking technique has been improved by decreasing the number of clock pulses to perform the watermarking technique. And the power consumption of all the modules is 104.25nW which is very better comparatively.

The PSNR value of the retrieved image bits with transmitted image bits is 45.32, which is comparatively better than the previous proposed method.

Table 5.1. Image Watermark Insertion, Address generation and Watermark Extraction Synthesis Report.

Parameter	Top Module
Adders/ Subtractors (8 bit)	22
Counters	3
Accumulators	7
Registers	248
Xors	1
BELS	219
Slices	172 out of 14752 (1%)
Bonded IOBs	330 out of 376 (87%)
Minimum period	4.223ns
Memory usage	216408 kilobytes

6. Conclusion

The VLSI architecture of the watermarking and encryption scheme that was employed in our proposed paper was presented. The result of the FPGA implementation of the watermarking scheme and the techniques that were employed were also presented. The result of the FPGA prototyping of the watermark generation and extraction was presented. Our implementation of encryption unit yielded a higher throughput. The use of high-end FPGA prototypes has satisfied the capacity and performance requirements of the Digital authentication systems in today's Network security. So, in our paper the blend of both FPGA and watermarking scheme makes the authentication and security an easy and simple procedure.

7. Future Research

Our proposed method of watermarking had shown good results in secure watermark transmission, this will make the data transmission between two nodes of communication a reliable. Our proposed technique of watermarking can be implemented in communication data encryption and decryption technique where secure and reliable data transmission and reception can be made perfect.

In order to obtain a broad perspective on the quality of the watermarking algorithm and FPGA prototype given in this paper, performance statistics with reference to existing hardware based watermarking for video can be presented as a future scope. It is noted that the research presented, can be the current system of achieving real-time video watermarking and compression at rates exceeding existing broadcast standards.

References

[1] S.Bhargav Kumar, S.Jagadeesh, Dr.M.Ashok, "Lfsr Based Watermark And Address Generation For Digital Image Watermarking", International Journal of Computer & Organization Trendz- Volume2 Issue 3-2012, pp 73-79.

[2] R.Sundararaman and Dr. Har Narayan Upadhyay, *Stego System on Chip with LFSR based Information Hiding Approach*, International Journal of Computer Applications (0975 – 8887), Volume 18– No.2, March 2011, pp.24-31.

[3] W.A.S Wijesinghe, M.K Jayananda and D.U.J Sonnadara, *Hardware Implementation of Random Number Generators*, Proceedings of the Technical Sessions, 22 (2006) 28-38, Institute of Physics – Sri Lanka, pp.28-38.

[4] Nebu John Mathai, Student Member, IEEE, Deepa Kundur, Member, IEEE, and Ali Sheikholeslami, Member, IEEE, "*Hardware Implementation Perspectives of Digital Video Watermarking Algorithms*," *IEEE Transactions On Signal Processing, Vol. 51, No. 4, , pp. 925–938, April 2003.*

[5] B. Rajan and S.Ravi, "*FPGA Based Hardware Implementation of Image Filter With Dynamic Reconfigurable Architecture*," in *IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.12, December 2006*, p. 121-127.

[6] Deepthi P.P. and P.S. Sathidevi, "*Hardware Stream Cipher Based on LFSR and Modular Division Circuit*," International Journal of Electrical and Computer Engineering 3:12 2008, pp.791-799.

[7] Saraju P. Mohanty, Renuka Kumara C, and Sridhara Nayak, "*FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder*," CIT 2004, LNCS 3356, pp. 344–353, 2004.

[8] Xiangxue Li, Dong Zheng, and Kefei Chen, "*LFSR-Based Signatures with Message Recovery*," International Journal of Network Security, Vol.4, No.3, pp.266–270, May 2007.

[9] Pankaj U.Lande, Sanjay N. Talbar and G.N. Shinde, "FPGA Prototype of Robust Image Watermarking For JPEG 2000 With Dual Detection", International Journal of Computer Science & Security (IJCSS), Volume (4) : Issue (2), pp-226-236.

[10] Yonatan Shoshan, Alexander Fish, Xin Li, Graham Jullien, Orly Yadid-Pecht, "VLSI Watermark Implementations And Applications", International Journal "Information Technologies and Knowledge" Vol.2 / 2008, pp-379-386.

[11] Kevin Banovic, Mohammed A. S. Khalid, and Esam Abdel-Raheem, "FPGA-Based Rapid Prototyping of Digital Signal Processing Systems", 0-7803-9197-7/05/$20.00 © 2005 IEEE., pp-647-650.

[12] A. Mohamed Zuhair M.E., Lecturer,C. Mohamed Yousuf M.E., Lecturer, "FPGA Based Image Security And Authentication In Digital Camera Using Invisible Watermarking Technique", International Journal of Engineering Science and Technology Vol. 2(6), 2010, pp-1745-1751,