Indian Journal of Science and Technology, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/101888, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Area Efficient High Speed FPGA Based Invisible Watermarking for Image Authentication

Altaf O. Mulani[1] and P. B. Mane[2]

[1]Electronics and Telecommunication Department, Sinhgad Research Center, S. No. 44/1, Off. Sinhgad Road, Vadgaon Budruk, Pune - 411041, Maharashtra, India; aksaltaaf@gmail.com
[2]AISSMS's Institute of Information Technology, Pune, Kennedy Road, Near R.T.O., Pune - 411001, Maharashtra, India; pbmane6829@rediffmail.com

Abstract

Objectives: Present work deals with FPGA based implementation of either watermarking or cryptography alone. Objective is to improve the security using less number of slices with optimum speed. **Methods/Statistical Analysis:** Digital data is easy to process but it allows illegal users to access the data. For protecting data from illegal use, Digital Rights Management can be used. In this paper, hardware implementation of combined watermarking and cryptography algorithm based watermarking is discussed. With this approach, improved security can be achieved due to use of encryption algorithm. Complete system is designed using Verilog and simulated using Questasim and MATLAB Simulink model. **Findings:** The highest performance of FPGA based watermarking algorithm alone achieved is 4708 slices at 344.34 MHz. Our combined watermarking and cryptography algorithm utilizes only 2117 at maximum operating frequency of 228.064 MHz. Due to this improved speed and optimized area, our design is economical for real time image processing applications. At the same time, due to use of AES algorithm it is proved that improved security can be achieved.

Keywords: AES, DWT, Encryption, FPGA, Watermarking

1. Introduction

Digital Rights Management is a collection of different technologies. This technique enables licensing of digital information like image, audio and video. It consists of two important techniques like Cryptography and Watermarking. Cryptography is a technique of converting an information from its normal recognizable form (plain text) into incomprehensible form (cipher text). Cryptography is used to prevent illegal access of digital information. But encryption has its limitation in protecting Intellectual property (IP) rights because once digital information gets decrypted, there is nothing to prevent the user from illegally replicating it. Another technique is required to establish and prove ownership rights, ensure authorized access, facilitate content authentication and prevent illegal replication. This technique is known as Watermarking. Digital Watermarking is used to create metadata containing information about the digital content to be protected and then hide the metadata within the digital content. Information stored as metadata can be character, string or an image pattern. Watermarking technique embeds information in the original digital content so that it can be-detected or extracted by the owner to make necessary assertions about the illegal modifications of the digital content.

In this paper, we have suggested algorithm in both Watermarking and Cryptography algorithms are combined so that improved security of image can be achieved.

2. Literature Survey

In this section, work done previously on FPGA based implementations of image watermarking algorithm along with AES algorithm were discussed individually.

*Author for correspondence

[1]Suggested FPGA based implementation of AES which is suitable for high speed applications in real time. This implementation can be easily reset and immediately erase data on disk. In this implementation, the conventional S-box combinational logic is replaced by BRAM which gives instantaneous output.

[2]Suggested digital image watermarking algorithm design which was simulated using Simulink in MATLAB and then it is converted into HDL using Sysgen tool. This is implemented on virtex-6 FPGA and it occupies 4708 slices.

[3]Proposed FPGA implementation of AES algorithm. In this design, an iterative design method is used to reduce the hardware.

[4]Implemented spatial domain invisible image watermarking algorithm. This is implementation occupies only 457 slices with less power.

[5]Suggested efficient DWT processor which achieves 15% increase in speed.

[6]Proposed an improved version of the integer discrete wavelet transform (integer-DWT) based watermarking technique. With this approach, one can achieve ownership protection.

[7]Proposed a method which uses a concept of nested watermarks using Discrete Wavelet Transform and Cryptography using Spread Spectrum technique.

[8]Discussed a method to combine encryption and watermarking together in digital camera that will assist in protecting and authenticating image files. This DCT based watermarking algorithm is implemented on xc2v500-6fg256.

[9]Presented a novel invisible and blind watermarking technique embeds a binary watermark image invisibly into a host image for copyright protection against piracy of digital images.

[10]Proposed VLSI implementation of robust and fragile invisible image watermarking. It occupies 122 cells and power consumption is of 1.19 mW for this implementation.

[11]Described an imperceptible and robust combined DWT-DCT digital image watermarking algorithm which can improve the performance of watermarking.

[12]Suggested efficient FPGA implementation of AES Algorithm. This efficiency is achieved by pipelining techniques. Increased speed is achieved by processing multiple rounds simultaneously but this increases the area. This algorithm is implemented on Xilinx Virtex-2 device and it occupies 6279 Slices at frequency of 19.954 MHz. With this approach, throughput of 1.18 Gbps is achieved.

[13]Proposed FPGA implementation of fragile watermarking algorithm for content authentication. It requires 1112 slices at frequency of 350 MHz on virtex-6 whereas it requires 2103 slices at a frequency of 260 MHz on virtex-4.

[14]Suggested FPGA oriented invisible image watermarking encoder which requires 838 cells.

[15]Suggested an efficient FPGA implementation of AES algorithm. The proposed implementation is efficient and suitable for hardware critical applications.

[16]Introduced a new multiresolution watermarking technique for digital images which is based on the DWT. Pseudo-random codes are added to the large coefficients at the high and middle frequency bands of the DWT of an image.

[17]Presented an efficient method for hardware implementation of the improved Vigenere cipher. This is achieved by adding random bits of padding to each byte to diffuse the language characteristics and this make the cipher unbreakable.

From the above discussion, it is clear that no one has worked on combined implementation of watermarking and cryptography algorithms for image authentication. The highest performance of FPGA based watermarking algorithm is achieved by[2]. For this implementation, [2]utilized 4708 slices at 344.34 MHz. Due to conversion of MATLAB code to HDL, this implementation occupies more slices. But if the code is written in HDL, it would have occupied less area. Also, if encryption is combined with watermarking, then improved security can be achieved. In this paper, we have implemented DWT along with AES algorithm.

3. Our Method for Image Authentication

Figure 1. shows our proposed architecture. In this FPGA based implementation, initially original image is converted into array form. Then, the complete signal is converted into digital form. Finally, group of bits are stored in a file where thereafter using simulink blocksets an image is read. Similarly, encrypted secret image is also read.

DWT based watermarking is chosen for this implementation because DWT has many applications in

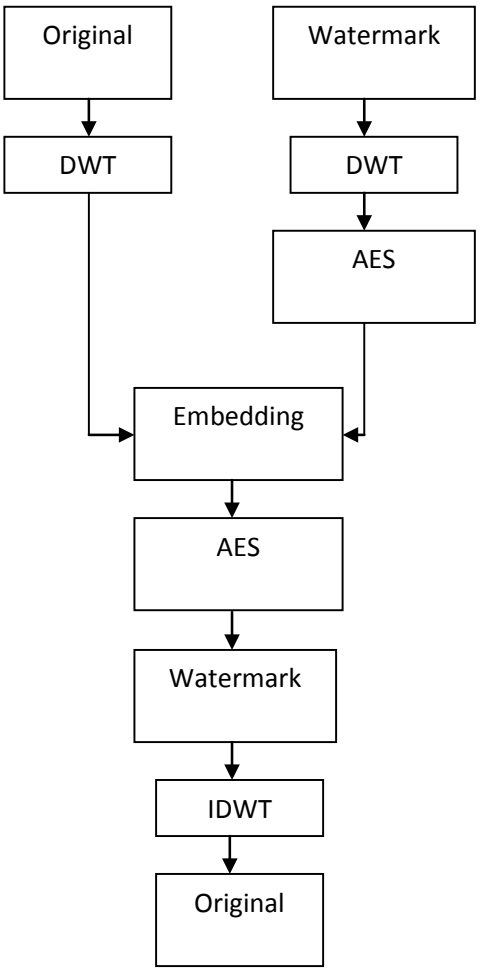

Figure 1. Our architecture.

engineering and science. It is commonly used to code the signal in order for representing a signal in more redundant form. DWT of signal 'x' can be found by passing the signal through series of filters. Initially, these are passed through LPF whose impulse response is 'g'. This results in a convolution as:

$$Y[n] = x[n] * g[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k] \quad (1)$$

Simultaneously, this signal is decomposed using HPF whose impulse response is 'h'. The outputs from HPF are detail coefficients and the outputs from LPF are approximation coefficients. Since DWT is based on sub-band coding, it performs fast computation. It can reduce the computation time and resources required. DWT uses filter banks to construct multiresolution time-frequency plane.

Figure 2. shows an image decomposition using DWT. Decomposing the signal into approximation and detail information, it analyses the signal at different frequency bands with different resolutions. This decomposition is obtained by successive HPFing and LPFing of time domain signal. HPF along with LPF becomes a pair of analysing filters. Each filter output contains half the frequency content and same number of samples as that of input signal whereas HPF outputs along with LPF outputs contain the same frequency content as that of input signal

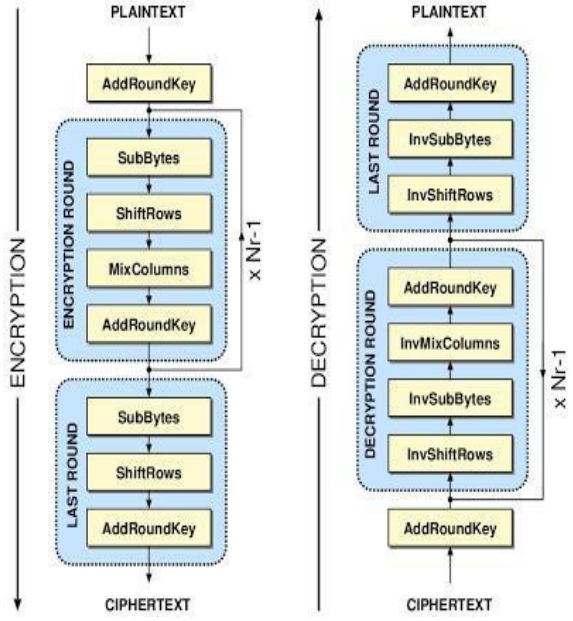

Figure 3. AES process flow.

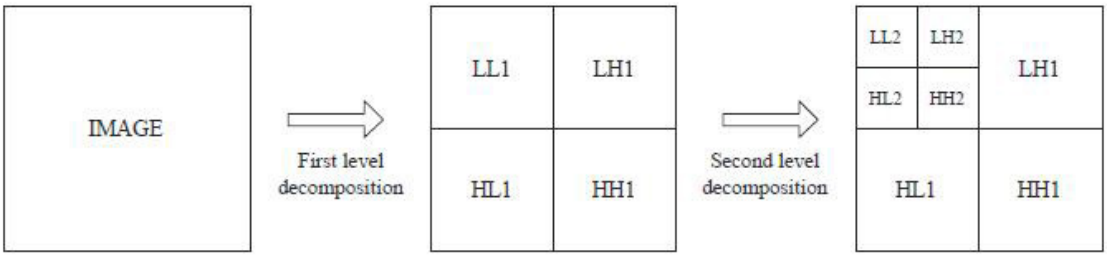

Figure 2. Decomposition of an Image using DWT.

but amount of data is doubled. Hence, filters outputs in analysis bank are down sampled by two.

After image decomposition, bits from original image are embedded into bits from encrypted watermark. Then, using simulink blocksets the embedded output is converted into an image since the output is in bit form.

Another technique which is used in this implementation is AES algorithm. Generally, AES is a cryptographic algorithm used for security purpose. The AES algorithm has 4 phases that execute the process in sequential manner. Encryption process is achieved by processing plain text and key for initial 9 rounds. Decryption process is similar to encryption except that it process in reverse manner. Figure 3. shows block schematic of AES process flow.

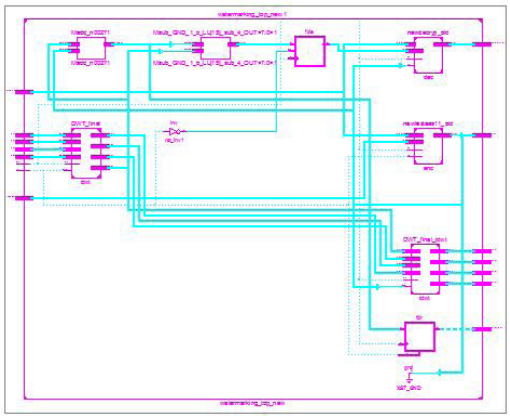

Figure 4. RTL schematic.

AES is a symmetric block cipher used to protect the classified information. In the proposed algorithm, AES encryption is used to encrypt the watermark before embedding process and AES decryption is used to decrypt the watermark after embedding process. By incorporating AES algorithm with watermarking, improved security can be achieved.

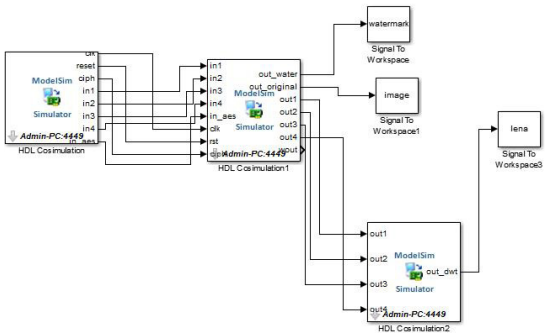

Figure 5. Simulink model of our algorithm.

4. Tools Used

4.1 Software Tools

Xilinx ISE_Design Suite 13.1 is used to synthesize the code. Questasim is used for si-mulation and MATLAB Simulink model is used to convert the bit files into image and vice-versa. Verilog coding is used.

4.2 Hardware Tools

The complete design is implemented on xc6vcx75t-2ff484. Logical blocks available on this device are as shown in Table 1.

Table 1. Characteristics of xc6vcx75t-2ff484

Sr. No.	Characteristics	Available
1	Number of Slice Registers	93120
2	Number of Slice LUTs	46560
3	Number of fully used LUT-Flip Flop pairs	2184
4	Number of bonded IOBs	240
5	Number of BUFG/BUFGCTRLs	32

5. Experimental Results

5.1 Synthesis Result

The synthesis result using xc6vcx75t-2ff484 is as shown in Table 2:

Table 2. Synthesis result

Sr. No.	Logic Utilization	Utilized
1	Number of Slice registers	664
2	Number of Slice LUTs	2117
3	Number of fully used LUT-FFpairs	597
4	Number of bonded IOBs	259
5	Number of BUFG/BUFGCTRLs	1

The synthesis result shows that this implementation occupies only 2117 slices and maximum operating frequency is 228.064 MHz.

5.2 RTL Schematic

The RTL schematic of our design is as shown in figure 4.

5.3 Performance Analysis

Since our implementation is new as we are combining both watermarking and cryptography together and the previous work done is only either on watermarking or on cryptography. But it is very important to compare the performance of our design with existing implementations to evaluate its efficiency. The comparison can be done based on area utilized and its operating frequency.

There are various FPGA implementations available on invisible image watermarking algorithm. Some of which utilizes optimum area and some achieves optimum speed. The Table 3 shows the performance analysis of various implementations. The highest operating frequency achieved in implementing the image watermarking is 344.34 MHz and it occupies 4708 slices. Our work utilizes only 2117 slices and its operating frequency is 228.064MHz.

Table 3. Comparative Analysis of Proposed algorithm with previous work

Authors	Virtex 6		
	Slices	Time (ns)	Frequency (MHz)
Proposed work	2117	4.385	228.064
[1]	4708	2.9	344.34
[2]	457	NA	NA
[4]	122	NA	NA
[5]	1112	NA	NA
[10]	278	6.991	143.04

5.4 Simulink Model of Our Design

Figure 5. shows Simulink model to simulate as well as to convert the outputs from bit form to image.

6. Conclusion

In this implementation, an efficient FPGA based invisible image watermarking along with cryptography for image authentication is suggested. The highest performance of FPGA based watermarking algorithm alone is achieved by[2]. For this implementation, 4708 slices are utilized at 344.34 MHz. Our combined watermarking and cryptography algorithm utilizes only 2117 at maximum operating frequency of 228.064 MHz. Due to this improved speed and optimized area, our design is economical for real time image processing applications. At the same time, due to use of AES algorithm it is proved that improved security can be achieved.

7. References

1. Khose PN and Raut VG. Implementation of AES algorithm on FPGA for low area consumption. International Conference on Pervasive Computing (ICPC). 2015 Jan.
2. Karthigaikumar P, Anumol, Baskaran K. FPGA implementation of High Speed Low Area DWT based invisible image watermarking algorithm. International Conference on Communication Technology and System Design. 2011.
3. Borkar AM, Kshirsagar RV and Vyawahare MV. FPGA implementation of AES algorithm. IEEE International Conference on Electronics Computer Technology (ICECT). 2011 April.
4. Karthigaikumar P and Baskaran K. An ASIC implementation of a low power robust in-visible watermarking processor. International Journal of System Architecture. 2010.
5. Kaur S and Mehra Rajesh. High Speed And Area Efficient 2D DWT Processor Based Image Compression. International Journal of Signal and Image Processing (SIPIJ). 2010 Dec.
6. Jih Yeh, Che-Wei Lu, Hwei-Jen Lin and Hung-Hsuan Wu. Watermarking Technique Based On DWT Associated With Embedding Rule. International Journal of Circuits, Systems And Signal Processing, 2010
7. Husaini Afrin Zahra and Nizamuddin M. Challenges and approach for a robust image water marking algorithm. International Journal of Electronics Engineering. 2010.
8. Mohamed Zuhair A and Mohamed Yousef A. FPGA based image security authentication in digital camera using invisible watermarking technique. International Journal of Engineering Science and Technology. 2010.
9. Dorairangaswamy MA. A Novel invisible and blind watermarking scheme for copyright protection of digital images. International Journal of Computer Science and Network Security. 2009 April.
10. Mohanty Saraju P, Ranganathan N. VLSI architecture and chip for combined invisible robust and fragile watermarking. Proceedings of the IEEE workshop on signal processing system. 2007.
11. Al-Haj Ali. Combined DWT-DCT Digital Image Watermarking. Journal of Computer Science. 2007.
12. Kaur Swinder and Vig R. Efficient Implementation of AES Algorithm in FPGA Device. IEEE International Conference on Computational Intelligence and Multimedia Applications. 2007 Dec.
13. Alomari Raja S and Al Jaber Ahmed. A Fragile watermarking Algorithm for content authentication. International Journal of Computing and Information Science. 2004.

14. Mohanty SP, R Kumara C and Nayak S. FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. Lecture Notes in Computer Science (LNCS), CIT 2004. Springer-Verlag. 2004.
15. Shuenn-Shyang Wang and Wan-Sheng Ni. An efficient FPGA implementation of advanced encryption standard algorithm. International Symposium on Circuits and Systems (ISCAS). 2004 May.
16. Wolfgang RG, Delp EJ. A watermark for digital images. IEEE International Conference on Image Processing (ICIP). 1996.
17. Sokouti Massoud, Sokouti Babak, Pashazadeh Saeid, Khanli Leili Mohammad. FPGA implementation of improved version of the Vigenere cipher. Indian Journal of Science and Technology. 2010 Apr; 3(4). DOI: 10.17485/ijst/2010/v3i4/29736.