Bulletin of Electrical Engineering and Informatics
ISSN: 2302-9285
Vol. 6, No. 2, June 2017, pp. 181~187, DOI: 10.11591/eei.v6i2.651

Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform

Altaf O. Mulani[1]*, P. B. Mane[2]
[1]Department of Electronics & Telecommunication Engineering, Sinhgad Research Center, Pune, Maharashtra, India
[2]Principal, AISSMS's Inst. of Information Technology, Pune, Maharashtra, India
*Corresponding author, e-mail: aksaltaaf@gmail.com

Abstract

Now-a-days, multimedia based applications have been developed rapidly. Digital information is easy to process but it allows illegal users to access the data. For protecting the data from this illegal use, Digital Rights Management (DRM) can be used. DRM allows secure exchange of digital data over internet or other electronic media. In this paper, FPGA based implementation of DWT alongwith Advanced Encryption Standard (AES) based watermarking is discussed. With this approach, improved security can be achieved. The complete system is designed using HDL and simulated using Questasim and MATLAB Simulink model. The synthesis result shows that this implementation occupies only 2117 slices and maximum frequency reported for this design is 228.064 MHz.

Keywords*: DRM, AES, DWT, FPGA, watermarking, encryption, multimedia*

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 Encryption and Watermarking. Encryption is a technique of converting information from its normal recognizable form (plain text) into incomprehensible form (cipher text). Encryption can be used to prevent unauthorized 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 Watermarking technique. Digital Watermarking is a technique 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.

Watermarking and encryption algorithms can be combined to improve the security of the watermarks. In proposed algorithm, watermark is first encrypted and then the encrypted output is embedded with the original image. With this approach, more secure transmission of image can be achieved.

This section provides the overview about some of FPGA implementations of digital image watermarking algorithm and AES algorithm individually.

P Karthigaikumar el at [1] suggested a method in which whole digital image watermarking algorithm is designed and simulated using Simulink block in MATLAB and then the algo-rithm is converted into HDL using system generator tool. The algorithm is implemented on virtex-6 FPGA and it occupies 4708 slices.

P Karthigaikumar el at [2] introduced a method to implement low power robust invisible wa-termarking algorithm in spatial domain. This implementation occupies 457 slices with less power. The algorithm is implemented both in FPGA and ASIC.

Received March 9, 2017; Revised May 10, 2017; Accepted May 24, 2017

Sarju P Mohanty el at [4] introduced VLSI architecture and chip for combined invisible ro-bust and fragile watermarking. It occupies 122 cells and consumes1.19 mW power for FPGA implementation of image watermarking algorithm.

A Mohamed Zuhair el at [5] discussed a method to combine encryption and watermarking to-gether in digital camera that will assist in protecting and authenticating image files. In this paper, DCT based watermarking algorithm is implemented on xc2v500-6fg256.

Raja S Alomari el at [9] suggested FPGA implementation of Fragile watermarking algorithm that occupies 1112slices at frequency of 350 MHz that is implemented on virtex-6 FPGA and other occupies 2103 slices at a frequency of 260 MHz that is implemented on virtex-4 FPGA. This watermarking algorithm is used for content authentication.

Sarju P Mohanty [10] discussed FPGA based invisible robust image watermarking encoder that occupies 838 cells for FPGA implementation.

Sugrev Kaur et al [11] suggested a high speed area efficient DWT processor which achieves 15% increase in speed.

Borkar A.M. el at [13] discussed FPGA implementation of AES algorithm using VHDL. Author has used an iterative design approach to minimize the hardware consumption.

Kaur el at [14] presented an efficient FPGA implementation approach of the Advanced Encryption Standard (AES) Algorithm. The architectural optimization is achieved by pipelining techniques. Speed is increased by processing multiple rounds simultaneously but at the cost of increased area. Algorithm is implemented on Xilinx Virtex XC2VP70-7 device and it occupies 6279 Slices. A 119.954 MHz clock frequency is achieved which translates to a throughput of 1.18 Gbps using and 5 BRAMs.

Shuenn-Shyang Wang el at [15] proposed an efficient FPGA implementation of advanced encryption standard (AES). The proposed implementation is efficient and suitable for hard-ware-critical applications.

KhoseP.N. el at [16] suggested that hardware implementation of AES is more suitable for high speed applications in real time. Implementation of AES algorithm 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.

From the above discussion, it is clear that no one has worked on combined implementation of watermarking and encryption algorithms for image authentication. The highest performance of FPGA based watermarking algorithm is achieved by [1]. For this implementation, P Karthigaikumar 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.

2. Research Method

In FPGA implementation of digital image watermarking for image authentication, original image is first converted into vector form. Then, the entire decimal signal is converted into binary signals which mean bit form. The group of bits stored in a file and using the simulink block sets read an image in a bit by bit format. The secret image also read in the same way except that it is encrypted.

DWT based watermarking is chosen for this implementation because DWT has huge number of applications in engineering, computer science, mathematics and science. DWT is commonly used for signal coding to represent a discrete signal in a more redundant form i.e. as a preconditioner for compression. DWT of a signal 'x' is calculated by passing it through a series of filters [11]. Initially, the samples are passed through a low pass filter (LPF) with impulse response 'g' resulting in a convolution:

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

Then the signal is decomposed simultaneously using a high pass filter (HPF) 'h'. The outputs give the detail coefficients which are coming from HPF and approximation coefficients

which is coming from LPF. Since DWT is based on sub-band coding, it is found to yield a fast computation of Wavelet Transform. Due to this, it is easy to implement and reduces the computation time and resources required. It uses filter banks for the construction of multi-resolution time-frequency plane [11].

Figure 1. shows the research method for image authentication.

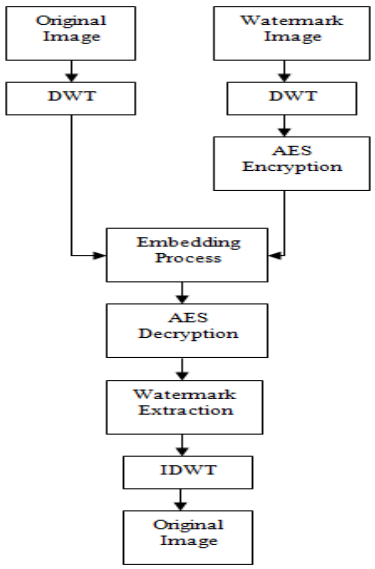

Figure 1. Research method for image authentication

Figure 2. shows the decomposition of an image using DWT

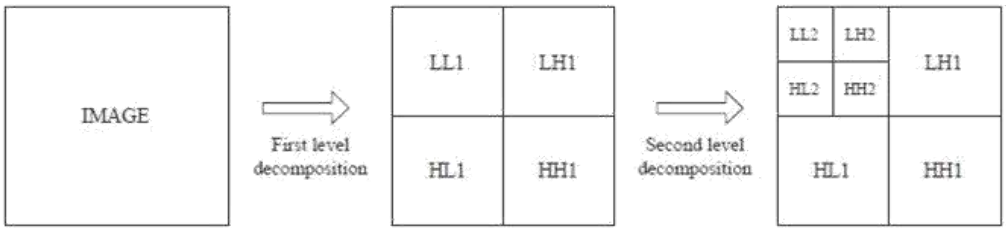

Figure 2. Image decomposition using DWT

DWT analyzes the signal at different frequency bands with different resolutions by decomposing the signal into an approximation and detail information. Decomposition of a signal into different frequency bands obtained by successive high pass filtering g[n] and low pass filtering h[n] of the time domain signal. The combination of high pass g[n] and low pass filter h[n] comprise a pair of analyzing filters. Output of each filter contains half the frequency content, but an equal amount of samples as the input signal. Two outputs together contain the same frequency content as the input signal; however the amount of data is doubled. Hence, down sampling by two is applied to the outputs of the filters in the analysis bank.

After DWT decomposition of original image, bits from the encrypted watermark is embedded into the bits of original input image. Then, the embedded output is converted into an image since it is in bit form using Simulink block set to get the Watermarked image.

Another technique which is used in this implementation is Advanced Encryption Standard (AES) algorithm. Basically, AES algorithm 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.

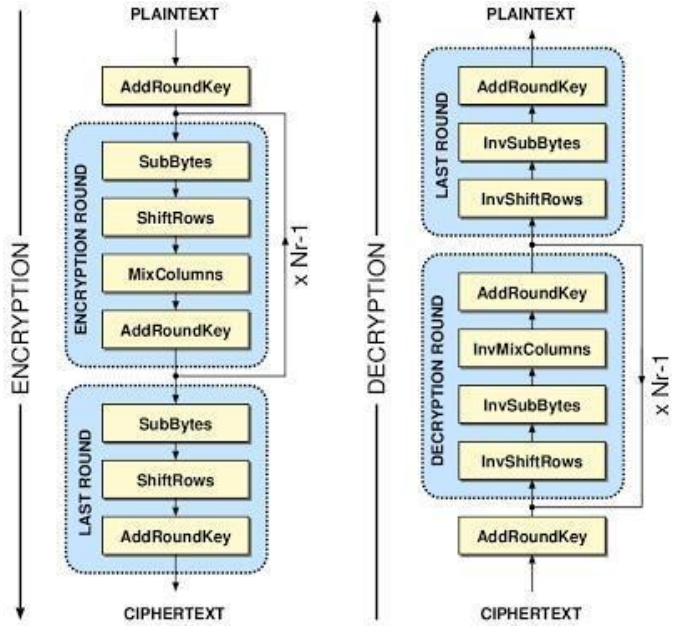

Figure 3. AES process flow

AES algorithm 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 decrypt the watermark after embedding process. By incorporating AES algorithm with watermarking, improved security can be achieved.

3. Tools Used

3.1. Software Tools

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

3.2. 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-FF pairs	2184
4	Number of bonded IOBs	240
5	Number of BUFG/BUFGCTRLs	32

4. Experimental Results

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 frequency reported for this design is 228.064 MHz.

RTL schematic:

The RTL schematic for the entire design is shown in Figure 4.

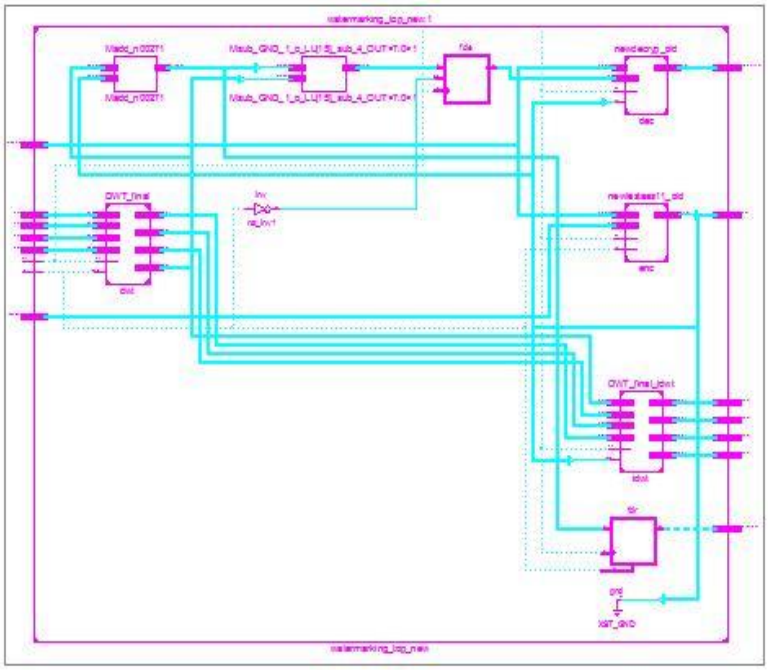

Figure 4. RTL schematic

Simulink Model of Our Work:

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

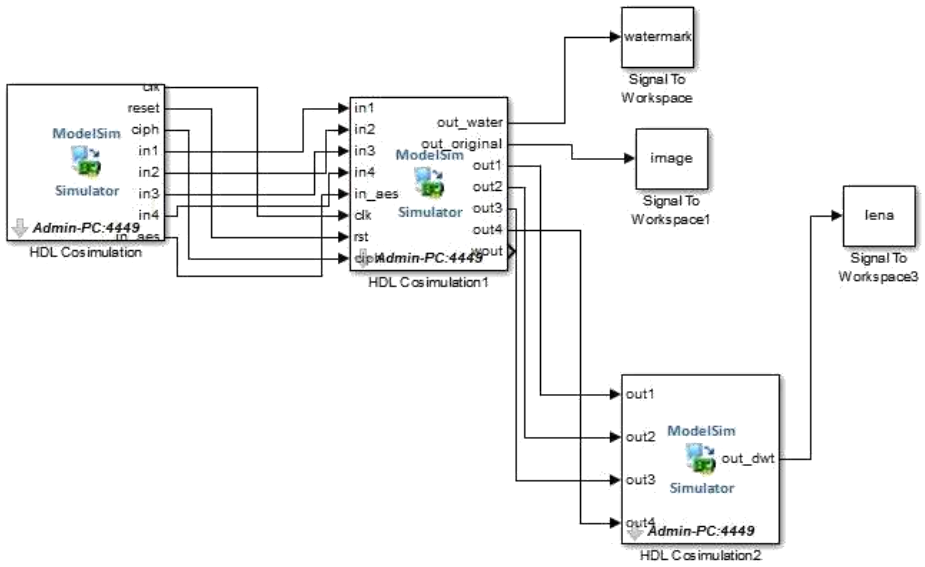

Figure 5. Simulink model of proposed algorithm

5. Performance Analysis

It is very important to compare the performance of proposed design with existing implementations for evaluating the efficiency. The comparison is done on the basis of area requirements, time and operating frequency.

The related works shows that different architectures are available for invisible robust image watermarking algorithm to get sufficient area requirements, speed which are suitable for various applications. The table 3 shows the comparative analysis of the proposed algorithm with previous work done. The highest operating frequency reported in the previous works is 344.34 MHz with 4708 slices. The proposed work utilizes only 2117 slices and it gives maximum frequency of 228.064MHz.

Table 3: Comparative Analysis of Proposed Algorithm with Previous Work

Authors	Slices	Time (ns)	Virtex 6 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

6. Conclusion

In this proposed algorithm, high speed and area efficient DWT based robust invisible image watermarking technique for image authentication was performed. The highest performance of FPGA based watermarking algorithm is achieved by P Karthigaikumar [1]. For this implementation, 4708 slices are utilized at 344.34 MHz. FPGA implementation of proposed robust invisible digital image watermarking algorithm can operate at a maximum frequency of 228.064 MHz. This improved speed has been achieved by consuming only 2117 slices of the FPGA device to provide cost effective solutions 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.

References

[1] P Karthigaikumar, Anumol, K Baskaran. FPGA Implementation of High Speed Low Area DWT Based Invisible Image Watermarking Algorithm. *International Conference on Communication Technology and System Design*. 2011, 2012; 30: 266–273.

[2] P Karthigaikumar, K Baskaran. An ASIC Implementation of a Low Power Robust In-visible Watermarking Processor. *International Journal of System Architecture*. 2010: 57(4): 404-411.

[3] MA Dorairangaswamy. A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images. *International Journal of Computer Science and Network Security (IJCSNS)* 2009; 9(4):71-78.

[4] Saraju P Mohanty, N Ranganathan. *VLSI Architecture and Chip for Combined Invisible Robust and Fragile Watermarking.* in Proceedings of the IEEE Workshop on Signal Processing System. 2007.

[5] A Mohamed Zuhair, A Mohamed Yousef. FPGA Based Image Security Authentication in Digital Camera Using Invisible Watermarkingtechnique. *International Journal of Engineering Science and Technology*. 2010, 2(6):1745-1751.

[6] Ali Al-Haj. Combined DWT-DCT Digital Image Watermarking. *Journal of Computer Science*. 2007; 3 (9): 740-746.

[7] RG Wolfgang, EJ Delp. *A Watermark for Digital Images* in: Proceedings of the IEEE International Conference on Image Processing (ICIP). 1996; 3: 219–222.

[8] Afrin Zahra Husaini, M Nizamuddin. Challenges and Approach for a robust Image Water Marking Algorithm. *International Journal of Electronics Engineering*. 2010; 2(1): 229-233.

[9] Raja S Alomari, Ahmed Al Jaber. A Fragile Watermarking Algorithm for Content Authentication *International Journal of Computing and Information Science*. 2004; 2(1): 27-37.

[10] SP Mohanty, R Kumara C, S. Nayak. FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. *LectureNotes in Computer Science (LNCS)*, CIT 2004, Springer-Verlag. 2004. 3356: 344-353.

[11] Sugreev Kaur, Rajesh Mehra. High Speed and Area Efficient 2D DWT Processor Based Image Compression. *Signal &Image Processing: An International Journal Sipij*. 2010; 1(2):22-31.

[12] Jih Pin Yeh, Che-Wei Lu, Hwei-Jen Lin, Hung-Hsuan Wu. Watermarking Technique Based On DWT Associated With Embedding Rule. *International Journal of Circuits, Systems and Signal Processing*, 2010; 2(4): 72-82.

[13] Borkar AM, Kshirsagar RV, Vyawahare MV. *FPGA Implementation of AES Algorithm*. IEEE International Conference on Electronics Computer Technology (ICECT), April 2011.

[14] Kaur Swinder, Vig R. *Efficient Implementation of AES Algorithm in FPGA Device*. IEEE International Conference on Computational Intelligence and Multimedia Applications, Dec. 2007.

[15] Shuenn-Shyang Wang, Wan-Sheng Ni. *An Efficient FPGA Implementation of Advanced Encryption Standard Algorithm.* International Symposium on Circuits and Systems (ISCAS) May 2004.

[16] Khose PN, Raut VG. *Implementation of AES Algorithm on FPGA for Low Area Consumption*. International Conference on Pervasive Computing (ICPC). Jan 2015.