Secure and area Efficient Implementation of Digital Image Watermarking on Reconfigurable Platform

Altaf O. Mulani, P. B. Mane

Abstract*: Now a day digital data is easy to process but it permits unauthorized consumers to access this information. To protect this information from unauthorized access, cryptography and watermarking are the commonly used techniques. In this paper, implementation of fast and area efficient Discrete Wavelet Transform (DWT) oriented invisible image watermarking system integrated with cryptography on reconfigurable platform is suggested. In DWT implementation, simplified formulae are derived for generation of approximation and detailed coefficients due to which this operation utilizes simply 306 slice registers and its maximum operational frequency is 556.174 MHz. In AES implementation, keys are initially generated using MATLAB and then these keys are used in the Xilinx System Generator based model due to which this implementation occupies 121 slice registers and its maximum operating frequency is 1102.536 MHz. Complete system is designed using Xilinx SysGen tool and Vivado. Simulation is accomplished using MATLAB Simulink. Watermark embedding system is implemented on Artix7 FPGA (xc7a100t-1csg324) and it utilizes 2961 slices at maximum operating frequency of 148.895 MHz. Watermark extraction system is implemented on Artix7 FPGA (xc7a35t-1cpg236) and it occupies 87 slices.

Index Terms*: Watermarking, Cryptography, DWT, AES, FPGA, VLSI.

I. INTRODUCTION

In the preceding decade, fast improvement in information technology and the extensive accessibility of digital customer device took place. However, at the same time, this leads to hacking susceptibility and duplication of the unique data. In order to protect this digital information from unauthorized access, Digital Rights Management (DRM) can be used which contains two methods viz. Cryptography and Watermarking. *Cryptography* is a process of sending the data in encrypted form so that only authorized users can access this data. Cryptography are classified into two types depending on types of key used. First, symmetric key cryptography, in which similar key is utilized in encryption as well as decryption. Second, asymmetric key cryptography, in which public key is used to encrypt the information and private key is used to decrypt the information. Digital information is represented in the form of bits rather than alphabets. Based on how these binary numbers are processed, symmetric key cryptography is classified into two types i.e. block cipher and stream cipher. In block cipher, plaintext is processed in blocks (group of bits) at a time whereas in stream cipher, plain text is processed one bit at a time. *Digital Watermarking* is a process of adding secret data related to digital information like image, audio, video, etc. within the information itself. Based on human perception, digital watermarking can be categorized into two types viz. *Visible watermarking* and *invisible watermarking*. In visible watermarking, watermark is clearly noticeable whereas in invisible watermarking, watermark is not noticeable. Invisible watermarking technique is more strong to signal processing attacks.

Watermarking can also be categorized into *Spatial domain technique* and *Transform (Frequency) domain technique* based on the process to embed the data. In transform domain technique, transform coefficients are modified instead of pixel values and inverse transform is used to extract the watermark.

DCT and DWT are frequently used transform domain techniques. In Spatial domain technique, watermark bits are directly embedded to the pixels of the cover image. Transform domain techniques are able to deliver better robustness against compression and filtering attacks, since coefficients of watermark are spread all over the cover image.

II. LITERATURE SURVEY

Altaf O. Mulani et al [1] proposed an effective FPGA implementation of DWT for image compression which can be applied for lossy as well as lossless compression. It utilizes 144 slice registers at an operational frequency of 43.63 MHz. Priyanka R. Kulkarni et al [2] recommended MATLAB based robust invisible image watermarking. This design was tested by applying various images and result shows that suggested design is robust. Altaf O. Mulani et al [3] discussed implementation of DRM techniques on FPGA and it uses 2117 slices at maximum operational frequency of 228.064 MHz and is useful for real time image processing applications. Adesh Kumar et al [4] suggested a system that focuses on the design, modeling and simulation using VHDL. The scheme was employed on Virtex-5 and it utilizes 249 slices and its operating frequency is 400 MHz. Priyanka R. Kulkarni et al [5] discussed MATLAB and DWT based robust invisible image watermarking. This design was tested by applying various colour and gray scale images and result shows that the suggested design is robust. The main goal of Khose P. N. et al [6] is hardware implementation of AES algorithm which uses less area and power consumption at the same time retain normal throughput. In the proposed design, general S-box logic is substituted by BRAM which generates instant output.

Revised Manuscript Received on 10 December 2018.

Altaf O. Mulani, Department of Electronics & Telecommunication, AISSMS Institute of Information Technology, Pune (Maharashtra), India

Dr. P. B. Mane, Department of Electronics & Telecommunication, AISSMS Institute of Information Technology, Pune (Maharashtra), India

Della B et al [7] suggested a information securing method based on steganography that is used to hide multiple color images into a single color image using DWT. Altaf O. Mulani et al [8] recommended an efficient implementation of DES on less dense FPGA. P. Karthigaikumar et al [9] proposed System Generator based hardware design in which initially watermark is inserted in the original information for validation. Synthesis result shows that this design utilizes 4708 slices and its operating frequency is 344 MHz. Borkar A. M. et al [10] suggested FPGA based AES algorithm which was simulated and optimized using software. In this design, an iterative design approach is used to reduce hardware. P. Karthigaikumar et al [11] presented ASIC implementation of crypto algorithm. The blowfish cryptography is prototyped in 130 nm custom IC. Kaur S. et al [12] proposed System Generator based partly pipelined sequential structure to improve the speed and resource utilization. It's operational frequency is 231 MHz by consuming power of 117mW at junction temperature of 28^0. Jih Yeh et al [13] recommended a technique which is able to achieve ownership protection. In the proposed design, initially original image is passed through Discrete Wavelet Transformations and then embedded with watermark in HL and LH blocks. Husaini Afrin Zahra et al [14] discussed various challenges and approaches in robust image watermarking algorithm. Mohamed Zuhair A. et al [15] presented a unique method in which biometric information is embedded into an image. Dorairangaswamy M.A. [16] presented a different method for protection of official document against piracy. Mohanty Saraju P. et al [17] presented the development of a VLSI structure for a high performance spatial domain watermarking chip that is able to achieve both invisible robust and fragile image watermarking. Al-Haj Ali [18] described robust invisible joint DWT-DCT digital image watermarking algorithm. Kaur Swinder et al [19] suggested an effective FPGA implementation of AES Algorithm which includes pipelining techniques as a part of architectural optimization. An optimized code is employed using Virtex-2 which utilizes 6279 Slices and 5 BRAMs at maximum operating frequency of 19.954 MHz. Chao-Tsung Huang et al [21] recommended complete analysis of VLSI structures for the 1-D and 2-D DWT and proposed three related design.

From literature review, it is clear that till now only one design is implemented but the result achieved by [3] is not that much efficient as compared to results of proposed design. Also there are various authors those have worked either on FPGA based digital image watermarking or on FPGA based AES algorithm implementations. The efficient result of FPGA based DWT oriented digital image watermarking is accomplished by [3]. For this employment, 2117 slices were used at maximum operating frequency of 228.064 MHz. Also there are various authors who have implemented image watermarking on reconfigurable platform but the result achieved are less efficient due to conversion of MATLAB code to HDL. Due to this kind of operation, design uses more area and also the operating frequency is less which affects the speed of the system. However, if design is done with HDL or system generator, an area efficient and optimum speed can be achieved. In addition, if cryptography is combined with watermarking, system can be more secure. In this paper, DWT based digital image watermarking along with AES algorithm on reconfigurable platform is recommended.

2. Proposed Design

Fig. 1. shows Watermark Embedding process for proposed design.

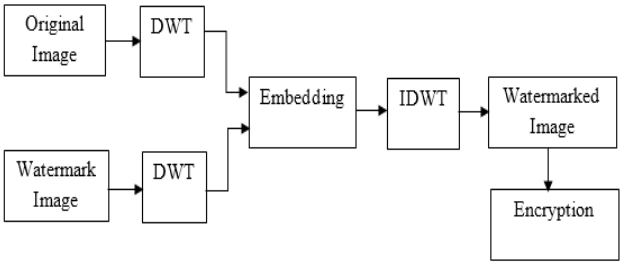


Fig. 1. Watermark Embedding Process

In watermark embedding, both original image and watermark are initially passed through DWT. Then the embedded output is passed through inverse DWT to get the watermarked image. Further, watermarked image is passed through AES encryption to produce encrypted watermarked image. Fig. 2. shows extraction of watermark.

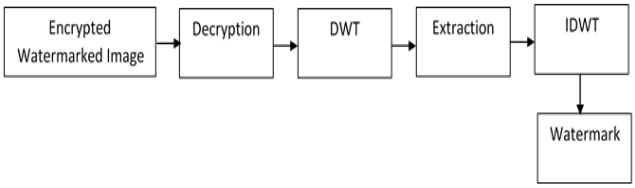


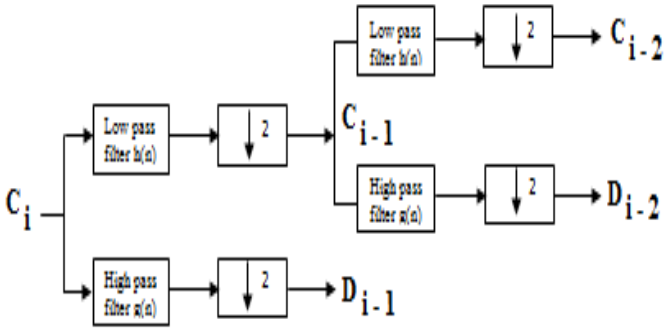
Fig. 2. Extraction of Watermark

In watermark extraction, encrypted watermarked image is fed as input to AES decryption which will give watermarked image as an output. Then, the watermarked image is wavelet decomposed. Then, the watermark is extracted using inverse DWT.

The main components of watermark embedding and watermark extraction are DWT-IDWT and AES Encryption and Decryption.

2.1. DWT and IDWT Implementation:

DWT is an implementation of transform in which wavelets are discretely sampled. It is an application of sub-band coding. In sub-band coding, input spectrum is decomposed into set of band limited components called sub-bands. These sub-bands can be assembled to reconstruct the original spectrum without an error. Generally, the structure used for wavelet analysis is as shown in the fig. 3 [1].



where Cx = Approximation coefficients
Dx = Detail coefficients

Fig. 3. One-Dimensional DWT Decomposition

DWT decomposes a signal into different sub-bands in order to get the lower frequency sub-bands that have finer frequency resolution and higher frequency sub-bands for coarser time resolution. Decomposition of an image can be single level, two level or three level as shown in fig. 4.

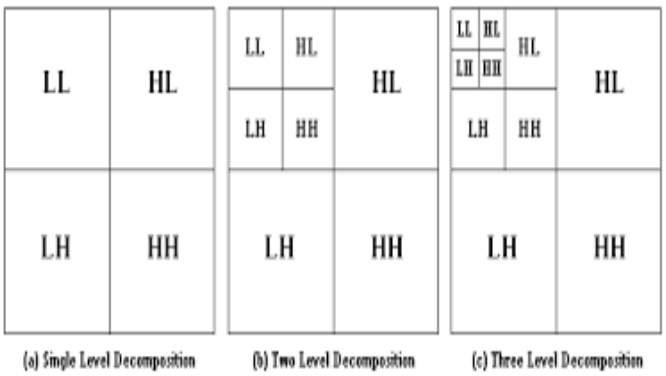


Fig. 4. DWT Decomposition

In proposed work, Approximation and detail coefficients are obtained using right shift and left shift operation instead of using multipliers and dividers. Due to this, area (slices/LUTs) required gets reduced. Also, operating frequency of this implementation is optimized.

Fig. 5. shows implementation of DWT-IDWT using system generator.

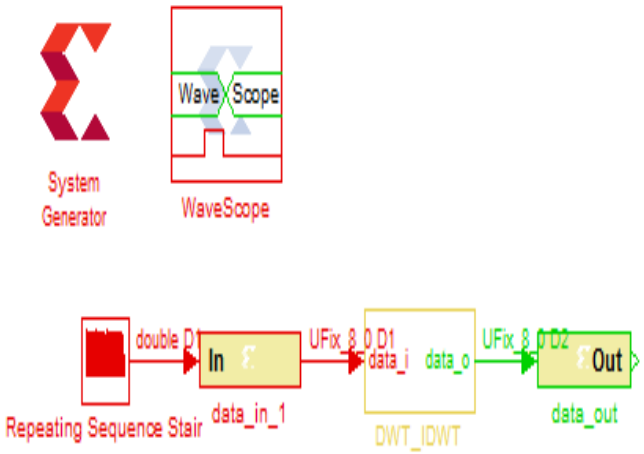


Fig. 5. System Generator based DWT-IDWT Implementation

Table 1. shows Design utilization summary of DWT and IDWT implementation on FPGA.

Table 1: Design Utilization Summary for DWT-IDWT

Logic Utilization	Used	Available
Slice Registers	287	126800
Slice LUTs	293	63400
Fully used LUT-FF pairs	250	114
Boded IOBs	56	210
BUFG/BUFGCTRLs	1	32

Fig. 6.Shows RTL schematic of DWT-IDWT Implementation

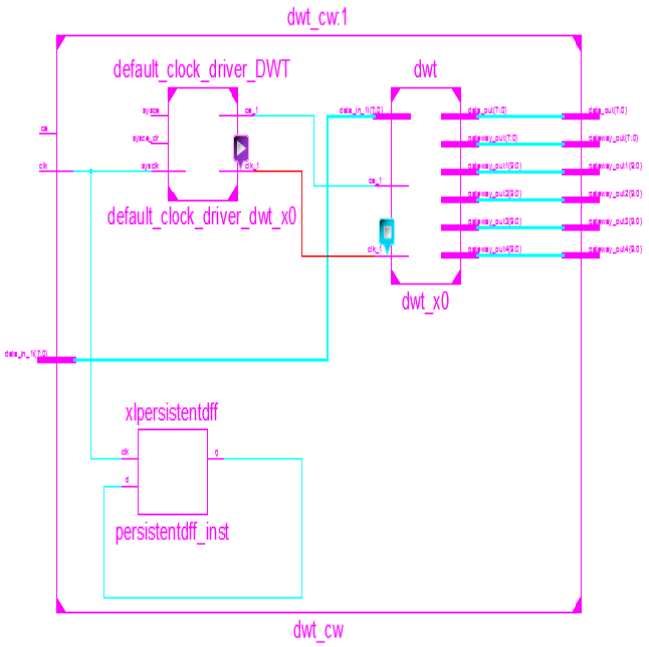


Fig. 6. RTL Schematic of DWT-IDWT Implementation

Fig. 7. shows implementation result for lena image.

a. Input Image

b. Single Level Decomposed Image

c. Reconstructed Image

Fig. 7. Implementation Result of DWT-IDWT

2.2. Implementation of AES Algorithm:

AES is a symmetric key block cipher because it allows the same key to be used in encryption as well as decryption. Design of AES algorithm is based on linear transformation.

In proposed work, keys for all rounds are generated using MATLAB programming and the same is used in VHDL code. Due to this, number of slices required for key generation process gets reduced.

Input to this algorithm is 128 bit block of plaintext and 128 bit block of key for both encryption and decryption. Fig. 8. shows implementation of AES algorithm using system generator.

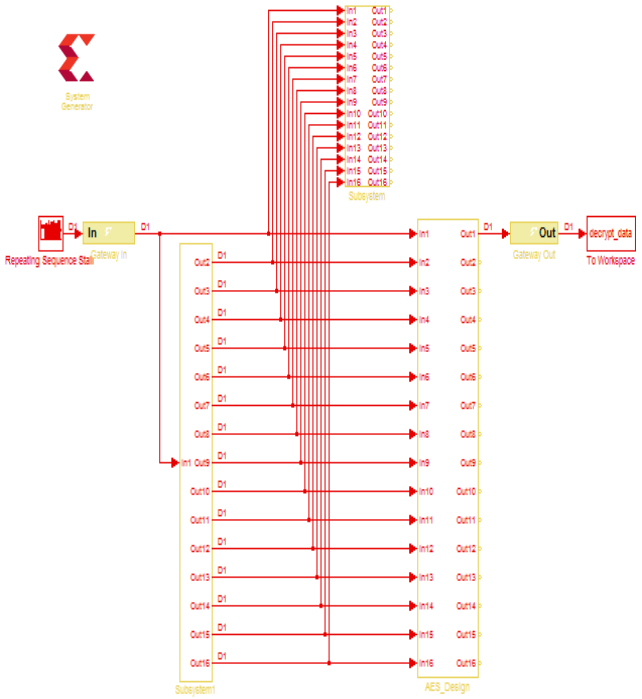


Fig. 8. Implementation of AES Algorithm using System Generator.

Table 2 shows Design utilization summary of AES algorithm implementation on FPGA.

Table 2. Design Utilization Summary for AES Algorithm

Logic Utilization	Used	Available
Slice Registers	121	126800
Slice LUTs	4782	63400
Fully used LUT-FF pairs	3	4900
Boded IOBs	25	210
BUFG/BUFGCTRLs	1	32

Fig. 9. shows RTL schematic of AES algorithm.

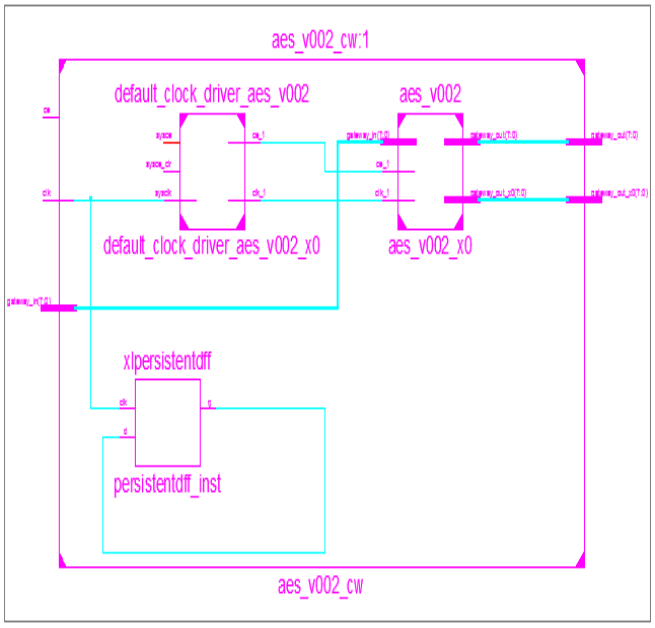


Fig.9. RTL Schematic of AES Algorithm

Fig. 10. shows Implementation Result of AES Encryption & Decryption

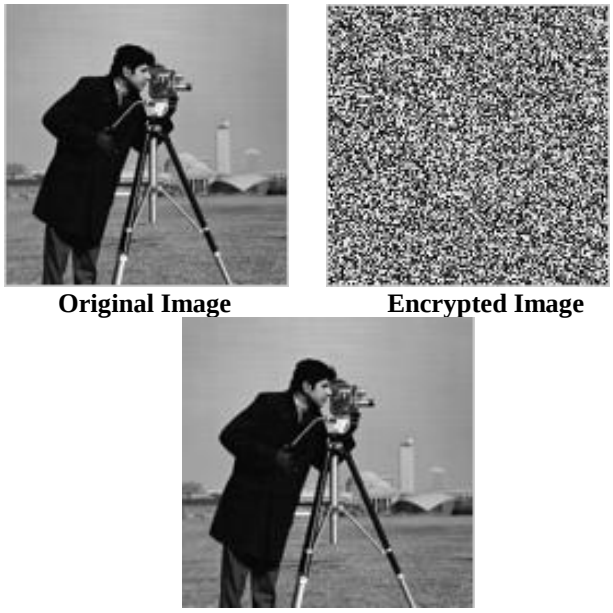


Fig. 10. Implementation Result of AES Encryption & Decryption

2.3. Overall Design Implementation:

Table 3 shows Device utilization summary for implementation of overall design.

Table 3: Device Utilization Summary for Implementation of Overall Design

Logic Utilization	Used	Available
Slice Registers	1851	126800
Slice LUTs	2961	63400
Fully used LUT-FF pairs	1360	4629
BUFG/BUFGCTRLs	1	32
Number of BRAM/RAM	4	135

Fig. 11. shows detailed RTL schematic of proposed design.

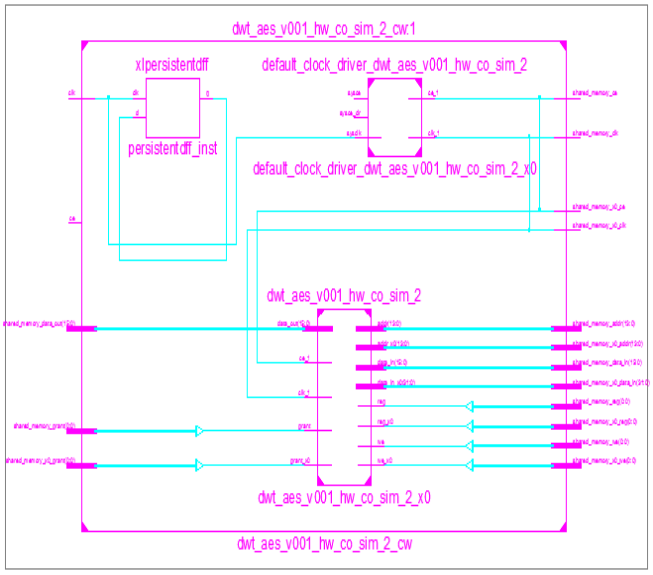
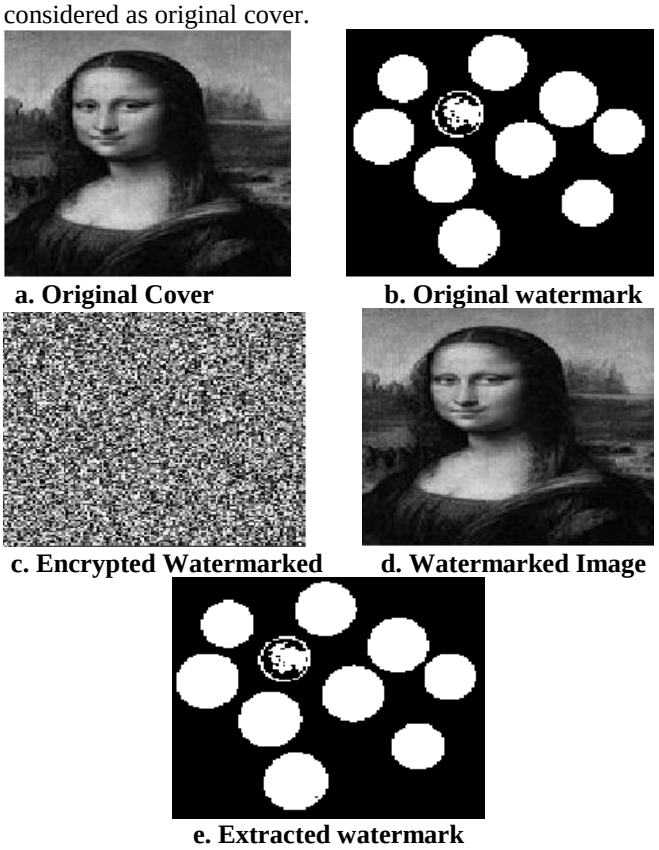


Fig. 11. RTL Schematic of Overall Design

The working of proposed design is tested by applying various images.

Fig. 12. shows one of the result where image of coins is considered as original watermark while other image is considered as original cover.



a. Original Cover b. Original watermark

c. Encrypted Watermarked d. Watermarked Image

e. Extracted watermark

Fig. 12. Various Results of Overall Implementation

The complete system is also simulated using MATLAB 2012 (System Generator based Simulink Model) and the results of the same by considering various inputs are as shown in Table 4.

Table 4: Simulation Results for Various

Sr. No.	Original watermark	Original Cover	PSNR	MSE
1	Penguin	Cameraman	49.72	0.6928
2	Coins	Cameraman	53.87	0.2667
3	Circuit	Cameraman	53.07	0.321
4	Rice	Cameraman	55.98	0.1641
5	Peppers	Cameraman	53.76	0.2733
6	Penguin	Lifting Body	49.74	0.6908
7	Coins	Lifting Body	53.87	0.2668
8	Circuit	Lifting Body	53.07	0.3207
9	Rice	Lifting Body	55.99	0.1638
10	Peppers	Lifting Body	53.79	0.2714

Simulink model for the overall implementation is prepared using MATLAB 2013. Fig. 13. shows Simulink model of our system generator based design.

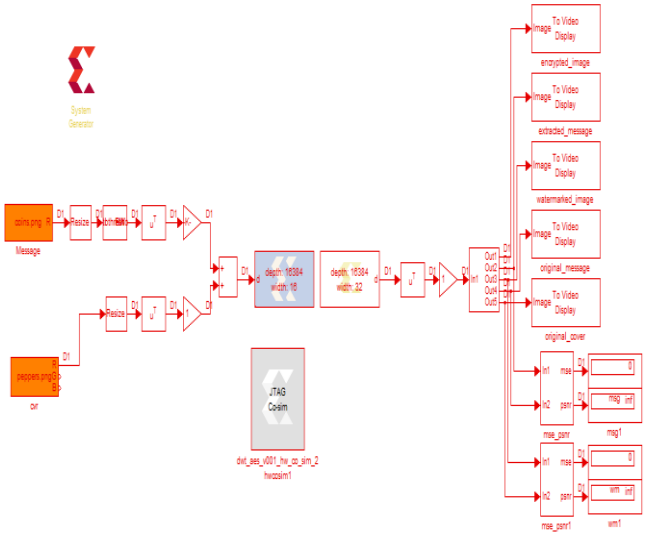


Fig. 13. Simulink Model of Proposed Design

3. Performance Analysis:

Comparison of our system with existing FPGA based implementations is required to evaluate proposed system's performance or efficiency. As this is a novel FPGA based system, we have compared the result of fairly similar FPGA based watermarking implementation. There are various FPGA based implementations which shows effective implementation of watermarking alone either in area utilization or in operating frequency.

Table 5 Shows the Comparative Analysis of Various Implementations.

Authors	Slices	Time (ns)	Frequency (MHz)
Proposed Work	2961	6.716	148.895
[3]	2117	4.385	228.064
[9]	4708	2.9	344.34

Table 5: Comparative analysis of various implementations

III. CONCLUSION

In this paper, secure and effective FPGA implementation of digital image watermarking is suggested. As per the literature survey, it is clear that the efficient performance of FPGA based image watermarking alone till now is accomplished by [3] which utilizes 2117 slices at maximum operating frequency of 228.064 MHz. Recommended design combines both DWT based watermarking and cryptography. Proposed design uses 2961 slices and its operational frequency is 148.895 MHz. Due to this improved speed and optimized area, proposed implementation is more efficient for image processing applications and also it is more secure due to integration of cryptographic algorithm.

REFERENCES

1. Mulani Altaf O. and P. B. Mane. "An Efficient implementation of DWT for image compression on reconfigurable platform", International Journal of Control Theory and Applications, Jan. 2017.
2. Kulkarni Priyanka R., Altaf O. Mulani and P. B. Mane, "Robust Invisible Watermarking for Image Authentication." Emerging Trends in Electrical, Communications and Information Technologies: Proceedings of ICECIT-2015. Springer Singapore, 2017.

3. Altaf O. Mulani and P. B. Mane, "Area Efficient High Speed FPGA Based Invisible Watermarking for Image Authentication", Indian Journal of Science and Technology, Vol. 9(39), DOI: 10.17485/ ijst/ 2016/ v9i39/ 101888, October 2016.
4. Adesh Kumar, Prakshi Rastogi, Pragyan Srivastava, "Design and FPGA Implementation of DWT, Image Text Extraction Technique", 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), March 2015.
5. Kulkarni Priyanka R., and Altaf O. Mulani. "Robust Invisible Digital Image Watermarking using Discrete Wavelet Transform." International Journal of Engineering Research and Technology (IJERT), Vol. 4. No. 01, Jan. 2015.
6. Khose P.N. and Raut V.G., "Implementation of AES algorithm on FPGA for low area consumption", International Conference on Pervasive Computing (ICPC), Jan. 2015.
7. Della Baby, Jitha Thomas, Gisny Augustine, Elsa George, Neenu Rosia Michael, "A Novel DWT based Image Securing Method using Steganography", International Conference on Information and Communication Technologies (ICICT 2014), Dec. 2014
8. Altaf O. Mulani and Dr.P. B. Mane, "Area optimization of cryptographic algorithm on less dense reconfigurable platform", IEEE International Conference on Smart Structures and Systems (ICSSS), Oct. 2014
9. 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.
10. Borkar A.M., Kshirsagar R.V. and Vyawahare M.V., "FPGA implementation of AES algorithm", IEEE International Conference on Electronics Computer Technology (ICECT), April 2011.
11. Karthigaikumar P. and Baskaran K., "An ASIC implementation of a low power robust in-visible watermarking processor", International Journal of System Architecture, 2010.
12. Kaur S. and Mehra Rajesh, "High Speed And Area Efficient 2D DWT Processor Based Image Compression", International Journal of Signal and Image Processing (SIPIJ), Dec. 2010.
13. 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.
14. Husaini Afrin Zahra and Nizamuddin M., "Challenges and approach for a robust image water marking algorithm", International Journal of Electronics Engineering. 2010.
15. 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.
16. Dorairangaswamy M.A., "A Novel invisible and blind watermarking scheme for copyright protection of digital images", International Journal of Computer Science and Network Security, April 2009.
17. 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.
18. Al-Haj Ali, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, 2007.
19. Kaur Swinder and Vig R., "Efficient Implementation of AES Algorithm in FPGA Device, IEEE International Conference on Computational Intelligence and Multimedia Applications, Dec. 2007.
20. S. P. Mohanty, N. Ranganathan and R. K. Namballa, "A VLSI architecture for visible watermarking in a secure still digital camera (S/sup 2/DC) design (Corrected)*," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 8, pp. 1002-1012, Aug. 2005.
21. Chao-Tsung Huang, Po-Chih Tseng and Liang-Gee Chen, "Analysis and VLSI architecture for 1-D and 2-D discrete wavelet transform," in *IEEE Transactions on Signal Processing*, vol. 53, no. 4, pp. 1575-1586, April 2005.
22. Alomari Raja S. and Al Jaber Ahmed, "A Fragile Watermarking Algorithm for content authentication", International Journal of Computing and Information Science, 2004.
23. Mohanty S.P., R. Kumara C. and Nayak S., "FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder", Lecture Notes in Computer Science (LNCS), CIT Springer-Verlag, Dec. 2004.
24. Xinmiao Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 957-967, Sept. 2004.