Indian Journal of Science and Technology, Vol 9(33), DOI: 10.17485/ijst/2016/v9i33/88449, September 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Analysis of Current FPGA-Based Image Watermarking Attempts

Taha Basheer Taha*, Ehkan Phaklen and Ngadiran Ruzelita

School of Computer and Communication Engineering, University Malaysia Perlis, 02060 Arau, Perlis, Malaysia;
eng.taha987@yahoo.com, phaklen@unimap.edu.my, ruzelita@unimap.edu.my

Abstract

Objective: Analysing of current FPGA-based image watermarking attempts to figure out the future requirements for such systems. **Analysis:** Hardware-based watermarking systems have been studied according to their performance in time, frequency and robustness measurements. A comparison has been made among current systems in terms of robustness, image quality achieved and system performance. **Findings:** Image watermarking was a very demand area of research in last decades, but hardware based attempts of image watermarking are still few in compare with software implementations although many modern systems nowadays rely on hardware-based real time algorithms. For their flexibility and reprogrammable nature, Field Programmable Gate Arrays (FPGAs) where adopted by many researchers for implementing watermarking hardware algorithms in cases where the need of high speed computations is a critical requirement. We find that many current watermarking schemes need to combine the required watermarking features as image quality measurements, using real size images, adaptable designs, and using FPGA features in using parallel high performance systems.

Keywords: FPGA, Image Processing, Spatial domain, Transform domain, Watermarking

1. Introduction

Copyright protection for digital media is one of the most important challenges in these days. Since a rate of 70 percent of transmitted data represented by digital images are critical parts of network exchange[1], finding a way to protect the copyrights of these images was a very demanding challenge for researchers and developers in last decades.

Watermarking is the process of embedding a piece of data like proprietary information inside digital media for copyright protection[2], alteration discovery or even to check the Quality of Service (QoS) of transmitting channels[3]. The word "watermark" is referred to the data that represent proprietary information, it may be called as robust watermark if it resists and still stable while exposing to different modifications. The term fragile watermark is used when the watermark is very sensitive to any modifications, or semi fragile watermark which is a level between fragile and robust[4]. Watermark can be visible as TV logos or invisible which is hidden within multimedia original data.

Watermarking process can be performed using software applications which are easier to implement but they are done using offline systems, or it can be performed using hardware devices in real time manner for hardware-based design, application specific integrated circuit (ASIC) or field programmable gate arrays (FPGAs) can be used. The choice among them is decided after comparison in power, cost and performance[5]. In last decades FPGA devices were the choice for many developers for their ability to design almost any type of digital systems, reconfigurable nature, and their high performance since the latest FPGAs could pass the 500 MHz operating frequency[6]. Hence, in this survey, FPGA-Based image watermarking attempts are presented, and analysed last published watermarking approaches. Finally a set of future needs for such designs are listed.

This paper is organized as following: section 2 explains general watermarking process, section 3 is watermarking requirements, Section 4 is watermarking applications while section 5 is the review for current watermarking

*Author for correspondence

techniques. Section 6 is analysing current works and list future requirements. Last but not least, section 7 is a conclusion of survey.

2. General Image Marking Process

Image watermarking is the process of inserting watermark pixels to original (host) image in a way that is still hidden (for invisible watermarking schemes) while in the same time, it has a security by which only authorized people can extract it. The process of adding watermark pixels to the host image is called embedding scheme (Figure 1), and on the other hand the process of extracting hidden watermark pixels from the watermarked image is called extracting process (Figure 2)[7].

Inputs for the watermarking embedding scheme are original image, watermark and optionally the secret key, which is used to enforce security in watermarking system. A watermark may be an image, text or sequence number. Embedding scheme produces watermarked image as an output. The decoding or extracting scheme inputs are

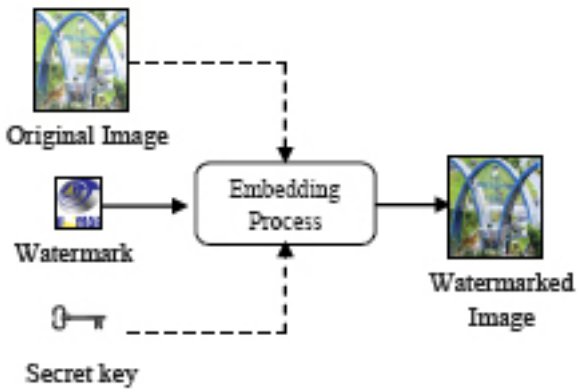

Figure 1. Watermark embedding scheme.

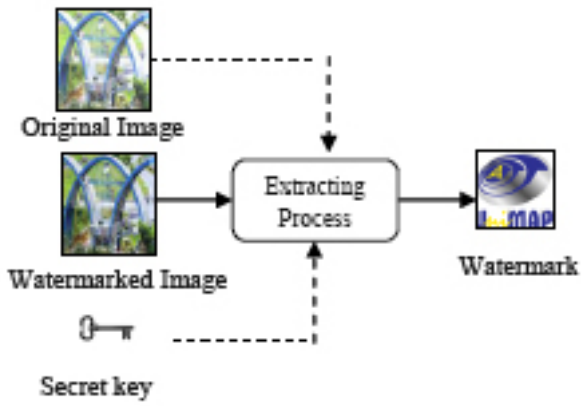

Figure 2. Watermark extracting scheme.

watermarked image and/or secret key and/or original image[7]. The watermarking algorithm which uses the original image to extract the watermark is called non blind, while blind watermarking relies on watermarked image only[8].

3. Watermark Requirements

Before designing or developing a watermark system, the requirements of a system must be studied as the importance of each requirement shapes the system design and its methodology. The five common watermarking requirements are as follow[9]

i. Robustness

Robustness is the ability to detect the watermark after unintended or intended distortion on watermarked data. However, this requirement is desirable in robust watermarking systems only. Since in fragile watermarking systems with authentication duty, any data modification is detected by the watermark damage. Hence, no need for robustness in such systems.

ii. Invisibility

Invisibility is to hide the watermark in a way that it cannot be observed by Human Visual System (HVS). This requirement is essential for invisible watermarking systems where the watermark is not preferred to be visible on host data. A similar word for invisibility is fidelity, which is the perceptual similarity between the host and watermarked data.

iii. Data Payload

Data payload is the number of embedded watermark bitswithin the original data. That number should uniquely definesthe copyright of the image. Possible attacks and distortions must be taken into consideration while choosing the data payload.

iv. Simplicity

Watermarking system must be as simple as possible, especially while working on real time systems, where the hardware resources are limited and the required processing time is short.

v. Real-time

Although this requirement is not mentioned frequently, but it is crucial feature in applications where no delay is permitted between capturing data and watermark embedding. Example of these are real time broadcasting and camera system in courtroom evidence[10]. Hardware

implementation is needed to apply this feature, and that is one of the major reasons to design and implement hardware based watermarking algorithms.

4. Watermark Applications

Watermark systems have wide distribution nowadays, five of major watermarking applications are listed as follow

i. Content Identification and Copyright Protection

Digital watermarking enables content of identifications asmetadata embedded in a way that it persists with media content. The watermark can carry information such as, who owns the data, date of creation, how it used, or any other details which owner aim to embed. Copyrights can be proved by extracting the watermark in type of text, image or unique sequence[4].

ii. Broadcast Monitoring

In broadcasting, watermark bits are embedded within shared media in a way that any attempt to remove or alter the watermark will ruin the entire material where that watermark is embedded[11]. Another usage of watermarking in broadcast monitoring is media tracking, where television, radio or online channels are monitored and when the owner's watermark is captured from unknown resources, details for these resources are captured and instantly reported.

iii. Tamper Detection

Watermark is used to ensure the integrity of the data by embedding a fragile watermark in a way that it will instantlybe destroyed if the original data is exposed to any tempering attempt. In semi fragile watermarking schemes, a watermark is still robust for some permitted modifications, but it will be destroyed for malicious attacks. For example, image compression can be done without affecting the watermark, but pixel alteration will ruin it[12].

iv. Intellectual Property (IP) Protection

Digital system designs are the result of knowledge and developers' efforts, hence design methodologies that allow the reuse of IP needs watermarking techniques to protect owners and programmers rights[13].

v- Quality of Service (QoS)

One of the non-conventional watermarking application is the QoS measurements for digital media, by evaluating the transmitting channel condition from the status of the received fragile watermark[3].

5. FPGA-Based Image Watermarking Survey

Current watermarking techniques could be classified into two main classes according to the domain where the watermark is embedded[14]. These include time spatial domain and frequency transform domain. In time spatial domain technique, watermark bits are embedded and extracted directly to/from the image pixels. In general, it is easy and fast for their few required resources. On the other hand, frequency domain deals with transformed components of the image while inserting watermark pixels, it requires more resources and more complicated operations than time partial domain technique. As a result, the watermark survives against many image processing manipulations[14,15].

Next subsections are spatial domain, transform domain, and dual mode (which is a mix between time and frequency) FPGA-based watermarking attempts.

i. Spatial Domain Attempts

Spatial time domain systems are easier to implement and achieve real time requirement, but more design efforts are needed to obtain security and robustness. Two of earliest spatial digital image watermarking architectures attempts using FPGAs were the schemes presented by[16] and[5]. [16]Added the watermark which is generated using Linear Feedback Shift Registers (LFSR) to the host image, the overall encoder period was 19.842 ns with 838 cells. Second attempt[5] was in 2007 proposed a new system which serve both robust and fragile watermark algorithms by adding the watermark to the third slice plane while they utilized FPGA and custom IC separately for this work. Both attempts have the same results for a time and number of slices**,** however the quality measurements such as PSNR is from a range of (21-56) dB by using Matlab where attacks are measured but no numeric values for geometric ones.

Two other attempts are followed by[17,18]. In[17], proposed a spatial semi-fragile watermarking scheme by taking advantage of spread spectrum and channel coding usage. A spread spectrum is used to distribute watermark bits on 8*8 image blocks and channel coding was utilized to increase robustness. The design required 11536 slices from Xilinx Virtex xc4vlx25-10ff676 FPGA to work within 219.542 MHz of frequency. Although encoding loss caused some distortion on the decoded watermark, algorithm is resistant to many attacks such as filtering,

noise, image sharpening, and compression. The next attempt by[18] was done using a spread spectrum utilizing a binary watermark. The conversion from integer to binary is done by Matlab. The size of the watermark was (64*64) while the cover image was in (256*256). The required number of slices was 959 with a frequency of 82.26MHz. Detailed measurements of PSNR, MSSIM, normalized correlation, and mean absolute error are given for the extracted watermark but not for the original image. The using of real size host image and watermark is a good step in watermarking, since visible and invisible watermarking techniques are required to clearly express authentication of owners. For instance, if you meant to add a TV logo, you would think of an image as watermark more than a random number.

Image to image communication algorithm is specified by[6] in which the aim was to achieve distortion free communication while the original data still unaltered. However, this attempt differs from the formers in that there is less care on carrier image quality (host image quality) which is utilized as a high frequency carrier signal in digital communication, hence no quality measurements values were given.

A novel six level pipelined watermarking architecture proposed by[2] in spatial domain were using Reversible Contrast Mapping (RCM). In this attempt, the least significant bit (LSB) is used for embedding the data after applying simple integer transform on two adjacent pixels. Here, watermark pixels can be reconstructed even if the LSB is lost, by one exception when the two pairs are in odd values. Two architectures are used here one for (8*8) block size image and other for (32*32) with watermark of (8*4) or (32*16) pixels. PSNR values were 29.46 dB and 30.41 dB for Lena and Boat images, respectively. A total of 9881 slices were needed for (32*32) bit architecture with operating frequency up to 98.6 MHz, no attacks measurements are shown in this work.

As a general notice of time domain watermarking attempts, simplicity and low overhead design can be noticed as well as real time achievement. However, we may see in many attempts the watermark implemented by a set of random sequences, not real images, although the watermark can be extracted here, there must be enough bits to uniquely define ownership[19]. Moreover, attacks in many cases are either not measured, or limited to traditional ones. As a result, many researchers meant to use frequency or dual domain for their watermarking systems.

ii. Transform Domain Attempts

In general, transform or frequency based watermarking schemes are resisting to some attacks and immune too many alterations[20], but the disadvantage of such systems is the complexity and high resource consuming. Developers usually try to find the possible ways to economize in their resources as floating number redemption or pipelining. One of the earliest FPGA-based frequency watermarking attempts was done by[21] when they presented a robust image watermarking scheme on image and video by using Altera Stratix II FPGA. They utilized Discrete Wavelet Transform (DWT) for their work with pipelined 2D-Scan based architecture running at maximum frequency of 100 MHz with PSNR equal to 31dB. However the extraction process was not explained and no attack had been presented to measure robustness[21].

[3]Proposed Spread Spectrum (SS) watermarking scheme with two major features, first is dual watermarking duties, one for integrity(robust watermark) and other for authentication purpose (fragile watermark). This had done by embedding more than one watermark in each image block. Second feature was employing the watermark for QoS measurements to check channels conditions. For frequency transformation, Walsh transform had been used while maximum frequency obtained was 80 MHz with number of 730 Configurable Logic Blocks (CLB) for XCS40 and XCS40L chips while a gray scale image of (8*8) was used to embed 4 bits watermark signal. PSNR for the watermarked image is 41.08. For authentication purpose, watermark has been tested and the alteration reflected on the watermark blocks. However, no attacks are listed for robustness evaluation. By using 4 bits as watermark that means there are only 16 possible watermarks may be created as identical case.

Xingfu Wang et.al[22] proposed Discrete Cosine Transform (DCT) scheme to embed the random series watermark into host image, with bit error rate (BER) of 5%, in this work but no quality measurement is listed for watermarked image. However, artifact which is one of the major issue in DCT transformations were noticeable on the watermarked image. The IDCT is done by transferring the watermarked data to another board connected via RS232[22].

[20]Developed reversible (Lossless) watermarking algorithm, they tried to achieve maximum embedding rate and robustness using integer wavelet transform. The PSNR was 31.37 for embedding capacity of 27% and up to 4 watermark bits have been embedded per coefficient.

The Xilinx Spartan 3 FPGA was used with frequency up to 62.073 MHz. Modelsim was used for simulation, but the input image was a text file previously converted by Matlab programming environment which means the system needs extra software support to be implemented. This, as a result, may negatively affects real time implementation requirement[20].

An adaptive watermark system has been proposed by Chen Feifei et.al[23] in 2012, the system is adaptive according to image format whether it is BMP or JPEG. In case of JPEG, the image is decoded into BMP before applying watermarking algorithm. Host data is a colored image of BMP or JPEG format with PSNR between (66.9152 - 77.7584) while the watermark is a binary image. No objective quality measurements are shown for extracted watermark but subjectively, watermark was not identical but could be recognizes even after cropping attack[23].

DWT based watermarking technique for colour and gray scale images had been used by[24] in 2012 and (256*256) of watermark image was used. This paper mentioned the reason beyond using the robust watermark to overcome issues like the high power consumption and large area requirements, however for most researcher's opinion that is not the core reason to use robust watermark, since it is used for copyright protection and confirm ownership[9]. No attacks are listed and the results show the watermark had been distorted after extraction. High frequency achieved by hitting frequency of 344MHz. Images is converted to bits using Simulink before it processed by FPGA. That's again, affects the real time requirement and it may be a reason that help to obtain a high frequency since not all steps are achieved using FPGA[24].

DWT also used by A.D. Darji et.al[25] when they presented a new pipelined, blind FPGA-based watermark approach using quantization method. A gray scale image is used as host image and a binary image is used as watermark. For the parallel architecture, a maximum frequency obtained is 29.017 MHz while in pipelined approach is 97.507 MHz. PSNR for the watermarked image was 44.408 dB while a range of (30-45) dB after attacks was given. They compared this range with[21] which is a video-image approach. It is important to mention that not all the steps for the algorithm were done by FPGA hardware, but DWT, IDWT and the extraction processes had been performed using Matlab[25].

S. Kiran et.al[26] used the mid frequencies of Haar DWT domain to embed watermark bits. No quality measurements values are listed. Components of the security keys were the original image size, wavelet transform filters and the channel in which watermark is embedded, however, these factors could be easily determined. No results for FPGA was shown[26]. DCT based approach has developed by Khoshki et.al. where auto code generation is utilized with the help of Matlab and Altera DSP builder. The code downloaded to DE2-115 Cyclone IV FPGA[27]. Nallathambi, B. and Karthigaikumar, P. (2014) fuse Iris images and fingerprint to create the secret key, they utilized and compared DWT, DCT and LSB which is spatial approach[28]. The comparison is done according to different attacks. However, Attacks' factors are not mentioned, for example, different noise ratio gives different PSNR and also the ratio of JPEG compression yields different results while differentiating between one algorithm and another[3].

Koushik and Mahanta et.al[4] (2014) proposed Message State Indicator (MSI) number based image watermarking architecture which relied on Walsh transform. The watermark can be extracted by MSI number which is generated in embedding process. Walsh transform has been applied for both host and watermark images. Results shows the watermark is successfully extracted but no numeric quality measurements are listed. In this work, watermark cannot be recovered in case of MSI damage[4].

As general scope of Transform-based image watermarking on FPGA devices, high image quality values could be achieved, hence more robustness. More bits are used to construct watermark data which it is mostly an image represents owner's logo. However, designs are more complicated and in many cases not all the watermarking processes is done by hardware while researchers in some cases rely on software to apply image conversion or even frequency transformation. Some researcher attempted to mix the advantages of time and frequency domains so they used dual mode watermarking architectures.

iii. Dual Domain Watermarking Schemes

Amit M Joshi et.al[10] (2011) used both bit slicing scheme (Spatial) and DWT (Frequency) to develop their watermarking algorithm. The approach applied lifting wavelet transform (to reduce the computations of wavelet convolutions) on (64*64) host image and applied bit space slicing on the low frequency band (LL) in DWT. A binary watermark which is the output of LFSR is embedded on LSB plane. It required number of slices 1078 and max frequency obtained on XC4VLX25-10FF676 FPGA Virtex

was 146.651 MHz. PSNR values obtained were 61, 60, and 59 for different images. As robustness measurement, some non-geometric (traditional) attacks are presented[10].

This work is compared with[17], but this comparison has some limitations since the later uses real images as watermark rather than LFSR sequence. These images need extra operations as they used as conversion to one dimension vector or any other processing steps. The second mixed attempt established by Sudip Ghosh et.al[17] in 2009 by fusing the fast Walsh Hamdard transform to their attempt in spatial[18] to propose a dual mode watermarking algorithm with Spread Spectrum concept. The xc4vlx200-11ff1513 from Virtex 4 FPGA series had been used. Maximum frequency obtained is 90.131 MHz and number of utilized slices were 570 and 831 for spatial and transform domain, respectively. Table 1 summaries current literature attempts for FPGA image watermarking[14].

6. Analysis

From the variety of measurements found in literature, two common and most mentioned factors are listed in Figures 3 and 4, PSNR and Frequency results respectively.

Table 1. Current FPGA-Based image watermarking attempts.

Number	Paper [ref.]	Domain	Year
1	16	TIME	2004
2	5	TIME	2007
3	17	TIME	2009
4	18	TIME	2012
5	6	TIME	2013
6	2	TIME	2014
7	21	FREQ	2009
8	3	FREQ	2009
9	20	FREQ	2010
10	23	FREQ	2012
11	24	FREQ	2012
12	25	FREQ	2013
13	26	FREQ	2014
14	27	FREQ	2014
15	28	FREQ	2014
16	4	FREQ	2014
17	10	Dual Mode	2011
18	14	Dual Mode	2012

Figure 3. Peak Signal to Noise ratio for different watermarking attempts.

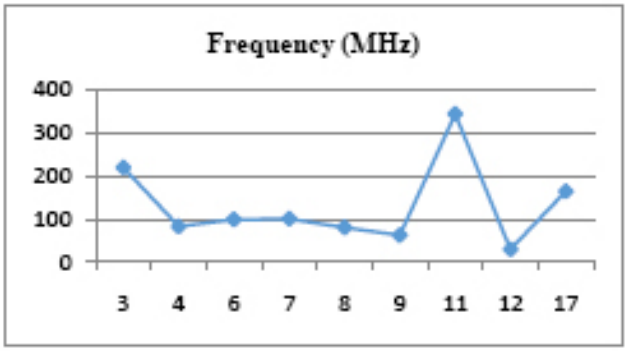

Figure 4. Maximum frequency obtained for different watermarking attempts.

An important notice must be taken while examine those values is that, attempts are differs from one approach to another, that is, for example[7] has high PSNR but the watermark had some distortion even before applying attacks, [24]had high PSNR but only 4 bits are embedded as watermark, and in paper[7] Images are converted to bits using software before FPGA processing and that reduces the system complexity and increase performance. For that reason, the listed data may be taken as reference to observe currently achieved values for frequency and PSNR, not for comparison establishment. The same aspect is applied on number of slices, for example, in[6], DWT and IDWT (which are the most resource consuming operations), are not included in FPGA design process.

Furthermore, different measurements of resources are given for different FPGA devices or families, for examples, in Spartan devices term of Control Logic Blocks (CLB) is used, each CLB contains two slices, each slice contains four 6-input LUTs and eight storage elements in 7 series of Spartan 3[29], while in Altera FPGA, Logic Elements (LE)

is mentioned instead of CLBs, LE in Cyclone III device family has a four-input LUTs, programmable registers and set of connectors[30].

Another aspect is the disparity of hardware while using different types of images, coloured, grayscale, or binary images, for example, five multipliers and six adders are needed to convert RGB image to YCbCr image[31]. YCbCr conversion is a middle step for applying image conversion operations such as time domain to DCT frequency domain, these resources are not required while using grayscale or binary images.

While comparing with software watermarking attempts, there are huge difference in number of works achieved in hardware and software. Maybe the number is not the only factor, many FPGA-attempts lack that comprehensive research aspects and results which clarify readers' doubts. Some of the features which are absent in many FPGA-based watermarking schemes are listed as follow

- Robustness against Basic Geometric Attack (Scaling, Rotation Cropping).
- Adaptable Algorithm.
- 2D-Images are utilized as watermark data.
- Dual purpose scheme (Robust and Fragile)
- Quality measurements (PSNR, MSE or any others)
- Pipelined design (For maximum system utilization).

Table 2 lists the existence of these features in literature attempts.

Table 2. The Existence of basic FPGA-watermarking features in literature

Ref. No.	Domain	Geometric Attacks	Adaptability	Watermark as Image	Dual Purpose	Quality Values	Pipelined System
16	TIME	-	-	-	-	-	-
5	TIME	-	-	-	-	✓	-
17	TIME	-	-	✓	-	-	-
14	TIME	-	-	✓	-	✓	-
6	TIME	-	-	✓	-	For Attacked images only	-
2	TIME	-	-	✓	-	✓	✓
21	FREQ	-	-	✓	-	✓	✓
3	FREQ	-	-	-	-	✓	-
22	FREQ	-	-	-	-	-	✓
20	FREQ	-	-	-	-	✓	-
23	FREQ	Cropping Only	JPEG-BMP Adaptable	✓	-	✓	-
24	FREQ	-	-	✓	-	-	-
25	FREQ	Attacks as general are mentioned	-	✓	-	✓	✓
26	FREQ	-	-	✓	-	-	-
27	FREQ	-	-	✓	-	-	-
28	FREQ	YES (without Specifying attacks' value)	-	Biometric Data	-	✓	-
4	FREQ	Mentioned it is robust against attacks without numbers	-	✓	-	-	-
10	Dual Mode	-	-	-	-	✓	Within Lifting based DWT
14	Dual Mode	-	-	✓	✓	-	-

7. Conclusion

Hardware-based watermarking becomes a need with the increase of real time image processing applications. Watermarking as authentication, integration and property protection tool need more researches and developments, since the limitations of resources and complexity of some hardware design tools bounded many researchers from presenting detailed papers which cover mostly all needed measurements. This paper presents a glance of the literature attempts and analysed those works to figure out future needs of FPGA-based image watermarking systems. Works are classified according to domain of embedding and extracting watermark bits, from simple low overhead time domain to more complicated frequency domain embedding ending with dual domain schemes. Our current work aims to create a comprehensive FPGA-based image watermarking system to shrink the gap between hardware and software image watermarking attempts.

8. References

1. Janani VSE, Ganeshkumar P. Compliant Data-centric Network Processing for Energy Economic Data Collection in Wireless Sensor Networks. Indian Journal of Science and Technology. 2015; 8(S9):506–12.
2. Maity HK, Maity SP. FPGA implementation of reversible watermarking in digital images using reversible contrast mapping. Journal of Systems and Software. 2014; 96:93–104.
3. Maity SP, Kundu MK, Maity S. Dual purpose FWT domain spread spectrum image watermarking in real time. Computers & Electrical Engineering. 2009; 35(2):415–33.
4. Mahanta K, Das DJ, Bhuyan HM, Dutta A, Gogoi M. Design and implementation of an MSI number based image watermarking architecture in transform domain. Noida: 2014 International Conference on Signal Processing and Integrated Networks (SPIN). 2014; p. 157–63.
5. Mohanty SP, Kougianos E, Ranganathan N. VLSI architecture and chip for combined invisible robust and fragile watermarking. IET Computers & Digital Techniques. 2007; 1(5):600–11.
6. Maity SP, Kundu MK. Distortion free image-in-image communication with implementation in FPGA. AEU-International Journal of Electronics and Communications. 2013; 67(5):438–47.
7. Hartung F, Kutter M. Multimedia watermarking techniques. Proceedings of the IEEE. 1999; 87(7):1079–107.
8. Gunjal BL, Manthalkar RR. An overview of transform domain robust digital image watermarking algorithms. Journal of Emerging Trends in Computing and Information Sciences. 2010; 2(1):37–42.
9. Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Morgan Kaufmann: USA: Digital watermarking and steganography. 2008.
10. Joshi AM, Darji A, Mishra V. Design and implementation of real-time image watermarking. Xi'an: 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). 2011; p. 1–5.
11. Digital Water Marking Applications. Date accessed: 11/1/2016: Available from: www.digitalwatermarkingalliance.org/applications.asp.
12. Huo Y, He H, Chen F. A semi-fragile image watermarking algorithm with two-stage detection. Multimedia tools and applications. 2014; 72(1):123–49.
13. Kahng AB, Lach J, Mangione-Smith WH, Mantik S, Markov IL, Potkonjak M, Wolfe G. Watermarking techniques for intellectual property protection. DAC'98, Proceedings of the 35th annual Design Automation Conference. 1998; p. 776–81.
14. Ghosh S, Talapatra S, Sharma J, Chatterjee N, Rahaman H, Maity SP. Dual Mode VLSI Architecture for Spread Spectrum Image Watermarking using Binary Watermark. Procedia Technology. 2012; 6:784–91.
15. Mundhada SO, Shandilya VK. Spatial and Transformation Domain Techniques for Image Enhancement. International Journal of Engineering Science and Innovative Technology (IJESIT). 2012; 1(2):213–16.
16. Mohanty SP, Kumara RC, Nayak S. Heidelberg: Springer-Berlin: FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. Intelligent Information Technology. 2004; p. 344–53.
17. Ghosh S, Ray P, Maity SP, Rahaman H. Spread spectrum image watermarking with digital design. Patiala: IACC 2009, IEEE International Advance Computing Conference. 2009; p. 868–73.
18. Ghosh S, Talapatra S, Chatterjee N, Maity SP, Rahaman H. FPGA based Implementation of Embedding and Decoding Architecture for Binary Watermark by Spread Spectrum Scheme in Spatial Domain. Bonfring International Journal of Advances in Image Processing. 2012; 2(4):1–8.
19. Abdel-Hamid AT, Tahar S, Aboulhamid EM. A survey on IP watermarking techniques. Design Automation for Embedded Systems. 2004; 9(3):211–27.
20. Venkateswarlu SC, Reddy PB, Raju YD. Watermarking for JPEG2000 compression standard on FPGA. Proceedings of the International Conference and Workshop on Emerging Trends in Technology. 2010; p. 309–14.
21. Karmani S, Djemal R, Tourki R. Efficient hardware architecture of 2D-scan-based wavelet watermarking for image and video. Computer Standards & Interfaces. 2009; 31(4):801–11.

22. Wang X, Qin Q, Cheng Y. Design and Implementation of Digital Image Watermark Based on FPGA. Heidelberg: Springer Berlin: Recent Advances in Computer Science and Information Engineering. 2012; p. 223–29.
23. Feifei C, Yuhui L, Bo L, Yu L. FPGA-based adaptive image watermark embedding method and implementation. Shenzhen: IET International Conference on Information Science and Control Engineering, ICISCE 2012. 2012; p. 1–4.
24. Karthigaikumar P, Baskaran K. FPGA Implementation of High Speed Low Area DWT Based Invisible Image Watermarking Algorithm. Procedia Engineering. 2012; 30:266–73.
25. Darji AD, Lad TC, Merchant SN, Chandorkar AN. Watermarking Hardware Based on Wavelet Coefficients Quantization Method. Circuits, Systems, and Signal Processing. 2013; 32(6):2559–79.
26. Kiran S, Nadhini Sri KV, Jaya J. Design and implementation of FPGA based invisible image watermarking encoder using wavelet transformation. Coimbatore: 2013 International Conference on Current Trends in Engineering and Technology (ICCTET). 2013; p. 323–25.
27. Khoshki RM, Oweis S, Wang S, Pappas G, Ganesan S. FPGA Hardware Based Implementation of an Image Watermarking System. International Journal of Advanced Research in Computer and Communication Engineering. 2014; 3(5):6400–05.
28. Nallathambi B, Karthigaikumar P. FPGA implementation of hiding information using cryptographic key. Coimbatore: 2014 International Conference on Electronics and Communication Systems (ICECS). 2014; p. 1–5.
29. 7 Series FPGAs Configurable Logic Block. Date accessed 17/11/2014: Available from: http://www.xilinx.com/support/documentation/user_guides/ug474_7Series_CLB.pdf.
30. Logic Elements and Logic Array Blocks in the Cyclone III Device Family Cyclone III Device Handbook. 2011 Dec; 1:1–8.
31. Mohanty SP, Kougianos E. Real-time perceptual watermarking architectures for video broadcasting. Journal of Systems and Software. 2011; 84(5):724–38.