

FPGA Implementation Using Efficient DWT-Digital Image and Text Watermarking

A.Jeyamurugan M.E., A.Margaret Emily Christelda

Assistant Professor, Department of ECE, Holycross Engineering College, Vagaikulam, Thoothukudi, India

M.E., Embedded System Technologies, Holycross Engineering College, Vagaikulam, Thoothukudi, India

ABSTRACT: This paper proposes a new multiresolution domain watermarking of grayscale images and has also shown its VLSI Implementation without altering its content in real time using a secret key. The proposed algorithm does not make any change in the host image. Thus it shows high robustness to signal processing attacks. The watermark extraction process is simple as the host content is extracted based on key. We have evaluated the robustness of the algorithm against several signals processing using MATLAB. Finally we have implemented the same algorithm in verilog HDL using Altera Quartus-II.

KEYWORDS: Digital Watermarking, Discrete Wavelet Transform, embedding, extracting, VLSI

I. INTRODUCTION

In this modern digital era the reproduction digital content is so easy due to the presence of lot of software packages. Digital watermarking is one of the promising methods to communicate secret data in an image, video or audio, visibly or invisibly, which can be used to manifest the owner copyrights. The secret data (watermark) can be embedded in the host content in robust, fragile or in semi fragile manner. There exist three main spaces or domains of watermark insertion viz; spatial domain, frequency domain, and multiresolution domain. The frequency domain techniques like DFT, DCT will modify the frequency components of host contents with a transformation of original content, which yields high robustness (i.e. persistent to signal processing attacks) with a higher computational complexity and low embedding capacity. Whereas the spatial domain techniques like LSB embedding, Pixel Value Differencing (PVD) will involve only the direct manipulation of pixel intensities. So there exists a high embedding capacity with less computational complexity, but it is less robust to signal processing attacks.

In this paper a text watermark is taken as input in the domain of insertion as frequency because of its low computation complexity and fidelity. The different multiresolution domain techniques have inherent merits and demerits. The proposed technique called Discrete Wavelet Transform multiresolution domain watermarking with VLSI architecture wherein we have added a threshold value in incrementing and decrementing fashion to get an exact match of the watermark content. In case there is no match, it retains the previous neighborhood pixel value of host as a secret key. Also the proposed algorithm does not affect the host image content but only takes its pixel value location as key for embedding and extraction of secret watermark content and overcomes all the demerits of all LSB, PVD.

II. PROPOSED METHOD

Watermarking is the procedure to cover up some information which will be named watermark or tag in to the original data(image, audio or video) in a way that watermark may be removed or recognized later to produce an assertion in regards to the object. Image watermarking systems are used to protect the digital images. Watermarks of varying level of visibility are put into demonstration media as a guarantee of authenticity, quality, ownership and source. The image watermarking systems have been popular to solve the copyright protection problems of digital picture related to illegal use or distribution. Watermarking scheme quality is decided applying robustness, transparency and capacity. Transparency indicates after installation of watermark the initial picture should not be distorted. Robustness relates to attacks. If watermark treatment is hard to different attacks like Intensity Transformation, noise then watermarking scheme is robust.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Digital watermarks can be divided into visible and invisible types. Based on human perception a visible watermark is a secondary translucent image overlaid on to the primary image in visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark. The invisible watermarks are categorized into watermarking techniques as fragile and robust. Generally, a robust mark is generally used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations, which attempt to remove or destroy the mark. These algorithms ensure that the image processing operations do not erase the embedded watermark signal. On the other hand a fragile or semi-fragile watermark are mainly applied to content authentication and integrity verification because they are very sensitive to attacks, i.e., it can detect slight changes to the watermarked image with high probability.

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. Discrete wavelet transform, which transforms a discrete time signal to a discrete wavelet representation. It gained widespread acceptance in signal processing, image compression & watermarking. The transformation of a signal is that converts one to another form of the signal to representing it. It does not change the data present in the signal. Discrete wavelet transform is a multiresolution decomposition of a signal. It hierarchically decomposes an image. Mapping an image into a set of coefficients is done by discrete wavelet transform. Basically non stationary signals are processed by discrete wavelet transform. Both frequency and spatial domain of an image are provided by discrete wavelet transform i.e. it captures both frequency and location information. In this, decoding is done in low resolution to high resolution manner. High and low frequency parts are obtained on decomposing an image by dwt. Information about edge components are contained in high frequency parts and, low frequency parts again decomposed into another set of low and high frequency parts. The image is divided into four multiresolution sub-bands LL, LH, HL and HH using DWT. Fine-scale DWT coefficients are represented by LH, HL, HH sub-bands and coarse-scale DWT coefficients are represented by LL sub-bands. LL sub-band is further decomposed into four multiresolution sub-bands to obtain next coarser wavelet coefficients. This process is repeated several times determined by application for which it is used.

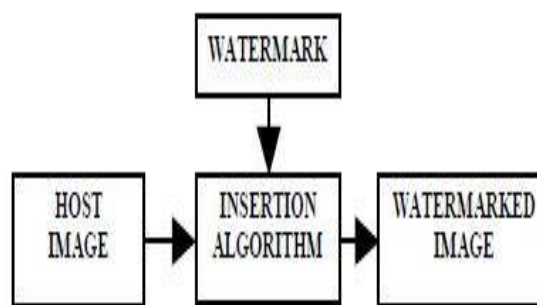


Fig.1. Watermark Insertion Procedure

In this paper we used 1-level DWT which decomposes an image into LL1 which is lower resolution approximation coefficient and LH1, HL1, HH1 which are detailed components of an image.

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden “mark” that is imprinted into the image.

In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from the content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment.

The major technical requirements for this application are as follows; The watermark does not incur visible (or audible) artifacts to the ordinary users. The watermark is independent of the data format. The information carried by the watermark is robust to content manipulations, compression, and so on. The watermark can be detected without the unwatermarked original content. The watermark can be identified by some kind of “keys” that are used to identify large number of individual contents uniquely. The contents may be changed to the other formats, edited or trimmed by the users or compressed for the storage and transmission, and it is desirable to be able to detect the watermark from those processed contents. Usually, the watermark signal embedded into the content does not disappear after the editing of the content, but becomes more and more difficult to detect while the content is distorted. In general, higher robustness can be achieved by increasing the strength of the watermark signal, thus improving the detection capability.

In other words, the robustness of the watermark is a trade-off between the amount of watermark signal that applies to the content and the overhead to the detection. Currently, several commercial products and services using watermarking technology are available. They include applications for watermark embedding/detection and services to search the Internet for the contents with certain designated watermarks. These applications are mainly taking place between the large content owners (e.g. Electronic publishers/distributors), and their customers (e.g. the content creators). Because the usage is limited within relatively smaller groups, each group tends to use their own proprietary watermark rather than a common one. Other applications of watermarking are Copyright Watermarks, Fingerprint Watermarks, Broadcast Watermarks, Annotation Watermarks, Integrity Watermarks.

It converts an input series into one high-pass wavelet coefficients series and one low-pass wavelet coefficient series. For many signals, the low-frequency content is the most important part. In wavelet analysis, the approximations (A) and details (D) are obtained after filtering. The approximations are the high-scale, low frequency components of the signal. The filtering process is schematically represented as in Figure.1. functional part of the cover data so that it results in watermarked image as shown in Figure.2. The original image and the watermark text undergoes the haar based DWT. The DWT image of the original image and the watermark image are embedded into one image.

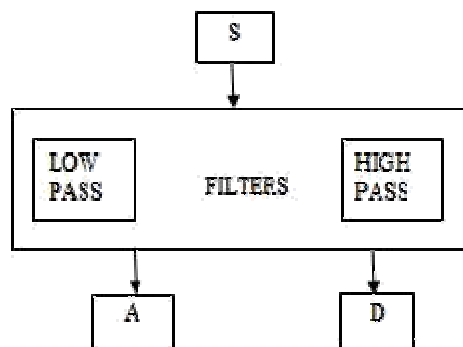


Fig.2. Single stage filtering

The original signal, S, passes through two complementary filters and emerges as two signals. Unfortunately, it may result in doubling of samples and hence to avoid this, down sampling is introduced. The one-dimensional forward wavelet transform is defined by a pair of filters s and that are convolved with the data at either the even $2r$ odd locations.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

The 1-D wavelet transform can be extended to a two-dimensional (2-D) wavelet transform using separable wavelet filters. With separable filters the 2-D transform can be computed by applying a 1-D transform to all the rows of the input and then repeating on all of the columns. The image undergoes the DWT transform and it is decomposed into 4 frequency districts. In that four districts one is low frequency district (LL) and other are the high frequency districts (HL, LH, HH). In this paper the low frequency district of the decomposition is used to store the main content. Since the low frequency district is prone to low noise if the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. This four LL, LH, HL HH district used to compress the image in wavelet transform as shown in Figure.2. This compression technique has been utilized to secure the digital data with the help of watermarking. If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. This paper implements the algorithm in two stage as shown in Figure.3.

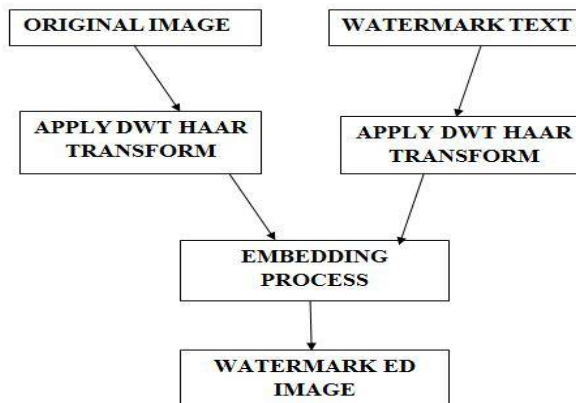


Fig.3. Image DWT decomposed

Stage 1: This watermark embedding stage consists of generating watermarked image from the host image and watermark image with the help of Haar based DWT Original image (cover) and watermark text are considered and watermark text is embedded into the

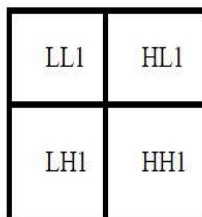


Fig.4. Encryption Unit

Stage 2: The watermark extraction stage consists of extracting watermark image from watermarked image with the usage of Haar based IDWT. The watermarked image undergoes the inverse discrete wavelet transform and both original image (cover) and the watermark image is separated by extracting process. Then the original image and watermark text is obtained as shown in the Figure.5

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

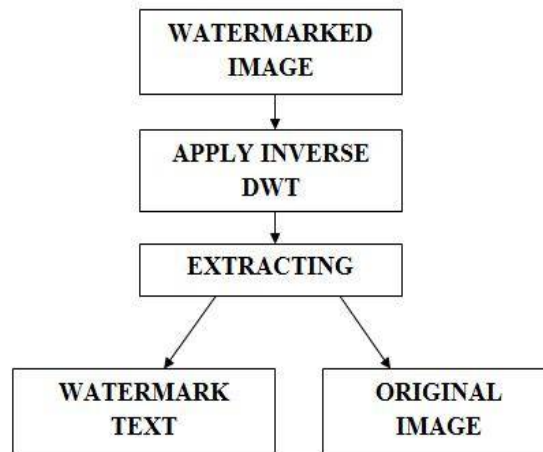


Fig.5. Watermarking Unit

III. CHIP LEVEL DESIGN OF WATERMARKING

For the chip level implementation, the datapath embedding and extraction units are modeled using verilog HDL. Then the Host image and watermark text is converted into binary form (hex-file or memory-initialization file) and stored in the RAM of corresponding sizes. The code modeled in verilog HDL is simulated and synthesized to get a real time chip. The entire VLSI flow is illustrated in Fig 6.

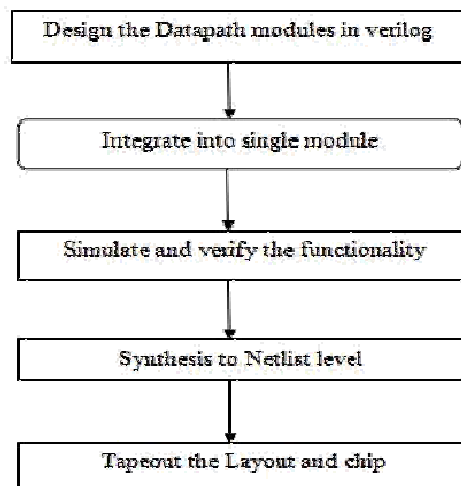


Fig.6. VLSI Flow

The datapath modules are modeled using Verilog HDL, integrated and then simulated using Modelsim-SE 6.5© and Finally synthesized using Altera Quartus-II 9.0© with a generation of netlist and layout.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IV. PERFORMANCE EVALUATION

This section gives the simulation results using MATLAB R2014b© and Altera Quartus-II 9.0©. In the MATLAB implementation process we have taken the host image of size 256 x 256 as Lena and the watermark is text. Then we have simulated DWT and generated a secret key for authentication. The host image and watermark text are shown in Fig-7 and 8.



Fig.7: Host Image

IFY

Fig.8: Watermark Text

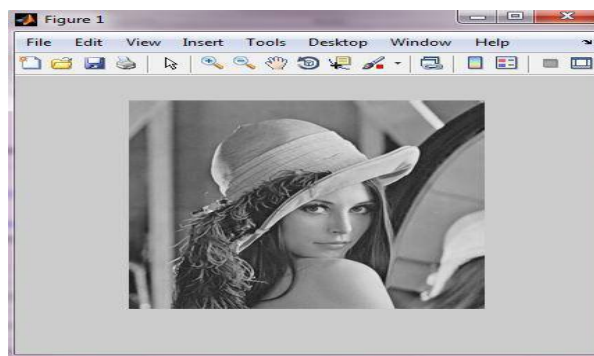


Fig.9. Watermarked Image

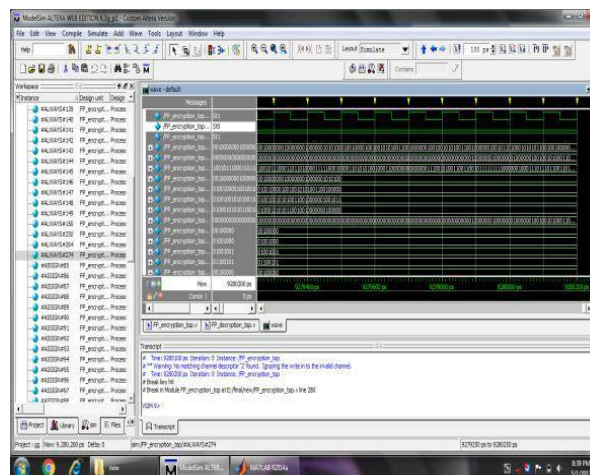


Fig.10. Embedding process in Modelsim

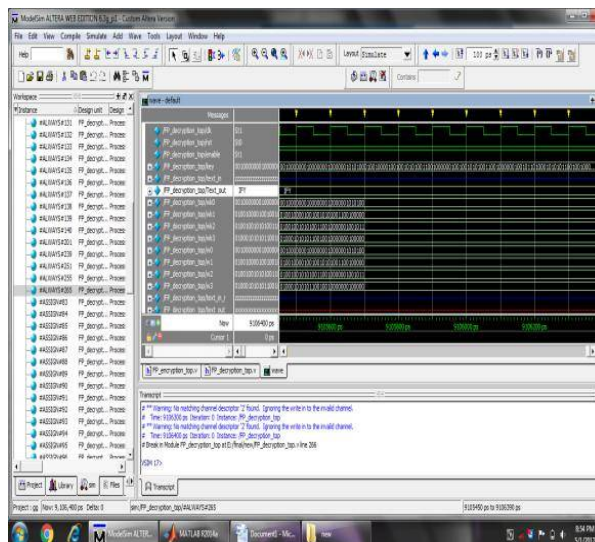


Fig.11. Extraction process in Modelsim

The same watermarking and extraction were modeled using Verilog HDL with initialization of image values in ram. Then executed the simulation and we verified that both the MATLAB simulation and Verilog simulation will have the same results. For the reconstruction of image file, we once again wrote all the secret key values from ram to text file during Verilog simulation. Then using MATLAB the text file is used as a key to generate the watermark image content. The Verilog simulation is done by Modelsim SE6.5b©. Then we have synthesized the entire watermarking embedding and extraction module using Altera Quartus-II 11.0 © with their layout generation. The Synthesis and layout generation of the chip generated are done using Altera FLEX10KA EP3C5F256C6 device family. From the synthesized report it is found that no critical path in the design.

The design constraints such as area, power and delay were satisfied. The reduction of area and delay is possible while generating the structural netlist. Both area and delay can be reduced simultaneously until they reach equilibrium or acceptable value range. The clock frequency is fixed in the design analyzer to optimize the design. Once the critical delay for the circuit is determined, the clock frequency is again adjusted.

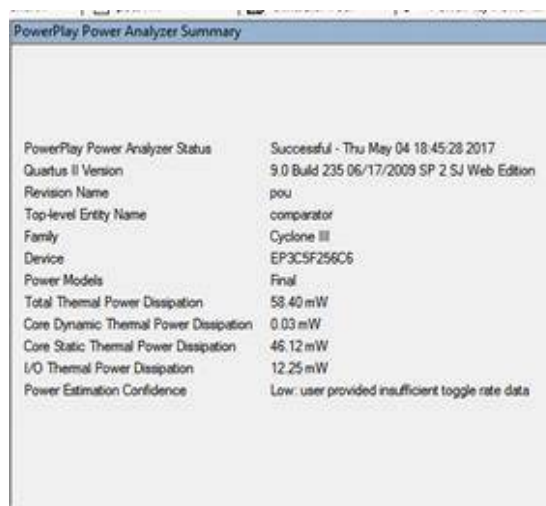


Fig.12: Summary of power analyser

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Flow Summary	
Flow Status	Successful - Thu May 04 18:41:47 2017
Quartus II Version	9.0 Build 235 06/17/2009 SP 2 SJ Web Edition
Revision Name	pou
Top-level Entity Name	comparator
Family	Cyclone III
Met timing requirements	N/A
Total logic elements	8 / 5,136 (< 1 %)
Total combinational functions	8 / 5,136 (< 1 %)
Dedicated logic registers	0 / 5,136 (0 %)
Total registers	0
Total pins	26 / 183 (14 %)
Total virtual pins	0
Total memory bits	0 / 423,936 (0 %)
Embedded Multiplier 9-bit elements	0 / 46 (0 %)
Total PLLs	0 / 2 (0 %)
Device	EP3C5F256C6
Timing Models	Final

Fig. 13: Device utilisation summary for EP3C5F256C6

V. CONCLUSION

In this paper we proposed a ASIC implementation of watermarking algorithm in real time without altering its content. Our algorithm does not make any change in the host image and the watermark is invisible. The watermark can be extracted only by the key hence it finds its application in security and copyright purposes. DWT provides an invisible, robust and real time high speed hardware implementation. The multiple watermarking finds its application where a digital content has more than one owner and each has to be authorized distinctly.

REFERENCES

- [1] Adamo SarajuO. B., MohantyP., KougianosE., VaranasiM.(2006)“VLSIArchitecturefor Encryption and Watermarking Units towards the Making of a Secure Camera” IEEE.
- [2] Anand Darji, Dr.ChandorkarA.N, Dr. MerchantS.N., Vipul Mistry*(2010)“VLSI Architecture of DWT based Watermark Encoder for Secure Still Digital Camera Design” Third International Conference on Emerging Trends in Engineering and Technology 978-0-7695-4246-1/10 ©IEEE Computer society.
- [3] Houtan Haddad Larijani, Gholamali Rezai Rad, “A New Spatial Domain Algorithm for Gray Scale Images Watermarking” Proceedings of the International Conference on Computer and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia978-1-4244-1692-9/08©2008 IEEE.
- [4] MohantyS. P., RanganathanN., and NamballaR. K., Jul. (2005) “A VLSI architecture for visible watermarking in a secure still digital camera (S2DC) design,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 13, no. 7, pp. 808–818
- [5] MohantyS.P., RanganathanN., Karthikeyan Balakrishnan, May 2006 “A dual voltage frequency VLSI chip for image processing in DCT Domain,”IEEE Trans. on Circuits and Systems, vol. 53, no. 5.
- [6] Na Li, Xiaoshi Zheng, Yanling Zhao, Huimin Wu, Shifeng Li “Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform” in International Symposium on Electronic Commerce and Security.
- [7] NaskarR.ChakrabortyR.S.,(2012) “Reversible Watermarking Utilising Weighted Median- Based Prediction” IET Image Process.
- [8] Sakthivel. S.M., Ravi Sankar.(2015), “VLSI Architecture of Grayscale images using Weighted Median Based Prediction”, IEEE sponsored 2ND international conference on electronics and communication systems (ICECS 2015).
- [9] Sudip Ghosh, Subhojit Chatterjee, Santi P. Maity and Hafizur Rahaman “A New Algorithm On Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security”.
- [10] Tianrui Zong, Yong Xiang, Song Guo, Yue Rong(2016) “Rank-Based Image Watermarking Method With High Embedding Capacity and Robustness” Received March 31, 2016, accepted April 12, 2016, date of publication April 25, 2016, date of current version May 9, 2016. Digital Object Identifier 10.1109/ACCESS.2016.2556723
- [11] F. Mintzer, G. Braudaway, and M. Yeung, “Effective and ineffective digital watermarks,” in *Proc. IEEE Int. Conf. Image Process.*, vol. 3, 1997, pp. 9–12.
- [12] N. J. Mathai, D. Kundur, and A. Sheikholeslami, “Hardware implementation perspectives of digital video watermarking algorithms,” *IEEE Trans.Signal Process.*, vol. 51, no. 4, pp. 925–938, Apr. 2003.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- [13] T. H. Tsai and C. Y. Lu, "A systems level design for embedded watermark technique using DSC systems," in *Proc. IEEE Int. Workshop Intell. Signal Process. Commun. Syst.*, 2001.
- [14] Garimella *et al.*, "VLSI implementation of online digital watermarking techniques with difference encoding for the 8-bit gray scale images," in *Proc. Int. Conf VLSI Des.*, 2003, pp. 283–288.
pp. L. D. Strycker *et al.*, "Implementation of a real-time digital watermarking process for broadcast monitoring on trimedia VLIW processor," *Proc. IEE Vision, Image Signal Process.*, vol. 147, no. 4, 371–376, Aug. 2000.
- [15] J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
- [16] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in *Proc. IEEE Int. Conf. Multimedia Expo.*, 2000, pp. 1029–1032.
- [17] S. P. Mohanty, "Digital watermarking of images," Master's thesis, Dept. Elect. Eng., Indian Institute of Science, Bangalore, India, 1999.
- [18] M. Kaul, R. Vemuri, S. Govindarajan, and I. Ouaiss, "An automated temporal partitioning and loop fission approach for FPGA based reconfigurable synthesis of DSP applications," in *Proc. IEEE/ACM Des. Autom. Conf.*, 1999, pp. 616–622.
- [19] S. Govindarajan, I. Ouaiss, M. Kaul, V. Srinivasan, and R. Vemuri, "An effective design systems for dynamically reconfigurable architectures," in *Proc. 6th Ann. IEEE Symp. Field-Programmable Custom Comput. Mach.*, 1998, pp. 312–313 [11] A. Agrawal, Z. Rezki, A. Khisti, and M. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 565–574, sept. 2011.