International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Image Authentication by Watermarking Technique using System Generator Architecture

Theodore Jesudas E Dandin
P.G Student, VLSI & Embedded Sys
UTL, VTU Extn Centre
Bangalore,India

Ramanareddy K. V
Assistant Professor
UTL, VTU Extn Centre
Bangalore,India

Dr. Siva Yellampalli
Prof & Head
UTL,VTU Etxn Centre
Bangalore,India

Abstract:- **This paper introduces a prototype for Digital Image Authentication System (DIAS). This system can perform visible and invisible watermarking on image. DIAS is applicable for gray images. The input image could be of any size, and the resultant image size would be same as input image. DIAS identifies the ownership of digital image using Digital Watermarking. The Digital watermarking concept is used to hide and detect information from image. It is the best way to copyright protection of the user. By the use of digital watermarking, user can blame on faker for ownership. This is known as an Authentication System for ownership identification [1]. The complete system consists of two functions, one for hiding information inside image, and the other for detecting information from image. In this approach, A system generator architecture for digital watermarking using Discrete Wavelet Transform (DWT) is designed.**

Index Terms – Watermarking, Discrete Wavelet Transform, System Generator Architecture

I. INTRODUCTION

These days, people are using social networking sites for sharing their life moments as images. And another side other users can access or even download those digital images. Faker can exploit by editing and modifying the original image [1]. Modified images can then be uploaded and shared. The illegal use of personal image comes under copyright law. Image authentication is one of the applications of digital watermarking which is used for authenticating the digital images [1]. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of image being tampered, it can easily be detected as the pixel values of the embedded watermark would change and do not match with original pixel values. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking techniques can be classified into two categories: spatial domain and transform domain techniques. In spatial domain technique, the watermark embedding is achieved by directly modifying the pixel values of the host image. The commonly used method in spatial domain technique is the LSB (least significant Bit). In transform domain, the host image is first converted into frequency domain by transforming method such as the discrete cosine transform (DCT), Discrete Fourier transform (DFT) or Discrete Wavelet Transform (DWT), etc. Then transform domain coefficients are modified by the watermark. The inverse transform is finally applied in order to obtain the watermarked image [10].

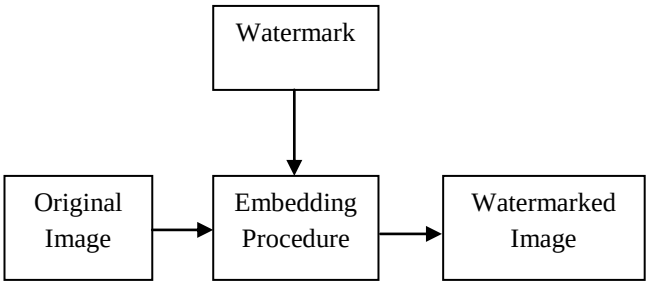


Fig 1: Watermark Embedding Process

II. GENERAL WATERMARKING MODEL

Digital Watermarking can be defined as the process of embedding a certain piece of information into multimedia content including text documents, images, audio or video streams, such that the watermark can be detected or extracted later to make an assertion about the data. A generalized watermarking model includes watermark embedding and watermark extraction process as shown in the Fig 1 and Fig 2. In the watermark embedding process, the embedding procedure i.e the algorithm accepts both the watermark image and the original image in which the watermark has to be inserted.

In the watermark extraction process the extraction procedure i.e algorithm extracts the embedded watermark.

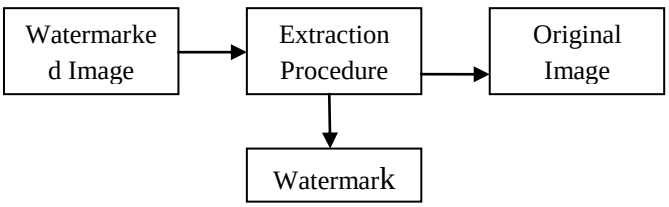


Fig 2: Watermark Extraction Process

A) Applications of Digital Watermarking

Digital watermarking can be used for the following purposes [15]:

- *Copyright protection:* This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.
- *Authentication:* Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.
- *Broadcast Monitoring:* As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.
- *Content Labeling:* Watermarks can be used to give more information about the cover object. This process is named as content labeling.
- *Tamper Detection:* Fragile watermarks can be used to detect tampering in an image. If fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.
- *Digital Fingerprinting:* This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.
- *Content protection:* In this process, the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

III. DISCRETE WAVELET TRANSFORM

Fourier Transformations are effectively utilized for representing and analyzing the stationary signals where frequency components do not change over period of time. However, sometimes it is required to determine the existence of frequency components along with their position in case of non-stationary signals. Images are usually non-stationary two-dimensional signals and wavelet transform is effective in such case [12]. The Discrete Wavelet Transform (DWT) generates a matrix which is used for image processing since it captures both frequency and location information. Discrete wavelet transformation (DWT) when applied on image, it decompose image into four frequency sub-bands (LL, HL, LH, HH) where LL refers to low pass band and other three sub-bands corresponds to horizontal (HL), vertical (LH) and diagonal (HH) high pass bands[13]. Figure 3 shows two-level DWT decomposition of image. In general, the watermark can be inserted into low frequency sub-bands (LL) because it increases the robustness of watermark but at the same time it may degrade the image significantly. High frequency bands (HH) contains edges and textures and changes that are caused due to watermark data inserted in such band cannot be noticed by human eye [14].

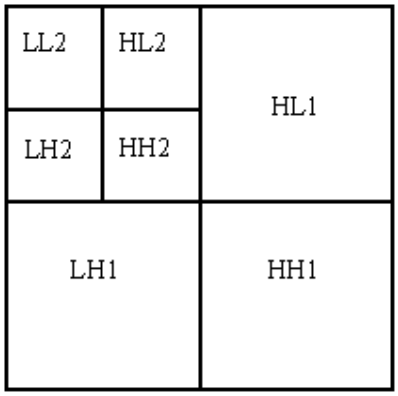


Fig 3: Two level DWT decomposition of an image

IV. SYSTEM GENERATOR

System Generator allows device-specific hardware designs to be constructed directly in a flexible high-level system modeling environment. It's a new version hardware tool that supports high end FPGA advanced architecture used for image and video processing. System Generator allows designs to be composed from a variety of ingredients. Data flow models, traditional hardware design languages (VHDL and Verilog), and functions derived from the MATLAB programming language, can be used side-by-side, simulated together, and synthesized into working hardware. System Generator simulation results are bit and cycle-accurate. This means results seen in simulation exactly match the results that are seen in hardware. System Generator simulations are considerably faster than those from traditional HDL simulators, and results are easier to analyze

V. PROPOSED WORK

A) Watermark Embedding

The block diagram of the system for watermark embedding is as shown below.

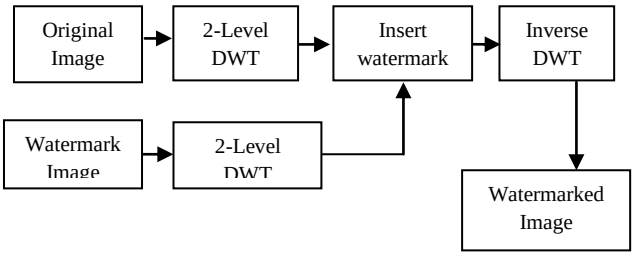


Fig 4: Watermark Embedding Block

Inputs to the watermark embedding block are Original Image and watermark image of size 256 ×256. A 2-level Haar Discrete wavelet transform is applied on both the images to obtain the sub-bands LL2. The equation which is used for inserting the watermark into the original image is given below.

$$WMI = k*(LL1) + q * (WM1) \ldots\ldots\ldots\ldots (1)$$

Where *WMI* = Watermarked Image
LL1 = low frequency approximation of the original image
WM1 = Watermark Image
k, *q* = scaling factors for the original image and watermark respectively.
The value of q is fixed at 1 whereas k can be varied to get the best result. Varying q will result in variation of the contrast of the image.
Once the watermark is inserted into the selected sub-band region, the decomposed image is now reconstructed back using the Inverse DWT operation.

B) Watermark Retrieval

The input to the watermark retrieval block would be the watermarked image which would have been sent over the communication channel. The entire purpose of this project is to authenticate or validate the contents of this watermarked image which has been received. This authentication process is just to ensure that the contents of the received watermarked image are not altered by an unauthorized source when it has been communicated over the channel from one end to the other. The process for watermark retrieval is almost similar to that of the watermark embedding block except that the watermark is retrieved by subtracting from the contents of the LL2 sub-band of the original image. The entire process of watermark extraction is as shown in the Figure 5.

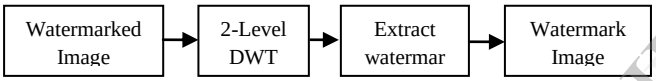


Fig 5: Watermark Retrieval Process

The watermarked image is first applied to the DWT block, where a 2-level haar DWT is applied to decompose the watermarked image to arrive at LL2 sub-band. Later, the watermark which is inserted in this sub-band is extracted using the equation 2.

$$RW = (WMI - k * LL2) \ldots\ldots\ldots\ldots (2)$$

Where *RW* = Recovered Watermark
LL2 = low frequency approximation of the original image
WMI = Watermarked Image
Value of k is same as the value which was used during embedding the watermark.

C) Simulink Model

The proposed system has been developed using matlab simulink, a hardware model for the same has been generated using Xilinx system generator and has been implemented over Spartan 6 board.

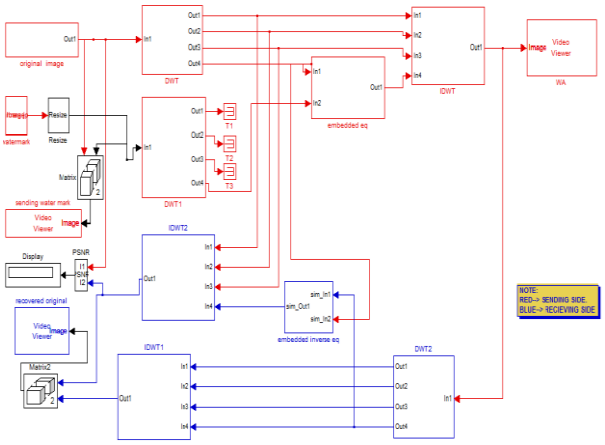


Fig 6: Simulink Model for proposed scheme

This model includes both the watermarking and the retrieval blocks working together. As a measure of the perceptibility of the extracted watermark, PSNR of the extracted watermark image is measured.

D) System Generator Architecture

System generator architecture for watermark embedding scheme is as shown in the Fig 7.

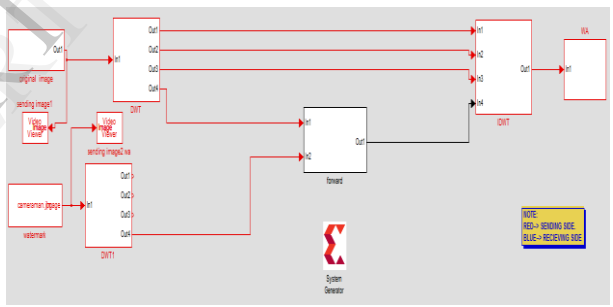


Fig 7: System generator architecture for watermark embedding

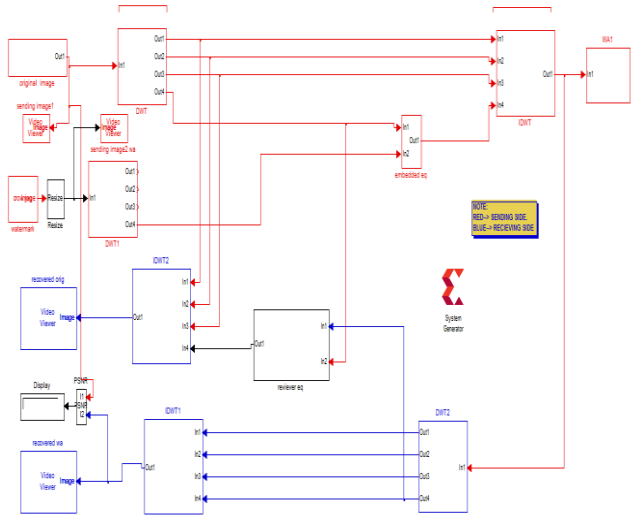
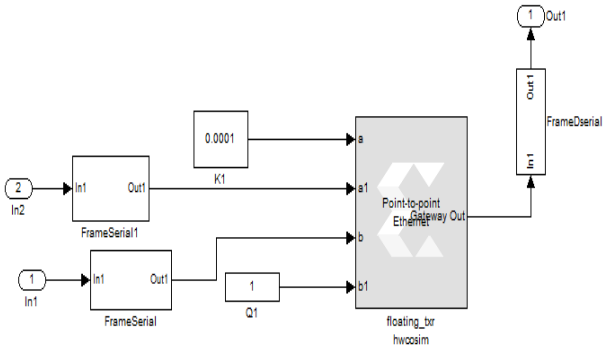
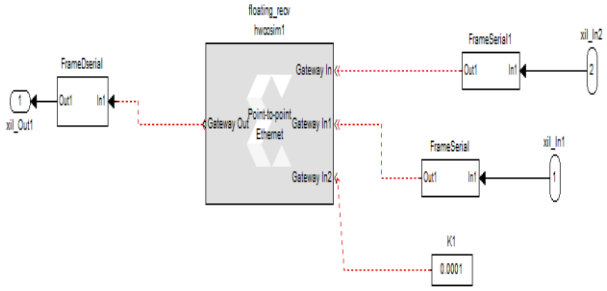


Fig 8: System generator architecture for watermark embedding and extraction.

The complete architecture which includes both the watermark embedding and extraction is as shown in the above Fig 8.



(a)



(b)

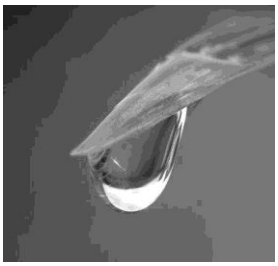
Fig 9 a) Watermark embedding subblock b) Watermark extraction subblock

VI. RESULTS

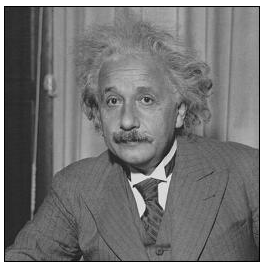
A. Selected input images

(a) Bridge

(b) Horse



(c) Dew Drop



(d) Einstein

Fig 10 Input Original Images

B. Selected Watermark Images

(a) Ship

(b) Crow

(c) Sunflower

(d) Hibiscus

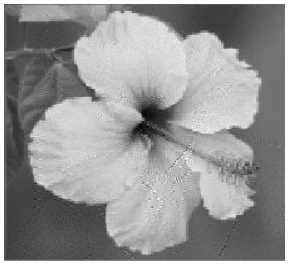
Fig 11: Input watermark Images

C. Watermarked Images

(a) Bridge

(b) Horse

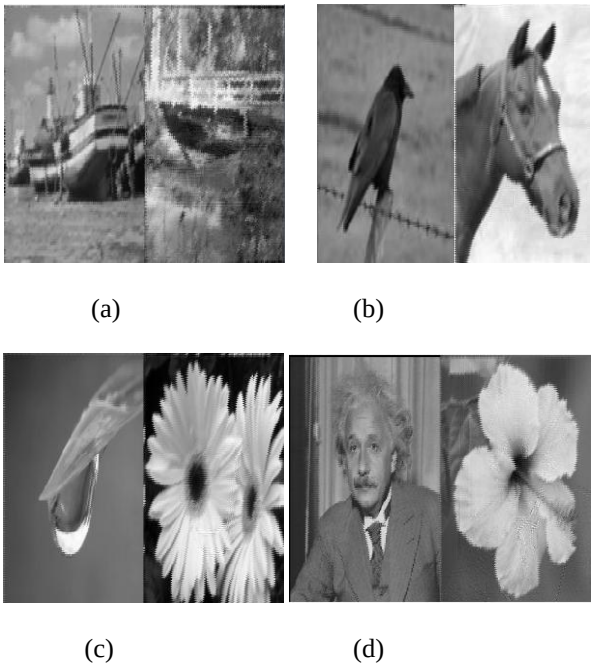
(c) Dew Drop



(d) Einstein

Fig 12 Watermarked Images

D. Extracted Watermark and Original Images



(a) (b)

(c) (d)

Fig 13 Extracted watermark and original images

VII. PERFORMANCE OF THE PROPOSED SCHEME

TABLE I Comparison between original and watermarked Image

Sr.No	Original Image	Watermark Image	PSNR Value
1	Bridge.jpg	Ship.jpg	23.64
2	Horse.jpg	Crow.jpg	27.64
3	Dew Drop.jpg	Sunflower.jpg	20.68
4	Einstein.jpg	Hibiscus.jpg	25.24

TABLE II Comparison between original and recovered watermark.

Sr.No	Original Watermark	Re.Watermark Image	PSNR Value
1	Ship.jpg	r_Ship.jpg	20.33
2	Crow.jpg	r_Crow.jpg	24.61
3	Sunflower.jpg	r_Sunflower.jpg	16.43
4	Hibiscus.jpg	r_Hibiscus.jpg	21.88

TABLE III PSNR for recovered watermark from hardware implementation

Sr.No	q	K	PSNR for recovered watermark
1	1	0.1	11.77
2	1	0.5	9.01
3	1	0.01	11.96
4	1	0.05	11.91
5	1	0.0001	11.97
6	1	0.0035	**12.22**
7	1	0.007	12.21
8	1	0.085	12.05
9	1	0.78	6.745
10	1	1	5.157

7. CONCLUSION

In current age of multimedia communication, authentication plays a vital role. This is just a means to ensure that the data which has been received, has been sent by a valid source or in other terms a means to exchange data securely without any modification in the contents of the actual information by an unauthorized source. This method of authentication by watermarking technique using DWT has been implemented to ensure that exchange of data between two entities are valid and also proves that the data has not been altered.

REFERENCES

[1] Neeraj Bhargava, M.M Sharma, Abhimanyu Singh Garhwal and Manish Mathuria, “Digital Image Authentication system Based on Digital Watermarking”, International conference on Radar, Communication and Computing, pp 185-189, December 2012.

[2] Gurupreet kaur, Kamaljeet kaur,”Image watermarking using LSB”, IJARCSSE, volume 3, Issue 4,pp858-861, April 25, 2013.

[3] Pravin M.Pithiya, H.L. Desai,”DCT based Digital Image Watermarking, De-watermarking & Authentication, IJLTET, vol.2, Issue 3,pp. 213-219, May 2013.

[4] Akhil Pratap Singh et. al.., “ Wavelet Based Watermarking on Digital Image”, Indian Journal of Computer Science and Engineering Vol 1 No 2, 86-91.

[5] Mustafa Osman Ali, Elamir Abu Abaida Ali Osman et. al.. “Invisible Digital Image Watermarking in spatial domain with random localization”, International Journal of Engineering and Innovative Technology, Volume 2, Issue 5, November 2012.

[6] R.S. Alomari, A AI-Jaber, "A Fragile watermarking algorithm for content authentication" in IEEE Trans. JCIS, vol. 2, No. 1, April, 2004.

[7] X. Zhang, S. Wang, "Fragile watermarking with error-free restoration capability," in IEEE Trans. on Multimedia, vol. 10, no. 8, December, 2008.

[8] Chih-Yang Lin and Yu-Tai Ching, “ A Robust Image hiding method using wavelet technique”, Journal of information science and engineering vol 22, 163-174 (2006)

[9] Cox, I. J., Kilian, J., Leighton, F. T., Shamoon, T.,”Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans.On Image Processing, No. 6, Vol. 12,pp 1673-1687, 1997.

[10] Ibrahim Nasir, Ying Weng, Jianmin Jiang, “ A new robust watermarking scheme for color images in spatial domain”,

[11] Henri Bruno Razafindradina and Attoumani Mohamed Karim," Blind and Robust Images watermarking based on wavelet and edge insertion", International journal on cryptography and information security, vol 3, No 3, September 2013.

[12] B. Chanda and D. DuttaMajumder, "Digital Image Processing and Analysis", Second Edition, PHI Publication.

[13] Peining Tao and Ahmet M Eskicioglue, " A Robust multiple watermarking scheme in Discrete Wavelet Transformation Domain".

[14] Ali Al-Haj, " Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science vol 3,No.9, pp 740-746,2007.

[15] Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, "A Survey on Digital WatermarkingTechniques",International Journal of Computer Science and Information Technologies, Vol. 4 (3) 2013, 451-456.