Implementation of FPGA based Image Identification using modified Watermarking Algorithm

[1]R. Radeep Krishna, [2]G.Sujitha Rajeswari, [2]S.Vani, [2]S.Visithra
[1]Assistant Professor-I, [2] Final year, B.Tech Electronics and Communication Engineering
Kalasalingam University, (KLU)

***ABSTRACT:* The digital watermarking is a method used to hide or embed a unique information into a digital image. The algorithm of digital watermarking is applied on a hardware. Several software based encryption and watermarking techniques already exist. Both the watermarking and encryption techniques on field programmable gate array (FPGA). These technique are used in government identification proofs. To avoid cheating in Passport and Aadhar card. The development of the system is utilized by MATLAB and SIMULINK for simulation environment. After this, water marking and encryption on FPGA is attempted using ALTERA KIT for water marking algorithm. In this major work describes a watermark embedding technique for images. The application of watermarking ranges from copyright protection, file tracking and monitoring. It was proposed in one of a main classification structures of watermarking techniques. A watermarking system conceals information inside some other data.**

Keywords—Digital Watermarking Technique, Encryption, FPGA, ALTERA Kit.

I. INTRODUCTION

Watermarking technique is to support and finding more solution for protection of intellectual property rights. It has number of current and potential application relating to the national security and law enforcement. In this algorithm, the whole form of data and converted it into target image as encryption. The encryption is suitable for the data security and authentication. To make the image secure and vulnerable for theft, encryption process is chosen. The prime attention is to maintain the original image same as the host image. Because the images are the combination of pixels arranged in proper manner. So encryption algorithm is applied maintained. The same technique is applied for biometric applications as keys. Digital watermarking technology is now drawing the attention as a new method of protecting copyrights for digital images. The embedded image or data is called watermark. So watermarking in digital images is the process by which a discrete data stream is hidden within an image imposing imperceptible changes of the image. The main aim of watermarking as an information hiding technique traced in ancient Greece as Steganography [3], the science of watermarking is a modern subject was organized developed in recent years. The application of watermarking ranges from copyright protection, file tracking and monitoring. It was proposed in one of a main classification structures of watermarking techniques. From this classification, there are two types of watermarks, the visible ones, like different logos either on paper or on a TV.

II. MOTIVATION AND PROBLEM IDENTIFICATION

The major problem happening everywhere is, images in the identification proofs are misused by some people. There were lot of ideas are used to prevent the illegal works done in the government proofs. The solution for this problem is creating an watermarking image. It provides the major solution for these illegal works. Encryption process can also done for the image security. The watermark is given to original image. So we are using the watermarking algorithm.

TYPES OF DIGITAL WATERMARKS

The watermarking techniques can be divided into various categories in various ways. Watermarking techniques divided into four categories according to the type of document to be watermarked as follows

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows

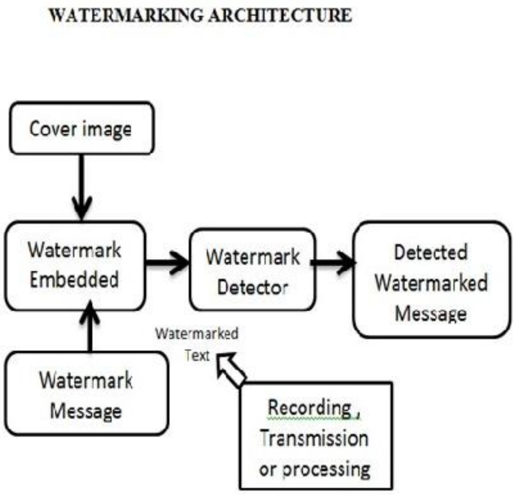
- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

III. WATERMARKING ALGORITHM

Digital watermarking is a proposed solutions for copyright protection of multimedia data. The technique is better than Signatures and other methods because it does not increase overhead. Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media such as the image, audio or video. The embedding take place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. In this paper cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks.

A. Discrete Wavelet Transform

The hierarchical property of the DWT offers the possibility of analysing a signal at different resolutions (levels) and orientations. This multiresolution analysis gives both space and frequency localization, and different orientations extract different features of the frame, such as vertical, horizontal, and diagonal information. Through wavelet analysis, an original image can be decomposed into an approximate image LL and three detail images LH, HL and HH. Using wavelet analysis on the approximate image again, fourlower-resolution sub-band images will be got, and among them, the approximate image hold most of the information of the original image, while the others contain some details such as the edge. Generally, edges and textures will be represented by large coefficients in the high frequency sub-bands, and they are well localized within the sub-band. In practice, wavelet analysis is performed using multilevel filter banks. Essentially this comprises a succession of filtering and sub sampling operations The DWT of an image has two parts: an approximation part (this is an image with smaller dimensions) and a detail part (this is a set of images with smaller dimensions containing the details of the original image). Hence the DWT gives the access to the details of the original image. This is very important because changing only the less important details of an image is easy to insert a watermark in this image, keeping the insertion procedure invisible.


WATERMARKING ARCHITECTURE
Cover image
Watermark Embedded
Watermark Detector
Detected Watermarked Message
Watermarked Text
Watermark Message
Recording , Transmission or processing

WATERMARK EMBEDDING ALGORITHM IN A WAVELET DOMAIN

In the embedded algorithm, we first decompose the image into several bands with a pyramid structure as shown in Fig. 2, and then add pseudo-random sequence to the large coefficients which are not located in the lowest resolution. DWT Watermark embedded algorithm is composed of four parts: original image, calculation of multi-level thresholds for selecting perceptually significant coefficients, watermark insertion process, and inverse wavelet decomposition (IDWT) of the coefficients with watermarks. Fig. 3 illustrates the overall process of watermark embedded algorithm.
The original image and digital watermark are represented as

f = f (i, j), 0 i < M1, 0 j < M2 --------> (3) W I =

w(i, j), 0 i N1, 0 j < N2 --------> (4)

Where ***f*** **(*i*, *j*)** ∈ **{0, 1, . . . , 2*y* − 1}** is the intensity of pixel **(*i*, *j*)** and *y* is the number of bits used in each pixel, ***w*(*i* , *j*)** ∈ **{0, 1}.**

To find the perceptually significant wavelet coefficients for each sub-band, the threshold value is calculated according to the decomposition level.

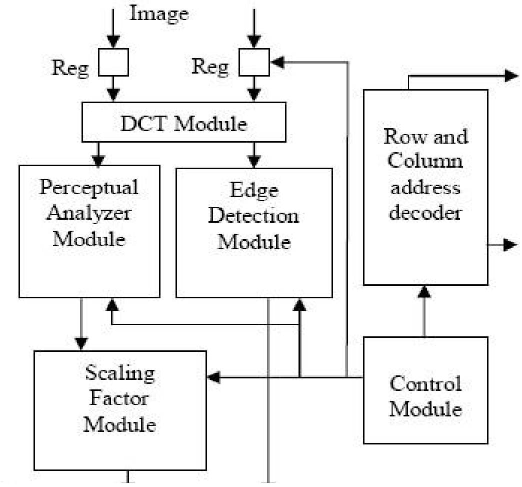
B. SPATIAL WATERMARKING

It can also be applied using color separation. The watermark appears in only one of the color bands, which renders the watermark visibly good such that it is difficult to detect under normal visibility. However, the mark appears immediately when the colors are separated. This reveals that, document is useless for the printer unless the watermark can be removed from the color band. This is commercially used for journalists to inspect digital pictures from a photo-stockhouse before buying unmarked versions.

*C.*VISIBLE WATERMARKING UNIT

The visible watermarking module is composed of several submodules, such as DCT, perceptual analyzer, edge detection, scaling factor, insertion, row and column address decoder, registers and controller. The DCT module which calculates the DCT coeffcients of host and watermark images before they are stored in the scratch memory. The controller governs the operations of all the other modules and the data in the watermarking unit. Address decoders are usually to decode the memory address where the image and watermark are stored.
FPGA Implementation:

Model based design to target FPGAs or ASICs an design and simulate systems with MATLAB Simulink and stateflow and then generate bit-true, cycle-accurate, synthesizable Verilog and VHDL code. Simulink code generation software used to automatically generate synthesizable hardware description language (HDL) code. Additionally, it provides automatic generation of HDL test bench, which enables design verification upon implementation. The simulation has been accomplished by using DWT algorithm. [256 256] dimensional matrix is represented as input image, which is a gray scale image. The original image converted into vector format and then decimal to binary conversion is also done.



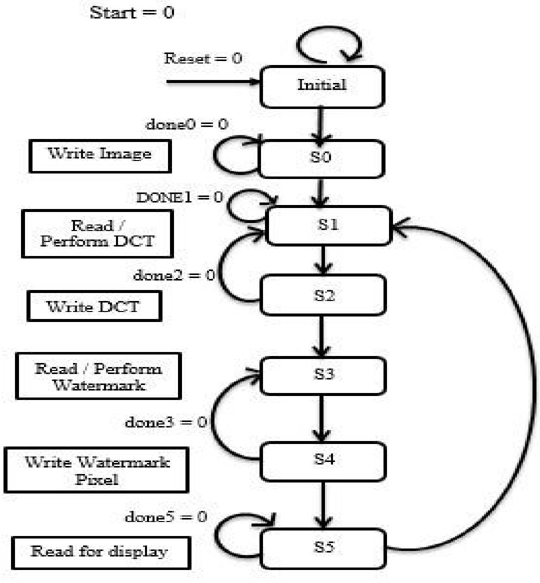


Fig.3. Finite State Machine of the Controller

DSP BUILDER COMPILER TO FPGA

Implementation of MATLAB Simulink file to the embedded system (FPGA board) done with DSP Builder software. When we create the final Simulink model, then we need to convert it to VHDL code for FPGA board [11]. VHDL code is one of the FPGA board languages [12]. By using of DSP Builder software we generate VHDL code for FPGA board then when the compilation was done without any error, we select Specific board; here in this project we used DE2-115 board made by Terasic (figure 5). This board uses Cyclone II E chip. DE2-115 FPGA board made by Terasic features the Cyclone IV E device and is the low cost, low power and a rich supply of logic,memory and DSP capabilities.

Fig. 4. DE2-115 board (www.Terasic.com)

Conclusion:

The image watermarking algorithm for copyright protection based on the discreet wavelet transform was presented in this paper. The process of the proposed algorithm, including watermark embedding, and watermark detection, is described. The pro-posed algorithm helps us to place watermark in a higher level sub band with an appropriate energy resulting in watermarked image that has more invisibility but still robust. A new metric that measure the objective quality of the image based on the detected water- mark bit is introduced. The experimental results have shown that the proposed watermark is invisible to human eyes and very robust to various attacks, such as image compression, image filtering, geometric transformations and noises.

Future Scope:

The design and architecture of FPGA implementation of the watermark unit werepresented. And the future scope of this project is to create an watermark for video processing and audio. It is the most easiest way to secure the data from the hacking and tha copyright protection is maintained.

References

1. G. L. Friedman, “The Trustworthy Digital Camera:Restoring Credibility to the Photographic Image,” *IEEE Transactions on Image Processing.* Vol. 39, no. 4 pp.905-910, Nov. 1993
2. I. J. Cox, J. Kilian, F.T. Leighton, and T.Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp.1673-1687, Dec. 1997.
3. S. P. Mohanty, N. Ranganathan, and R. K.Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S2DC) Design", *IEEE Transactions on VLSI Systems, Vol. 13, No. 7, July 2005, pp. 808-818.*
4. S. P. Mohanty, “Watermarking of Digital Images,” M. S.Thesis, Dept. of Electrical Engineering, Indian Institute of Science, India, 1999.
5. N. Memon and P. W. Wong, “Protecting Digital Media Content,” *Communications of the ACM*, vol. 41, no. 7, pp.34–43, July 1998.
6. http://www.altera.com/technology/dsp/dsp
7. -builder/dspsimulink. html DSP Builder information
8. http://www.mathworks.com/products/slhd lcoder/description1.html
9. http://www.mathworks.com/company/eve nts/webinars/wbnr51985.
10. html -- Webinar on Simulink HDL coder