International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 19th Dec 2018. Link :

http://www.ijiemr.org/main/index.php?vol=Volume-07&issue=ISSUE-13

Title: **DESIGN AND IMPLEMENTATION OF VISIBLE AND INVISIBLE WATERMARKING**

Volume 07, Issue 13, Pages: 604–609.

Paper Authors

MS. G. MANAVATHA VARDINI, DR. K. HEMACHANDRAN

Ashoka Institute of Engineering and Technology

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DESIGN AND IMPLEMENTATION OF VISIBLE AND INVISIBLE WATERMARKING

[1]MS. G. MANAVATHA VARDINI, [2]DR. K. HEMACHANDRAN$_{PH.D}$
[1]M.Tech Scholar, VLSI System Design (ECE), Ashoka Institute of Engineering & Technology
[2] Professor & HOD, Department of ECE, Ashoka Institute of Engineering & Technology
[1]gmvardini@gmail.com , [2]hemachandranvcet@gmail.com

Abstract

Presently, digital watermarking would emphasizes on the data hidden techniques and logical concepts which would focus on either image, video, audios, or from the signal source. This concept relates to a steganography where both the design process are emphasized on securing the input data within the digital signal. To improvise the encryption we modify multimedia data from one form of digital object to another form, where this work would leave the source frame as intact and as recognizable. The current design is modelled based on the low power, real time, reliable and multiple images based on secured watermarked systems, which are achieved through hardware implementations. This thesis paper, we present the Verilog model for the implementation of an invisible and visible watermarking encrypter and decrypter . It's a hardware model for video validation framework utilizing this watermarking procedure structures least video quality corruption and can survive certain potential assaults, i.e., conceal assaults, trimming, and portion expulsion on video successions. Moreover, the proposed equipment based watermarking framework includes low power utilization, ease of execution, high handling rate, and unwavering quality

1. Introduction: Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

2.Research Work:

Recent researchers on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and robustness of a watermarking scheme. In this approach, watermark is created from the content of the host image and Discrete Wavelet Transform (DWT) is used for embedding watermarks, since it is an excellent time frequency analysis method which can be adapted well for extracting the information content of the image .Lin et al put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence. In addition, watermarking in DWT domain has drawn extensive attention for its good time-frequency features and its accurate matching of the Human Visual System (HVS).Chen et al proposed two DWT-based audio watermarking algorithms that one of them is based on optimization scheme using group-amplitude quantization and the other embeds information by energy-proportion scheme. Therefore, normalized energy is used instead of probability which rewrites the entropy in information theory as energy proportion function.Preda et al proposed three DWT-based video watermarking approaches in which the watermarks used are binary images. Although, in one of them a spread-spectrum technique is used to spread the power spectrum of the watermark data, in the two others, watermarking methods are based on a combination of spread spectrum and quantization.

3. Implementation

3.1 Broad Classification Of watermarking Techniques:

Watermarking techniques can broadly be classified based on their inherent characteristics:

3.1.1 Visible watermarks:

A visible alteration of the digital image by appending a “stamp” on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.

3.1.2 Invisible watermarks:

By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non repudiation.

3.2 The following are criteria for a visible watermark:

1. The watermark must be apparent on all kinds of images.

2. The size of the watermark is crucial. The more pervasive the watermark the better so that the watermarked area cannot be modified without tampering with the image itself.

3. The watermark must be fairly easy to implant in the image.

The Watermarking Process

The watermarking process comprises of the following stages .

1. Embedding stage

2. Extraction phase

3. Distribution stage

4. Decision stage

3.2.1 Embedding stage:

In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients .

3.2.2 Extraction stage:

In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image .

3.2.3 Distribution stage:

The watermarked image obtained above is then distributed through digital channels (on an Internet site). In the process, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a few. Peter Meerwald [refers to the above as “coincidental attack”. Any of the above may put the watermarking scheme to test, as we will see in the ensuing section. In addition, malicious attacks also are possible in this stage to battle with the watermark. These are referred to in Meerwald’s work as “hostile attacks”.

3.2.4 Decision stage:

In this stage, the extracted watermark is compared with the original watermark to test for any discrepancies that might have set in during distribution. A common way of doing this is by computing the Hamming distance .

$$\mathrm{HD} = \frac{(\mathrm{W}^{\mathrm{mod.}}\ \mathrm{W})}{\parallel \mathrm{W}^{\mathrm{mod}} \parallel . \parallel \mathrm{W} \parallel}$$

Where, both the numerator and the denominator are the dot products.HD obtained above is compared to a threshold, T, to determine how close Wmod is to W.

3.3 Block diagram of digital watermarking:

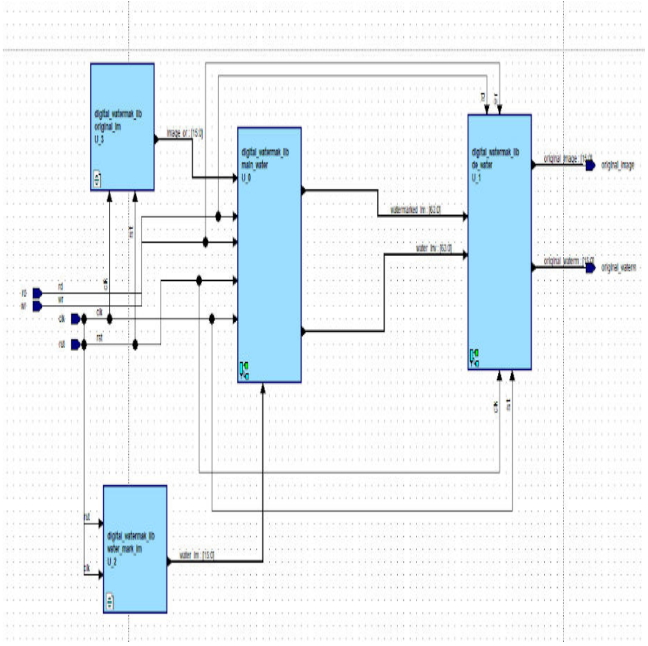

Fig 3.3 Block Diagram

3.4 Discrete Wavelet Transform:

Discrete Wavelet Transform (DWT) is a neoteric technique consecutive used in digital image processing, compression, digital watermarking etc. Discrete wavelet transform is more efficient than discrete cosine transform method. The image is dissolved into high and low frequency elements in two level Discrete Wavelet Transform (DWT). The robustness with respect to divers attacks increases when the watermark is embedding in low frequencies gained by Wavelet Decomposition (WD). Now first digital media is segmented into frames, Then discrete wavelet transform is applied to luminance element of each frame which outcomes into discrete sub bands. Again these bands are dissolved into discrete components. Now covariance matrix is calculated for each component. Now watermarked luminance component of the frames are gained by applying inverse discrete wavelet transform. Ultimately watermarked digital media is gained by renewing the watermarked frame.

3.5 Review Of LSB :

The Least Significant Bit (LSB) technique is used for simple operation to embed information in a cover image. The LSB technique is that inside of a cover image pixels are changed by bits of the secret message. Although the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be changed according to the embedded message. On the average, only half of the bits in an image will need to be modified to hide a secret message using a cover image. Because the quality of the Watermarked image is low, less than over the 4-bit LSB, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits, since, it has performed very simple operation. For example, Figure 1 shows the 1-bit LSB. In Figure 1, the pixel value of the cover image is 141(10001101)2 and the secret data is 0. It applies to LSB-1 that the changed pixel value of the cover is 140(10001100)2. LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.

3.6 Proposed Method :

`Based on LSB technique, we propose a new watermarking algorithm. Most of researchers has proposed the first LSB but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. This is because of the security reason. So, no one will expect that the hidden data in the third and the forth LSB. Figure 2 shows the framework of the proposed method. First, we select the image which is a grayscale image and we will transfer the data to binary value after typing it. Then, we hide the data in the image using the proposed algorithm. Figure 3 shows the embedding algorithm in Verilog. Then, we will get the watermarked image. Then, the receiver will retrieve the data back. Figure 4 shows the extracting algorithm in Verilog. The data will be extracted from the watermarked image.

3.6.1 Embedding Algorithm :

In this section, we describe the embedding algorithm. After we select the image and type the secret data, we transfer the secret data to binary values and determine the coordinates of the image which the data will be embedded in. First, we will embed the length of the data in five pixels starting from the first coordinate which we select and jump by 5 until we embed it in the five pixels in the 3rd and 4th LSB, but if the length of data is more than 1023 characters, it will ask us to rewrite the data and it should be not more 1023 characters. Then, the data will be embedded in the image in the 3rd and 4th LSB. Then, watermarked image will be produced and it will be saved.

3.6.2 Extracting Algorithm :

In this section, we will describe the extracting algorithm. After receiving the watermarked image, we will get the length of the secret data from the 3rd and 4th LSB in the five pixels starting from the determined coordinates and jump by 5 until we get it from the five pixels. Then, we will get secret data also from the 3rd and 4th LSB in binary values. After that, we transfer the binary values to characters which will be shown as the secret data.

4. Applications

- Signature.
- Fingerprinting.
- Broadcast and internet monitoring.
- Authentication and integrity.

- Copy and copyright protection.
- Covert communication.

5.RESULTS:

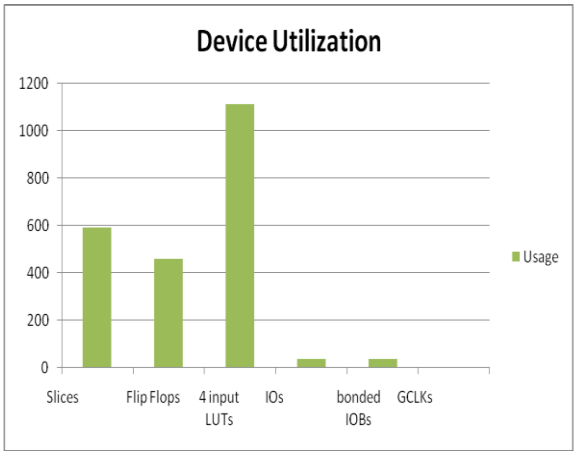

Fig 5.1 Device Utilization

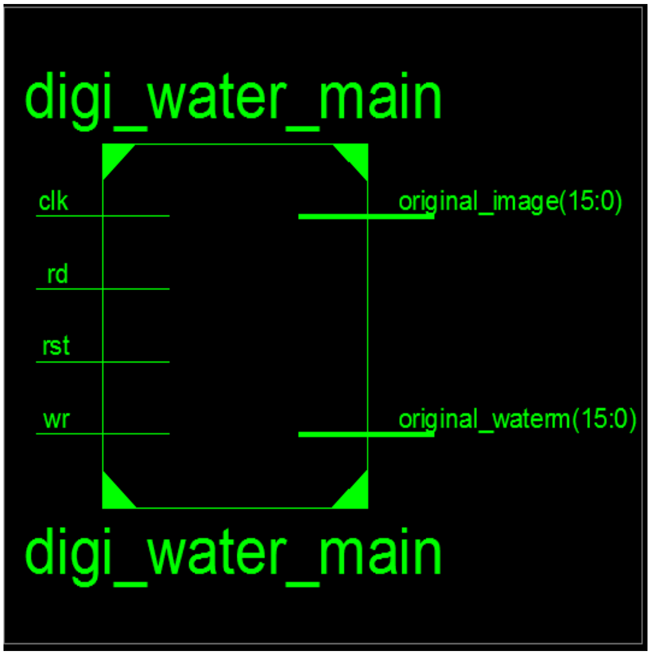

Fig 5.2 RTL Schematic Diagram

Here we are giving inputs as clk,rd,rst,wr to read the original image data and cover image data in this DWT-LSB process can applied then we get the watermark of original image data and cover image data.

5.1 Concept of digital watermarking:

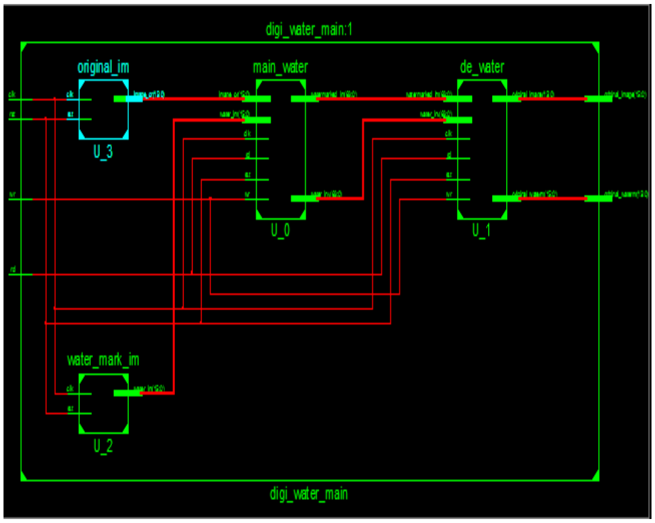

Fig   5.1 Concept of digital watermarking

This is concept diagram of digital watermarking here, we are creating the images by divide image into different n×n blocks and then we are intializing the values as we reqired. After completion of creating images are original image and cover image.These two images are given to the main water block here embedding preocess can be done in both ways invisible and visible types. Then we get the invisivle and visible watermarked images.Then these two images are given to the de- water block in this extraction preocess can be done then we will get the original image and cover image.

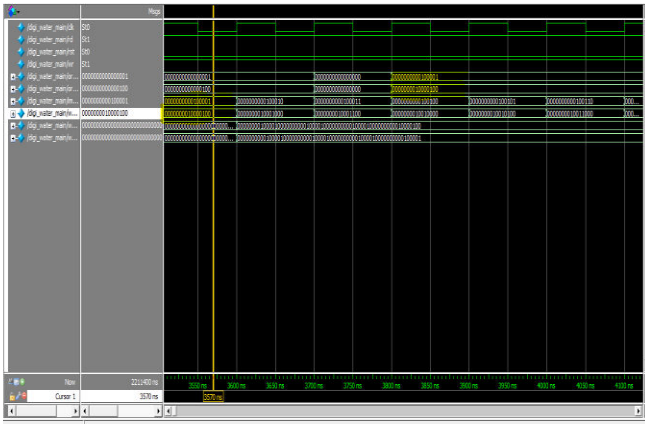

Fig 5.2 Output with respect to input

Here we can observe the original image data and cover image data after de watermarking and before watermarking.

5.2 Conclusion

The goal is to develop low power, real time, reliable and, secure watermarking systems. Over the past decade, numerous watermarking algorithms have been invented and their software are available.

5.3 Future Research:

Future research should concentrate on applying the watermarking algorithm to other modern video compression standards, such as MPEG-4/H.264, so that it can be utilized in various commercial applications as well. Embedding the watermark information within high resolution video streams in real time is another challenge.

References

[1] V. M. Potdar, S. Han and E. Chang. 2005. “A survey of digital image watermarking techniques,” in Proc. IEEE Int. Conf. Ind. Informatics, Aug. pp. 709–716.

[2] A. D. Gwenael and J. L. Dugelay. 2003. “A guide tour of video watermarking,” Signal Process. Image Commun., Vol. 18, No. 4, pp. 263–282.

[3] A. Piva, F. Bartolini and M. Barni. 2002. “Managing copyright in open networks,” IEEE Trans. Internet Comput., Vol. 6, No. 3, pp. 18–26.

[4] Y. Shoshan, A. Fish, X. Li, G. A. Jullien and O. Yadid-Pecht. 2008. “VLSI watermark implementations and applications,” Int. J. Information Technol. Knowl., Vol. 2, No. 4 pp. 379– 386.

[5] X. Li, Y. Shoshan, A. Fish, G. A. Jullien and O. Yadid-Pecht. 2008. “Hardware implementations of video watermarking,” in International Book Series on Information Science and Computing, no. 5. Sofia, Bulgaria: Inst. Inform. Theories Applicat. FOI ITHEA, pp. 9–16 (supplement to the Int. J. Inform. Technol. Knowledge, Vol. 2.

[6] K.E. Zhao J. 1994. Embedding robust labels into images for copyright protection, Technical Report, Fraunhofer Institute for Computer Graphics, Darmatadt, Germany. P. Bas, J.-M. Chassery and B. Macq. Image watermarking: an evolution to content based approaches Pattern Recognition, Vol. 35, pp. 545– 561.

[7] L. D. Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes and G. Depovere. 2000. “Implementation of a real-time digital watermarking process for broadcast monitoring on Trimedia VLIW processor,” Proc. Inst. Elect. Eng. Vision, Image Signal Process. Vol. 147, No. 4, pp. 371–376.

[8] Y. Shoshan, A. Fish, X. Li, G. A. Jullien and O. Yadid-Pecht. 2008. “VLSI watermark implementations and applications,” Int. J. Information Technol. Knowl., Vol. 2, No. 4 pp. 379– 386.

[9] X. Li, Y. Shoshan, A. Fish, G. A. Jullien and O. Yadid-Pecht. 2008. “Hardware implementations of video watermarking,” in International Book Series on Information Science and Computing, no. 5. Sofia, Bulgaria: Inst. Inform. Theories Applicat. FOI ITHEA, pp. 9–16 (supplement to the Int. J. Inform. Technol. Knowledge, Vol. 2.

[10] K. Jack. 2001. Video Demystified: A Handbook for the Digital Engineer, 2nd ed. Eagle Rock, VA: LLH Technology Publishing.