An Effective Image Watermarking using Weighted Median Prediction

Deepa H H[1] Asha. R[2] M N Eshwarappa[3]
[1]P.G. Student [2]Assistant Professor [3]HOD
[1,2,3]Department of Electronics and Communication Engineering
[1,2,3]VLSI Design and Embedded System, Shridevi Institute and Engineering Technology
Tumkur, Karnataka, India

Abstract— Now a days developing digital technology and security of digital data becomes a serious problem. Digital watermarking technique provide an effective security protection to digital data. Watermarking is recognizable an embedded image or pattern in a paper, people can observe it by transmitted or reflected light. It is often used as security features of banknotes, passports, postage stamps and other documents. Similarly, digital watermarking means embedding information in a digital signal. It is mainly used to verify the digital signals to authenticity or identity of its owners. Common contents of digital watermarking are audio, picture, or video. This proposed project discusses the basic concept of watermarking grayscale images using weighted median prediction operation. This mechanism will have minimum computation complexity. In this VLSI based data hiding process the secret digital signature is hidden in the host image. Performance will be increased. Along with that the PSNR value and PAYLOAD value increases.

Key words: Real Time Data Hiding/Watermarking, Spatial domain embedding, Reversible data hiding, Gray Scale Image, weighted median prediction

I. INTRODUCTION

Digital watermarking is the process of hiding a secret signature in host content to resolve the privacy and privacy issues during transmission and sharing of multimedia contents. The multimedia data may be an image, audio, video and random data bits. In the digital watermarking process, if the host is an image then the process is called digital image watermarking and the secret data to be embedded is called a watermark. The data hiding operation is reversible if the host content is reconstructed without any loss after the extraction of digital signature. It is irreversible if the host content is not retrieved accurately after the extraction of secret signature.

In the proposed data hiding technique the host is taken as a gray-scale image and the secret data (watermark) as a sequence of binary data bits. Here using median prediction operation on the neighbour Pixels and by applying weighted values technique hide the data in a reversible manner in real time. Majority of the watermarking algorithms focuses software based approach as an offline processing (i.e. the authentication and copy right protection is happening in captured and stored data values) whereas the hardware based watermarking happens in real time with a custom designed circuitry.

The concept of weighted median prediction of the image by dividing the image into three sets of pixels followed by data embedding strategy in the gray scale image. Predicting and replacing the neighbor pixel values by median based operation a redundant space is created to hide a lot of secret bits without affecting the visual quality of the image. (i.e. the median prediction process has to be carried out in a manner such that the sharpness of edges and artifacts are not created in the median predicted image). In weighted median prediction concept stated quality is well achieved with the help of median operation using the nearest neighbor pixel values.

II. AIM OF THE PROPOSED PAPER

The aim of the project is to design watermarked image using weighted median prediction with the help of MATLAB and Verilog. Initially these designs were developed using MATLAB to obtain a pixel values. After getting the pixel values, the design is then implemented on the Xilinx Spartan 6 FPGA development board. Finally, watermarked image is obtained with lesser distortion. These designs were developed using Verilog programming language in design entry software.

III. LITERATURE SURVEY

Digital image watermarking is one such technology that has been developed to protect digital images from illegal manipulations. In this author has discussed digital image watermarking algorithms which are based on the discrete wavelet transform have been widely recognized to be more prevalent than others. This is due to the wavelets excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the human visual system.

In this paper, author describe an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm. The algorithm watermarks a given digital image using a combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform. The discrete wavelet transform (DWT) and the discrete cosine transform (DCT) have been applied successfully in many in digital image watermarking.

This paper presents a novel invisible robust watermarking scheme for embedding and extracting a digital watermark in an image. Invisible insertion of the watermark is performed in the most significant region of the host image such that tampering of that portion with an intention to remove or destroy will degrade the quality and value of the image. One feature of the algorithm is that this sub-image is used as a region of interest for the watermarking process and eliminates the chance of watermark removal. Another feature of the algorithm is the creation of a compound watermark using the input user watermark and attributes of the host image.

This facilitates the homogeneous fusion of a watermark with the cover image, preserves the quality of the host image, and allows robust insertion-extraction.

Watermark creation consists of two distinct phases. During the first phase, a statistical image is synthesized from a perceptually important sub-image of the image. A compound watermark is created by embedding a watermark into the statistical synthetic image by using a visible watermarking technique. 3] With the widespread use of networks, intellectual properties can be obtained and reproduced easily. This creates a high demand for content protection technique like watermarking, which is one of the most efficient ways to protect the digital properties in recent years. This paper reviews several aspects and techniques about digital watermarking.

This paper reviews various techniques for watermarking data files like text, image, audio and video. In this paper author conclude that watermarking is a potential approach for protection of ownership rights on digital properties. According to different applications, there are different requirements of the watermarking system. However, it is hard to satisfy all the requirements at the same time. So, benchmark is used to evaluate and compare the performance of different watermarking systems.

With the fast development of web technology and the digital multimedia, the usage of multimedia (audio, video and image etc.) has been widely spread. By increasing of these things, intellectual properties can be obtained and reproduced simply. So there is need of our content protection therefore to do so there is a technique like watermarking, which is one of the most effective ways to safeguards the digital properties of our object. This paper reviews various techniques and aspects about digital watermarking.

IV. PROPOSED SYSTEM

This paper reviews many techniques for watermarking data files like audio, text, image and video. So, we can conclude that watermarking is a significant approach for protection of copyrights on digital properties. Different watermarking techniques are used for various types of requirements. However, it is difficult to satisfy all the requirements at the same time. So, benchmark is used to compare the performance of different watermarking systems and this section explains the concept of weighted median prediction of the image by dividing the image into three sets of pixels followed by data embedding strategy in the grayscale image. As we are predicting and replacing the neighbour pixel values by median based operation a redundant space is created to hide a lot of secret bits without affecting the visual quality of the image. (i.e. the median prediction process has to be carried out in a manner such that the sharpness of edges and artifacts are not created in the median predicted image).In weighted median prediction concept the above stated quality is well achieved with the help of median operation using the nearest neighbour pixel values.

A. Weighted Median Prediction

In the weighted median operation, the four sets of pixels, base pixel, first neighbour pixel, second neighbour pixel and the third neighbour pixel values are determined first. For every four pixels the first one is to be considered as the base pixel and the pixel left to it is considered to be the third neighbour pixel. Similarly the pixels below the base pixel in the left side are considered as second neighbour and the pixel in diagonal side is marked as first neighbour pixel.

By performing the median operation, the correlation between the neighbour pixels is well maintained in such a way that there is no edge shifting and occurrence of new artifacts in the host image is eliminated. The calculation of neighbour pixel values using median operation results in good visual quality with higher resolution at the cost of higher complexity. In the weighted median operation, first the three sets of pixels are identified with a base pixel value. Then the three sets of the pixel values are replaced by its weighted median values from its neighbour pixel. Here the base pixel, first set pixel, second set pixel and the third set pixel values

0	3	0	3	0	3
2	1	2	1	2	1
0	3	0	3	0	3
2	1	2	1	2	1
0	3	0	3	0	3
2	1	2	1	2	1

Fig: 1: Image Block with One Base Pixel and Three Identified Pixels

To find the median values

$$\text{Median}(X_1, X_2, X_3 \ldots X_n) = \begin{cases} \\ (X_{(n)/2} + X_{(n+1)/2})/2 & \text{otherwise} \end{cases}$$

To find the weighted median prediction value

$$WM(\{X_1, X_2, X_3 \ldots X_n\}\{w_1, w_2, w_3 \ldots w_n\})$$
$$= \text{median}(X1 \Theta w_1, X_2 \Theta w_2 \ldots Xn \Theta w_n)$$

Where w_1, w2, w3….w_n represent the weights assigned to the corresponding pixel values and the symbol Θ represents the repetition of the gray integer pixel values according to their weights.

167	240
168	255

→

167	240
168	204

Fig -2 a) 2 X 2 Sample Image Block before Weighted Median b) 2 X 2 Sample Image Blockafter Weighted Median.

For the above 2 X 2 image block calculating the median values using the weighted median as follows

$$WM(\{167,168,240,255\}.\{1,1,1,1\})$$
$$= \text{median}(167,168,240,255) = 204$$

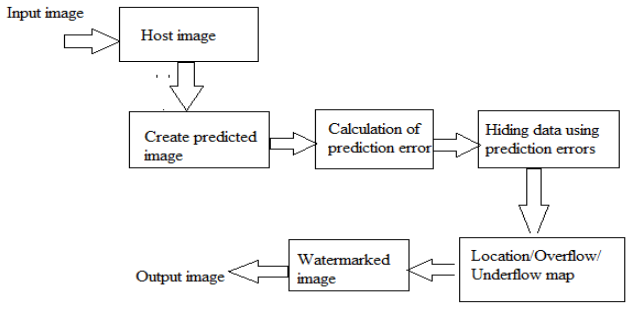

Fig. 3: Block diagram of digital watermarking of gray scale image

B. Watermarking in Image

In the watermarking process first the median values of the three sets of the pixels are calculated and replaced by its value. Then the error difference between the original image and median processed image is calculated using the integer transform.

$$E = P' - P$$

Those pixels having error difference closest to zero are used to hide the watermark secret data bits. For the entire watermarking process we adopt a threshold value (m) associated with each error difference. For those pixels if the error difference is less than or equal to threshold (i.e. |E|<=m) we can hide a secret bit by multiplying the error difference by a factor k (k is considered as 2 here) and adding with the secret data bit. Similarly for those pixels whose predicted values are greater than the error difference (i.e. |E||>m) a constant shifting of magnitude by a factor of (m+1) is carried out uniformly.

C. Embedding Process

a) Read the host image and secret digital signature from the memory.
b) Perform the prediction of base and three sets of pixels on the host image.
c) Calculate the weighted median values for each sets of pixel with their respective weighted values
d) Replace the value of the three sets of pixel with their corresponding weighted median values.
e) Calculate the difference in error between the original and weighted median predicted.
f) For those pixels having the error less than the threshold (m) we can hide the data and for greater than threshold we undergo constant magnitude shifting.

V. Proposed VLSI Architecture

In this section the proposed hardware data path architecture for the watermark embedding and extraction using weighted median prediction operation is discussed one by one as below.

A. Data Path for Watermarking

The watermarking Data path unit consists of two memories (ram or rom) of size host image and secret data. Then a predictor circuit consists of buffer to predict the three sets of pixels along with base pixels. After the predictor circuit median calculator, data path contains a comparator circuit to carry out the sorting operation in ascending order of the pixel intensities to find the median values. Then the difference in error between the original and median predicted value is calculated using a sub tractor circuit. Finally the watermark secret data bits are added to the host using an adder circuit.

B. Data Path for Extraction

The same data path structure is used for the data extraction process with a slight difference. The difference is the adder circuit is replaced by shifter circuit to retrieve the secret hidden in the host content. Here also a predictor circuit consists of buffer to predict the three sets of pixels along with base pixels. Then comparator based circuit is used to calculated the weighted median operation followed by subtract or circuit to find the error difference. Once again a shifter circuit is used to separate the watermark content from the predicted median watermarked content and restore the original data as such.

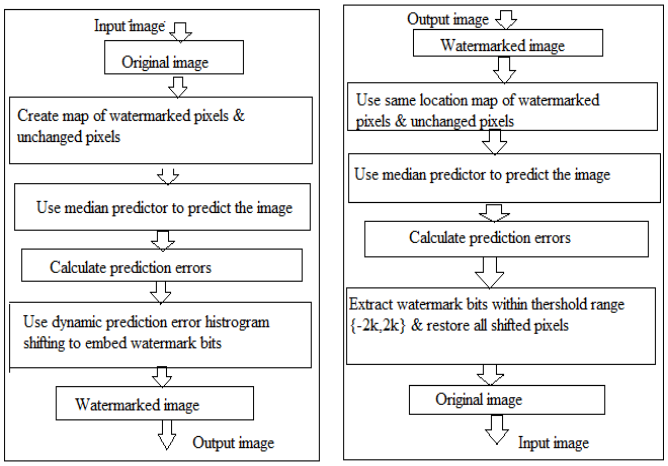

Fig. 4: Flowchart of proposed embedding and Extraction technique for watermarked image

VI. Experimental Results and Discussion

This section gives the simulation results using MATLAB R2012b© and Altera Quartus-II 11.0©. In the MATLAB implementation of watermarking process we have taken the boat as a host image of size 256 x 256 and the secret digital signature has to be considered as a random binary data. Then using the weighted median concept the secret data is watermarked inside the host with the predicted values of base pixel and three sets of pixels. The input and output images before and after watermarking is shown in the Fig-9. Here the PSNR and Embedding capacity is used as evaluation metrics to evaluate the effectiveness of this watermarking strategy. The corresponding values of the PSNR and embedding capacity is tabulated in table-I. In the same way we have compared our approach with 1-Bit LSB and 2-Bit LSB Substitution data hiding. Then we have modelled the same algorithm using Verilog HDL language with the initialization of the host image and secret data as a hex value in a ram. After executing the simulation, we verified that both the MATALB simulation and Verilog simulation will have the same results with no deviation. Then the entire watermarking embedding and extraction module is synthesized using Altera Quartus-II 11.0 © with their layout generation.

VII. Simulation Results

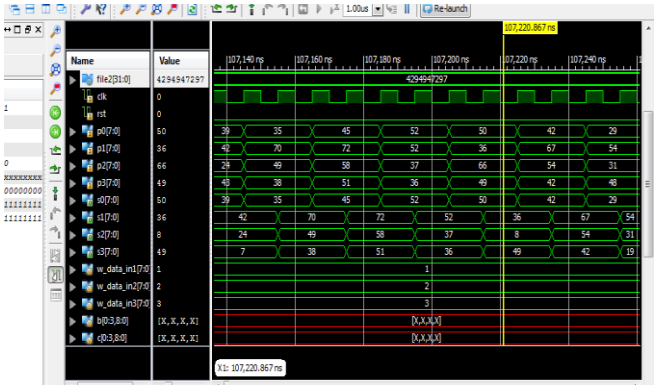

Fig. 5:

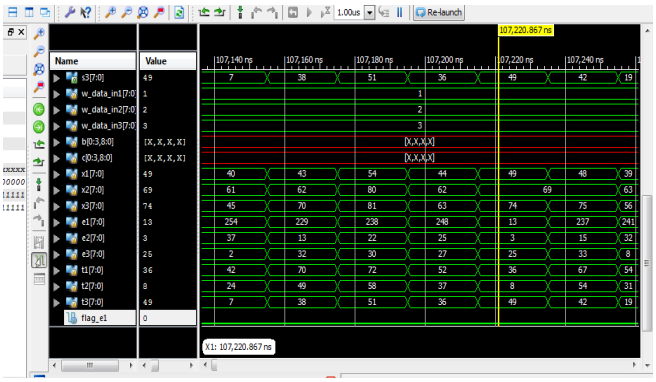

Fig. 6:

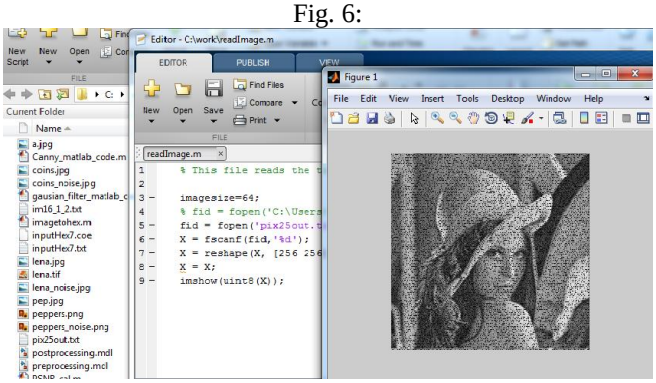

Fig. 7:

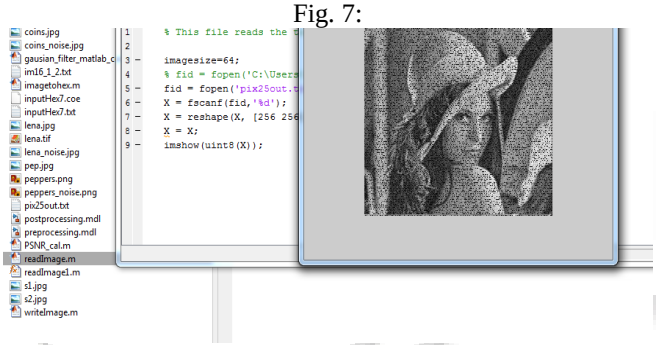

Fig. 8:

It is noted that there is no critical path in the design during the synthesis. The device utilization summary of the entire algorithm is given in the Table-II. The entire watermarking and extraction strategy consumes 646 logical elements, 312 combinational LUTs, 334 registers and 95IO pins.

Lenna IMAGE	Proposed	1BIT LSB	2 BIT LSB
Embedding Capacity	33087 bits	262144 bits	524288bits
PSNR(db)	46.33	44.89	43.36

Table 1: PSNR Value and Embedding Capicity Comparison

The imperceptibility and embedding capacity of this data hiding process is good when compared with the 1-bit LSB and 2-bit LSB embedding techniques which is well quantified by the PSNR values and embedding capacity. To highlight the runtime efficiency of the proposed hardware implementation over the software simulation a comparative study was made for a 256 x 256 gray scale image as host image. The software simulation is done using MATALB R2012b© platform running on a Intel® corei32350M processor with 8GB internal RAM and 2.3GHz Operating speed. This PC system takes 88.984 s for the entire process the algorithm. Alternatively the proposed architecture requires only 1043µs for an image of same size at 58.48MHz clock frequency. This implies that the proposed hardware architecture is quite fast in watermarking and most suitable for real-time applications.

VIII. Conclusion

In this paper we proposed a FPGA implementation of watermarking and extraction algorithm in real time with its VLSI architecture. Our algorithm does not make any change in the host image and the watermark is invisible. The watermark can be extracted by reversing the weighted median prediction embedding mechanism with a shifting operation. So the proposed algorithm provides an invisible, robust and real time high speed hardware implementation.

References

[1] Sakthivel. S.M., Ravi Sankar." A VLSI Architecture for Watermarking of Grayscale Images using Weighted Median Prediction" Ieee sponsored 2nd international conference on eletronics and communication system (icecs 2015)

[2] M.Hussain,M.Hussain,A survey of Image Stegnography Techniques, International Jouranl of Advance science and technology, Vol.54.May 2013

[3] A.M. Eskicioglu, E.J. Delp, An overview of multimedia content protection in consumer electronics devices, Elsevier Signal Processing Image Communication 16 (2001) 681-699.

[4] C.T. Li, Digital fragile wateramrking scheme for authentication of JPEG images, in: Proceedings – Vision, Image and Signal processing, vol. 151(6), 2004, pp. 460-466.

[5] P.Karthigaikumar,K.Baskaran, FPGA and ASIC implementationof robust invisible binary image watermarking algorithm usingconnectivity preserving criteria, Microelectronics Journal 42(2011),pp.82-88.

[6] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy,

[7] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[8] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security,vol. 3, no. (2008) September 3, pp. 488-497.

[9] Saraju P. Mohanty, N. Ranganathan and Ravi K. Namballa, "VLSI Implementation of Visible Watermarking for a Secure DigitalStill Camera Design", IEEE Proceedings of the 17th International Conference on VLSI Design (VLSID'04).

[10] S.P. Mohanty, N. Ranganathan, K. Balakrishnan, "A dual voltagefrequency VLSI chip for image watermarking in DCT domain", IEEE Transactions on Circuits and Systems II (TCAS-II) 53 (5) (2006),pp. 394–398.

[11] R.Naskar, R.S.Chakraborthy, Reversible Watermarkiing utilizing Weighted median based prediction, IET Image Processing.

