ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Invisible Image Water Marking Using Hybrid DWT Compression/Decompression Technique

B.Sai Kiran
M.Tech (VLSI),
CMR Institute of Technology.

Mr.Shahbaz Khan
Associate Professor,
CMR Institute of Technology.

Mrs.S.Siva Priyanka
Assistant Professor,
CMR Institute of Technology.

Abstract:

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. The complete system consists of two functions, one for hiding information inside image and other for detecting information from image. In this approach, digital watermarking performed using Lifting based Discrete Wavelet Transform and analyzed its results..This Paper proposes to implement the invisible LSB-watermarking technique with Lifting compression technique by using the microblaze Processor.

Keywords:
LSB hiding Technique, Lifting, Spartan3EDK, FPGA

Introduction:

The last decade has witnessed the rapid development in information technologies and the wide availability of digital consumer device such as digital cameras ,scanners etc .But at the same time this leads to the hacking vulnerability and duplicity of the original information. The most modern solution technique to this problem is digital watermarking scheme .Digital watermarking algorithms could be considered as digital communication scheme where auxiliary message is embedded in digital multimedia signal and are available where ever the later signals move.Watermarking is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object [1]. Watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality, ownership and source. In general, any watermarking scheme consists of three parts, such as the watermark, the encoder (insertion algorithm) and the decoder and comparator (verification or extraction or detection algorithm).

The insertion algorithm incorporates the watermark into the object, whereas the verification algorithm authenticates the object, determining both the owner and the integrity of the object. The watermarks can be applied either in spatial or in frequency domain (FFT, DCT or wavelet). Even though spatial domain watermarking is less robust, the spatial domain schemes have less computational overhead compared to frequency domain schemes. According to the human perception, the digital watermarks can be divide into four different types, such as visible, invisible robust, invisible-fragile and dual .

Each of the above watermarking schemes is equally important due to its unique applications. In this work, we focus on VLSI implementation of an invisible-robust and an invisible-fragile spatial domain watermarking algorithm. The VLSI chip can insert any one or both the watermarks depending on the requirements of the user. The proposed watermarking chip can be easily incorporated as a module in any existing JPEG encoder and a secured JPEG encoder can be developed. We provide an outline of such a secure JPEG encoder. It may be noted that the corresponding watermark extraction module has to be inbuilt in a secure JPEG decoder. The secure JPEG codec can be a part of a scanner or a digital camera so that the digitized images are watermarked right at the origin.

In most of the algorithms designed based on the principle of data hiding, requires the sending original cover image along with the encoded cover image to the receiver. This approach makes thedesigned algorithm weaker as it conveys some idea of data hiding to the sender. But our method only the encrypted image will be sent to the receiver. The design of this technique is based on extensive analysis of the data-hiding process.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Digital Watermarking Technique:

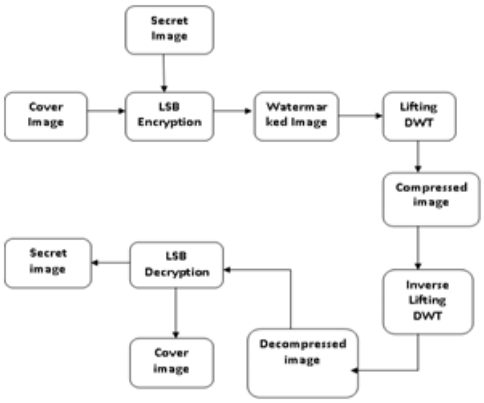

Fig1: Block Diagram of Digital Watermarking

The Block diagram of Invisible watermarking method using lifting method is shown in the figure.. First create a header file for cover Image by using the matlab software . Cover Image headerfile is inputed to the Least Significant Bit LSB technique to embed the data in that cover image, After getting the watermarked image apply the Lifting based DWT to compress the image. The above process will repeat in reverse process means getting decompression and LSB reverse method to get original image

Creation of Header file:

By using Matlab software to create the header file for Cover image and secret software.

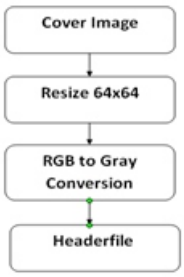

Fig2: Header file Creation

LSB Hiding Technique:

Fig. shows the 1-bit LSB. In Fig. 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 64 x 64 pixel image, it can thus store a total amount of bytes of embedded data.

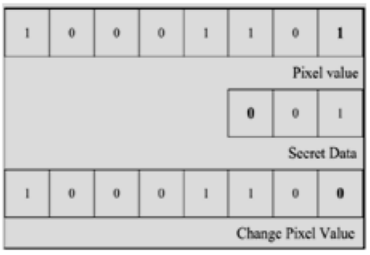

Fig3: LSB technique Description

LSB technique:

Proposed method based on LSB technique, we propose a new watermarking algorithm. Most of researchers have proposed the first LSB and the third and forth LSB for hiding the data but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. And using the RGB watermark image embedding in blue component of original image because of less sensitivity. This is because of the security reason. So, no one will expect that the hidden data in the third and the forth LSB. Fig. 2 shows the framework of the proposed method. First, we select the image which is a colour 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. Fig. 3 shows the embedding algorithm in VLSI.

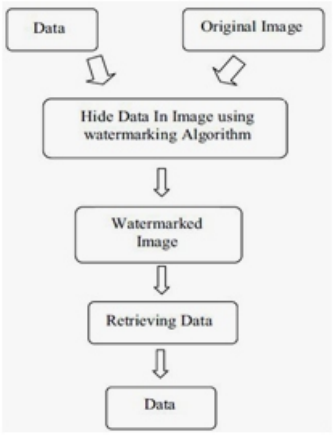

Fig4: Watermarking algorithm

Proposed Lifting Technique:

Fig. I shows the classical implementation and the litiing based implementation of DWT. Classical implementation is realized by the convolution of the input signals with the low pass filter (h,) and the high pass filter (hi). The lifting scheme is a new method to construct wavelet basis, which was first introduced by Swelden's.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The lifting scheme entirely relies on the spatial domain, has many advantages compared to filter bank structure, such as lower area, power consumption and computational complexity. The lifting scheme can be easily implemented by hardware due to its significantly reduced computations. Lifting has other advantages, such as "in-place" computation of the DWT, integer-to-integer wavelet transforms which are useful for lossless coding. The lifting scheme has been developed as a flexible tool suitable for constructing the second generation wavelets. It is composed of three basic operation stages: split, predict and update. Fig.3. shows the lifting scheme of the wavelet filter computing one dimension signal. The three basic steps in Lifting based DWT are:

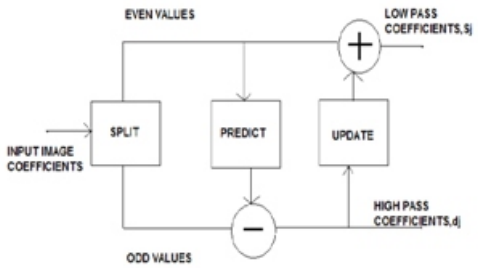

Fig5: Block Diagram of lifting technique.

Split: where the signal is split into even and odd points, because the maximum correlation between adjacent pixels can be utilized for the next predict step. For each pair of given input samples x(n) split into even x(2n) and odd coefficients x(2n+1).

Predict: The even samples are multiplied by the predict factor and then the results are added to the odd samples to generate the detailed coefficients .Detailed coefficients results in high pass filtering.

Update: The detailed coefficients computed by the predict step are multiplied by the update factors and then the results are added to the even samples to get the coarse coefficients .The coarser coefficients gives low pass filtered output.

The inverse transform could easily be found by exchanging the sign of the predict step and the update step and apply all operations in reverse order as shown in Fig.4.The implementation of lifting based inverse transform (IDWT) is simple and it involves order of operations in DWT to be reversed.

Hence the same resources can be reused to define a general programmable architecture for forward and inverse DWT.

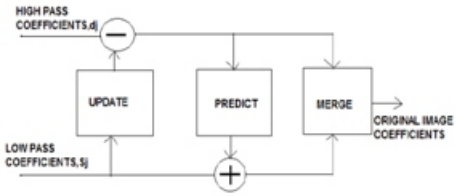

Fig6: Block diagram of Inverse Lifting technique

Xilinx Platform Studio:

The Xilinx Platform Studio (XPS) is the development environment or GUI used for designing the hardware portion of your embedded processor system. B. Embedded Development Kit Xilinx Embedded Development Kit (EDK) is an integrated software tool suite for developing embedded systems with Xilinx MicroBlaze and PowerPC CPUs.

EDK includes a variety of tools and applications to assist the designer to develop an embedded system right from the hardware creation to final implementation of the system on an FPGA. System design consists of the creation of the hardware and software components of the embedded processor system and the creation of a verification component is optional.

A typical embedded system design project involves: hardware platform creation, hardware platform verification (simulation), software platform creation, software application creation, and software verification. Base System Builder is the wizard that is used to automatically generate a hardware platform according to the user specifications that is defamed by the MHS (Microprocessor Hardware Specification) file. The MHS file defines the system architecture, peripherals and embedded processors]. The Platform Generation tool creates the hardware platform using the MHS file as input.

The software platform is defamed by MSS (Microprocessor Software Specification) file which defines driver and library customization parameters for peripherals, processor customization parameters, standard 110 devices, interrupt handler routines, and other software related routines. The MSS file is an input to the Library Generator tool for customization of drivers, libraries and interrupts handlers.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

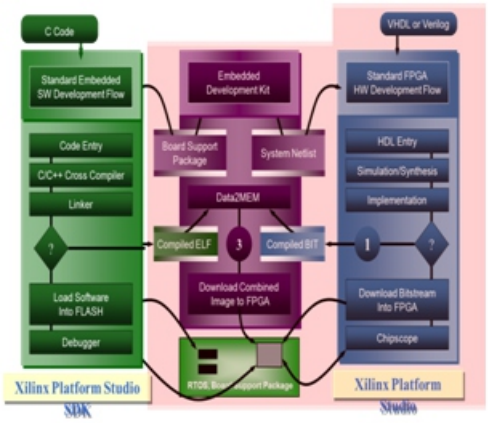

Fig7: Embedded Development Kit Design Flow

The creation of the verification platform is optional and is based on the hardware platform. The MHS file is taken as an input by the Simgen tool to create simulation files for a specific simulator. Three types of simulation models can be generated by the Simgen tool: behavioral, structural and timing models. Some other useful tools available in EDK are Platform Studio which provides the GUI for creating the MHS and MSS files. Create / Import IP Wizard which allows the creation of the designer's own peripheral and import them into EDK projects. Platform Generator customizes and generates the processor system in the form of hardware netlists.

Library Generator tool configures libraries, device drivers, file systems and interrupt handlers for embedded processor system. Bit stream Initializer tool initializes the instruction memory of processors on the FPGA shown in figure2. GNU Compiler tools are used for compiling and linking application executables for each processor in the system [6]. There are two options available for debugging the application created using EDK namely: Xilinx Microprocessor Debug (XMD) for debugging the application software using a Microprocessor Debug Module (MDM) in the embedded processor system, and Software Debugger that invokes the software debugger corresponding to the compiler being used for the processor.

C. Software Development Kit Xilinx Platform Studio Software Development Kit (SDK) is an integrated development environment, complimentary to XPS, that is used for C/C++ embedded software application creation and verification. SDK is built on the Eclipse open source framework. Soft Development Kit (SDK) is a suite of tools that enables you to design a software application for selected Soft IP Cores in the Xilinx Embedded Development Kit (EDK).The software application can be written in a "C or C++" then the complete embedded processor system for user application will be completed, else debug & download the bit file into FPGA. Then FPGA behaves like processor implemented on it in a Xilinx Field Programmable Gate Array (FPGA) device.

Results:

Fig8: Headerfile creation

Fig9: Cover Image

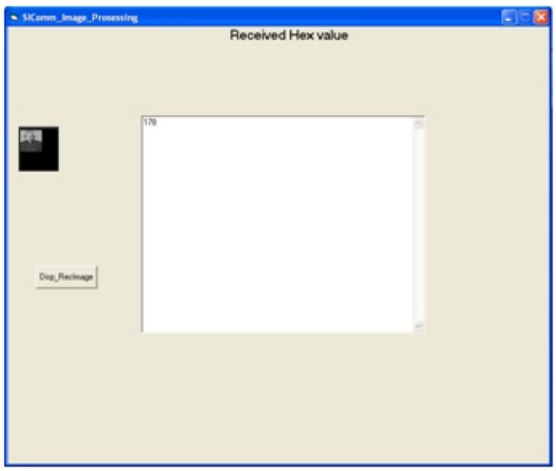

Fig10: Lifting Image

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

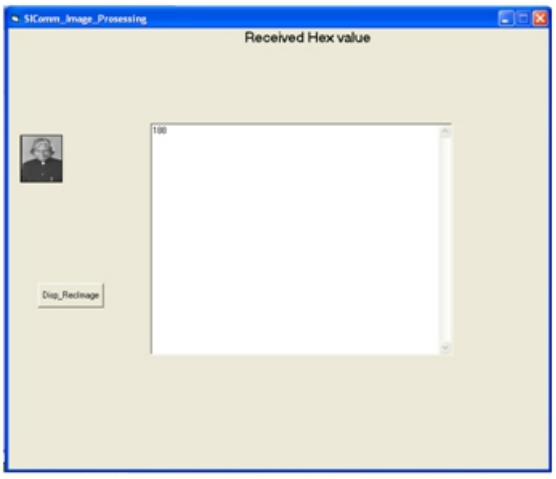

Fig11: Decompressed Cover Image.

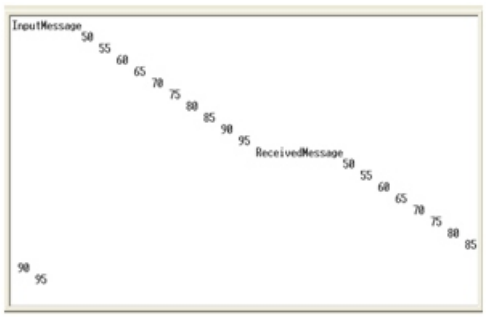

Fig12: Secret Image Data.

```
Selected Device : 3s500efg320-4

 Number of Slices:                2649  out of   4656   56%
 Number of Slice Flip Flops:      3343  out of   9312   35%
 Number of 4 input LUTs:          3794  out of   9312   40%
    Number used as logic:         3118
    Number used as Shift registers:  356
    Number used as RAMs:             320
 Number of IOs:                     83
 Number of bonded IOBs:             40  out of    232   17%
    IOB Flip Flops:                 55
 Number of BRAMs:                    7  out of     20   35%
 Number of MULT18X18SIOs:            3  out of     20   15%
 Number of GCLKs:                    7  out of     24   29%
 Number of DCMs:                     2  out of      4   50%

Timing Summary:
---------------
Speed Grade: -4

   Minimum period: 12.384ns (Maximum Frequency: 80.749MHz)
   Minimum input arrival time before clock: 41.553ns
   Maximum output required time after clock: 13.840ns
   Maximum combinational path delay: 3.344ns
```

Fig13: Synthesis report

Conclusion:

In this Paper the high speed low power invisible watermarking technique is implemented by using discrete wavelet transform technique to the secret image to get the better results. The hardware implementation of this digital watermarking could be significant in the copyright networks for the processing of the secret network based images.

The related work for this implementation could be recognized over the processing of this LSB technique for the tamper proofing also.

REFERENCES:

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.

[4] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in Proc. SPIE, Media Forensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.

[5] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar. 2006.

[6] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in Proc. Int. Workshop on Multimedia and Security, 2001, pp. 27–30.

[7] A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.

[9] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., ol. 13, no. 5, pp. 285–287, May 2006.

[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[11] W. Hong, T. S. Chen, and C. W. Shiu, "A minimal Euclidean distance searching technique for Sudoku steganography," in Proc. Int. Symp. Information Science and Engineering, 2008, vol. 1, pp. 515–518.

[12] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[13] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," Signal Process., vol. 90, no. 11, pp. 2954–2964, 2010.

[14] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus onedata embedding scheme," IEEE Signal Process. Lett., vol. 14, no. 11,pp. 848–851, Nov. 2007.

[15] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing onwet paper," IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp.3923–3935, Oct. 2005.

[16] J. Fridrich and T. Filler, "Practical methods for minimizing embeddingimpact in steganography," in Proc. SPIE, Security, Steganography.,Watermarking of Multimedia, 2007, vol. 6050, pp. 2–3.