International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 3 (May-June 2014), PP. 80-83

LSB & DWT BASED DIGITAL WATERMARKING SYSTEM FOR VIDEO AUTHENTICATION.

Prof. R.V.Babar, Mr. Akshay. A.Jadhav
Dept of Electronics and Telecommunication Engineering
STES's Sinhgad Institute of Technology, Lonavala,
University Of Pune, India.

***Abstract*— Nowadays, digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking. Embedding a hidden stream of bits in a file is called Digital Watermarking. This paper introduces a LSB information hiding algorithm which can lift the wavelet transform image. LSB based Steganography embeds the hiding text message in least significant bit of the pixels. The proposed method has good invisibility, robustness for a lot of hidden attacks. As we think about the capacity lead us to think about improved approach which can be achieved through hardware implementation system by using Field Programmable Gate Array (FPGA). In this paper hardware implementation of digital watermarking system is proposed. MATLAB is used to convert images into pixel-format files and to observe simulation results. To implement this paper XPS & VB are needed. In XPS, first select hardware & software components then by adding source and header files & converting into bit streams and download into FPGA, to obtain Stego image.**

***Index Terms*— Steganography, Wavelets Transform, XPS, GUI and FPGA.**

I. INTRODUCTION

In the digitized world extensive increase of use of extensive data communication the problem of security, authentication of the multimedia data also increases. The solution to this is digital watermarking. Digital watermarking is the process of the modification of original multimedia data to embed a watermark containing key information such as authentication or copyright codes. The embedded data must leave original data unchanged. Steganography is an art of hiding information in a way that apart from an intended recipient, suspects the existence of secret message. Steganography derived from Greek meaning is that "Covered writing." Three types of Steganography are there as follows

1) Physical Steganography
2) Digital Steganography
3) Printed Steganography.

Here we are using Digital Steganography means In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

II. Methods Of Hiding The Data In To The Digital Image

A. Least Significant Bit (LSB)

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1.The LSB based Steganography is one of the Steganography methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

240 011110000

RESULT: (00100110 11101001 11001001)

(00100111 11001001 11101000)

(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed.

B. Watermarking In The Frequency Domain

For better imperceptibility as well as robustness, the insertion of the watermark is done in a frequency domain. Many transform formats are available; mainly DCT and DWT are widely used. In this technique –frequency domain- the watermark actually spread throughout the image, not just operating on an individual pixel. The schemes for embedding the watermark in the transform domain are also called the multiplicative embedding rule, which can be denoted by:

$$X'i = Xi\ (1 + \gamma Wi) \quad (2)$$

Where: X'and X stand for the watermarked-image and the

Base-image, respectively, W denotes the watermark I represent the positions to be embedded, and γ is the gain factor (weight). Wavelet-based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. The wavelet transform is closer to the human visual system since it splits the input image into several frequency bands that can be processed independently. Its amulti-resolution transforms that permits to locate image features such as smooth areas, edges or textured areas. Here is wavelet-based watermarking algorithm to illustrate the basic idea of embedding and extraction of a watermark into a digital image:

1) Reorganize color and size of the base-image to be [M×M] Gray color.
2) Compute 2D wavelet transform for the base-image.
3) Initiate the weight of the watermarking.
4) Reorganize size and color of the watermark to be [M×M] Gray image.
5) Divide the transformed base-image into 4-blocks,namely, LL, LH, HL and HH respectively.
6) Multiply watermark by watermarking weight and then add The result to the blocks of the base-image.
7) The inverse wavelet transform is then taken to get the Watermarked-image.

On the other hand the extraction algorithm can be done by taking the forward wavelet transform of the watermarked image and then subtracted it from the base-image to get the watermark.

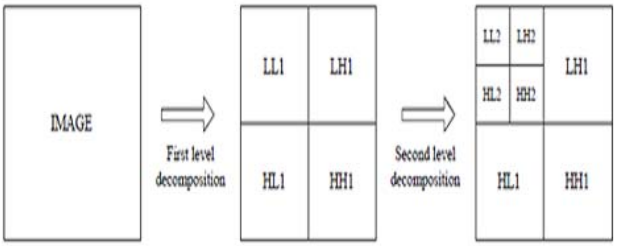

Fig 1.Wavelate Decomposition.

III. HARDWARE IMPLEMENTATION PROCESS

The implementation steps of the LSB and DWT based digital watermarking is done as follows. MATLAB is used to convert input images into header files using GUI feature. Xilinx Platform Studio(XPS) is a part of an EDK system and it includes the XPSGUI and all tools run by the GUI to process hardware & software components within XPS. FPGA hardware is chosen because of it has some advantages like reconfigurability, low power dissipation, small size. Fig.2 shows the flowchart for the implementation of using wavelet transform &LSB. The process is done as per below.

Step 1:First Select the Hardware configuration like processor,IO peripherals etc. The HDL codes are generated automatically for the each specified hardware selection and then convert it into bit streams.

Step 2: After that the selection of software architecture is started. It selects drivers, libraries etc. the header files of input Images and source file (which consist of DWT, compression and IDWT code written in the system-C language) are added and convert it into bit stream.

Step 3: Then download hardware and software architecture bit streams into FPGA and run it. The image output can't be Shown in FPGA. For this purpose Visual Basic is used to Observe the fused image output.

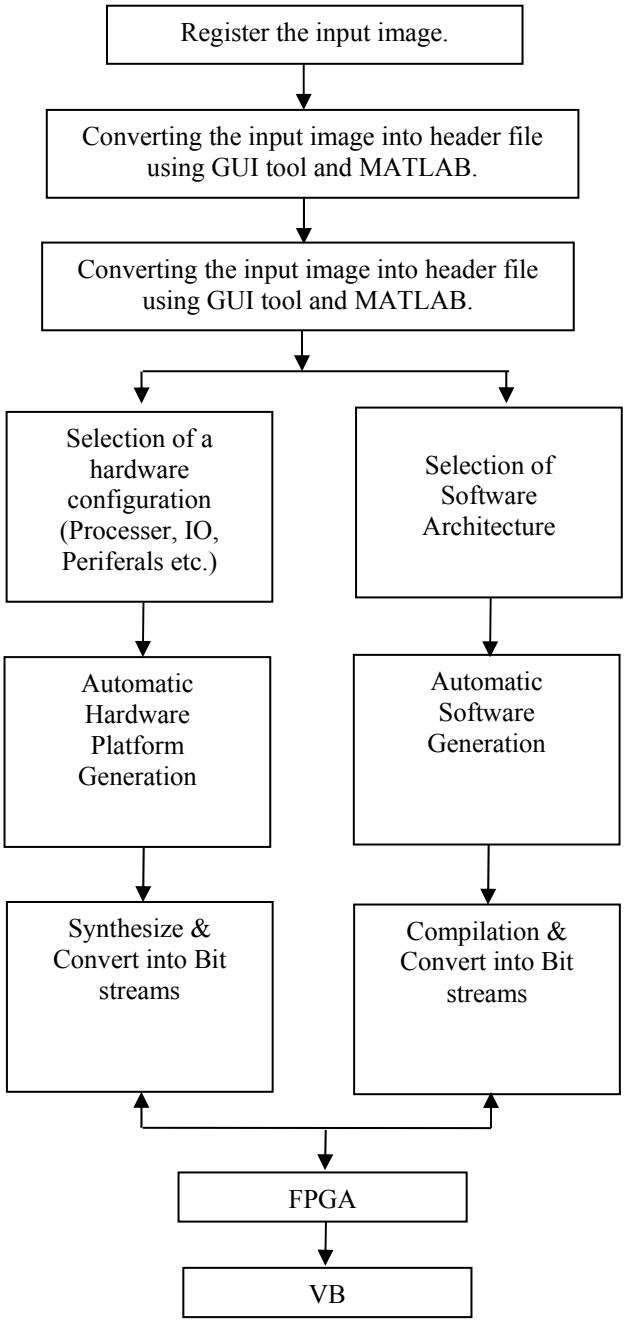

Fig 2 . Flow Chart of FPGA Implementation.

IV. SIMULATION RESULTS

The cameraman image shown in fig 3 is the input image. [256×256] dimensional matrix is represented as input image, which is a gray scale image. The cameraman image converted into the header files(text file contains the pixel values.). In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. In this case MCK image shown in Fig 4 used as secret image. The discrete wavelet transformed output of secret image shown in Fig 6 will embed in to DWT output part of the cameraman image shows in fig 5. The DWT filter uses high pass and low pass filter to decompose the image into its detail and approximate information respectively. 2D-DWT is applied on grayscale image which is shown in figure 7 and 8.It transforms an image into sub-bands such that the wavelet coefficients in the lower level sub-bands typically contain more energy than those in higher level sub bands. It can be accomplished by applying one-dimensional DWT filter in a separable manner. The first stage of the DWT divides an image into four sub-bands by applying low-pass and high pass filters. The first level of decomposition is consists of two steps. In the first step, each row of an image is transformed using a 1D vertical analysis filter bank. The first step is shown in figure 1. In the second step of the first level of decomposition, each column of the transformed image is again transformed using same filter bank horizontally. The second step is shown in figure 1. Each row and column of the lowest sub-band has been replaced by 1D-DWT. The result of the second level of decomposition has been shown in figure 5 and 6.The discrete wavelet transformed output of secret MCK image and that DWT output of Secret image shown in Fig 6 will embed in to DWT output part of the cameraman image shown in Fig 5.

Fig3. Input cameramen image

Fig 4. Secret image.

Fig 5. DWT of cameramen image.

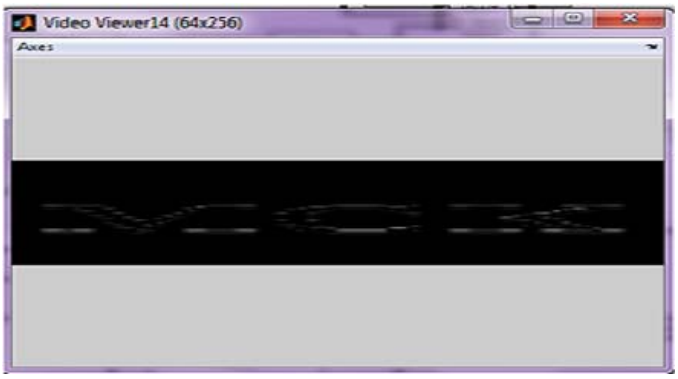

Fig 6. DWT of Secret image.

Fig 7. Watermarked Image.

Fig 8 . Recovered Secret Image.

Fig 9. Recovered input image.

The fig 7, 8, 9 will shows the watermarked image, recovered Secret image, recovered input image.

CONCLUSION

In this Paper, low power high speed and area efficient DWT & LSB based Image robust watermarking technique for color and gray scale images was performed. The RGB image is converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using invisible watermarking algorithm. Here the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately. Checking the watermark insertion and quality analysis various parameters like PSNR, Cross correlation etc.

REFERENCES

[1] P. Phanindra, J. Chinna Babu, V. Usha Shree, VLSI implementation of Medical Image Fusion Using Haar Transform , International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 ISSN 2229-5518.

[2] Anumol T J, Binson V A,. Asst.Prof.AEI Dept Saintgits college of engineering Kottayam, Soumya Rasheed Asst.Prof.ECE Dept Ilahia college of engineering Muvattupuzha, FPGA Implementation of Low Power, High Speed, Area Efficient Invisible Image Watermarking Algorithm for Images, international journal of scientific & engineering research volume 4, issue 8, august-2013 ISSN 2229-5518.

[3] Dr. Ekta Walia , Payal Jain, Navdeep. An Analysis of LSB & DCT based Steganography. Global Journal of Computer Science and Technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[4] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish,Member, IEEE,and Orly Yadid-Pecht,Fellow, IEEE, Hardware Implementation of a Digital Watermarking System for Video Authentication, IEEE transactions on circuits and systems for video technology, vol. 23, no. 2, february 2013.

[5] Mohammad Imroze Khan, Samiksha Soni, Bibhudendra Acharya, and Shrish Verma, Department of Electronics & Telecommunication, National Institute of Technology Raipur, Chhattisgarh, India. IMPLEMENT ATION OF DIGITAL WATERMARKING USING VHDL, IJCSC Vol. 3, No. 1, January-June 2012, pp. 15-21, ISSN : 0973-7391.