RESEARCH ARTICLE OPEN ACCESS

FPGA Implementation of Digital Watermarking Using Integer Wavelet Transform and AES Techniques

[1]K. Deepika, [2]Sudha M. S., [3]Sandhya Rani M.H
1PG student, 2Assistant Professor, 3HOD
[1, 2, 3] Department of Electronics and Communication
[1, 2, 3]Sapthagiri College of Engineering Bangalore-560057.

Abstract:

A digital watermarking scheme based on integer wavelet transform and histogram techniques is proposed in this paper. Lifting scheme based integer wavelet transform is used to provide ease of transformation of compressed data and to increase the data embedding capacity. Also histogram technique which is one of the reversible data hiding is used to embed the secret data into original image and retrieve the original data back after extraction. The AES encryption is used to encrypt the embedded image to provide authentication. This algorithm is developed using verilog code and implemented on FPGA Artix 7 board in order to increase throughput, reduce area and power consumption.

Keywords — **Watermarking, IWT, Histogram, AES**

I. INTRODUCTION

The rapid development in information technology and communication systems has increased the use of digital data and its application over internet or through some other media. To prevent illegal copy or claims the ownership of digital media and to protect data from being tampered from unauthorized users digital image authentication is required. In order to authenticate digital image a number of authentication techniques were developed. They are broadly classified into Data hiding- based and Cryptography based Digital image authentication techniques. Some other authentication techniques are OTP, Biometric, digital signature etc. One of such technique is watermarking technique.

Watermarking is a process of embedding an visible or invisible image, data or signature inside an image to show authenticity or proof of ownership. The hidden watermark should be inseparable from the host image, robust enough to resist any manipulations while preserving the image quality. Thus through watermarking, intellectual properties remains accessible while being permanently marked. Watermarking adds the additional requirement of robustness. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. There are four essential factors which make watermarking effective. The first one is robustness which is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, collision attacks, resizing, cropping etc. Second is imperceptibility i.e quality of host image should not be destroyed by presence of watermark. Third is capacity which includes techniques that make it possible to embed majority of information. Lastly blind watermarking Extraction of watermark from watermark image without original image. Watermarking can be classified based on perceptually as visible and invisible watermarking, based on application as robust and fragile watermarking and based on level of information required to detect the embedded data as blind, semi-blind and non blind watermark. Integrity refers to originality of transmitted image. In this paper, a description of IWT and Histogram embedding technique is discussed.

II. RELATED WORK

In this section Kaushik Deb et al. [1] proposed a joint DWT-DCT based watermarking technique for avoiding unauthorized replication. Low frequency band of each DCT block of selected DWT sub-band is used to embed watermark bit. Imperceptibility is improved by weighted correction. The watermark is extracted by reversing the embedding operations without an original image.

Sumalatha Lingamgunta et al. [2] proposed reversible watermarking for image authentication using IWT which hides data and the bookkeeping information in the high frequency subbands of CDF(2,2) integer wavelet coefficients whose magnitude are similar to predefined threshold. Parent child structure of the transformed coefficients called "quadruple wavelet tree" is used as embedding technique.

Anjana Joshy et al. [3] proposed a dual security approach for image watermarking using AES and DWT. In this, two watermarks were embedded in the host image for authentication and tamper detection. UC as first robust watermark was used which was then embedded using the 2-level DWT. For tamper detection hash code of host image was calculated and was used as secondary watermark.

Deepa M. et al. [4] proposed separable encrypted colour image watermarking using VLSI, where visible logo is embedded using curvelet transform. The three secret images are then embedded in RGB planes. Then encryption key is used to encrypt the embedded image. The least significant bits are compressed using image hiding key to create a sparse space to accommodate the secret binary image image.

Ashwini B. M. et al. [13] in their paper implemented Encrypted Visual Cryptographic Shares using RSA Algorithm on FPGA, which combined advantages of both visual cryptography and public key cryptography and therefore enhances the security of VC shares by encrypting with public key cryptography i.e secret information in form of printed text, images and hand written material is transferred with strong security.

Abdullah Bamatraf et al. [12] proposed digital watermarking algorithm using combination of least significant bit and inverse bit to improve quality of watermarked image. In this, before embedding the watermark the algorithm uses LSB by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates.

III. EMBEDDING ALGORITHM BASED ON INTEGER WAVELET TRANSFORM

In the proposed system, a reversible watermarking technique based on Lifting scheme integer wavelet transform is used to embed data in the high frequency sub bands such as HH, HL and LH since human eyes are less sensitive to these regions. Hiding information in these regions make the design more robust and helps to maintain the visual quality of the image. Integer wavelet transform maps integer data set into another integer data set and hence there will no loss of information as in case of DWT where in it has floating point coefficients. Histogram is graphical representation of an image. It represents pixel value and density at a particular pixel. Using histogram the secret data is embedded into the original image. Histogram yields highest point and lowest point depending on which we embed the data. Advanced encryption standard(AES) is one of the strongest encryption method used to encrypt the information to maintain privacy of data.

A. Encryption Algorithm

Step1: The input is a gray scale image of any size

Step 2: Integer wavelet transform is applied to the input image which decompose image into different sub-band frequencies.

Step 3: IWT is calculated by equations given below:

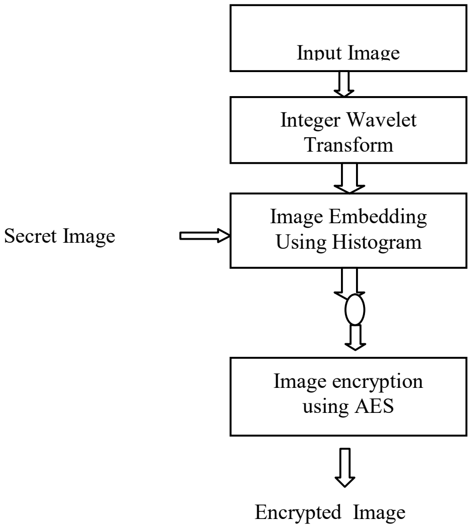

Input Image
Integer Wavelet Transform
Secret Image
Image Embedding Using Histogram
Image encryption using AES
Encrypted Image

Fig 1: Encryption Algorithm

$$d_{l.\ n}=S_{0.2n+1}-S_{0.2n}$$

$$S_{I.\ n=}0.2n+(d1, n/2)$$

Step 4: Next embed secret image into the output of IWT using histogram modification technique to get watermarked image.

Step 5: Finally AES encryption is applied to watermarked image.

B. Decryption Algorithm

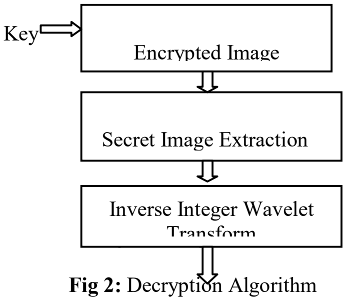


Fig 2: Decryption Algorithm

Step 1: Encryped Image is obtained
Step 2: Reverse AES is applied using the same key as used at the receiver side to obtain the decrypted image.
Step 3: Apply reverse histogram method to separate secret image and compressed image
Step 3:Then inverse IWT is applied to obtain original image, the inverse IWT is calculated by

$$S_{0.2,\,n}=S_{1,n}-(d1,\, n/2)$$
$$S_{0.2n+1}=d_{l,n}+S_{0.2n}$$

C. Histogram Algorithm

Consider an input image of MXN. grayscale value of each pixel x ranges between 0 to 255.
Step 1: Generate Histogram of input image.
Step 2: In the histogram, find the peak point.
Step 3: Set all the pixel values below the peak point to '0' and move the histogram after peak point by '1' unit.
Step 4: Again scan the input image, once peak point is reached check to be embedded bit. If it is one the grayscale value of pixel is shifted by 1 unit to right else remains intact.

D. Reverse Histogram Algorithm

Step1: The watermarked image is scanned, if a pixel with grayscale value shifted by 1 is found then '1' is extracted else '0' is extracted.
Step 2: The histogram is shifted back.
Step 3: Finally we get original image.

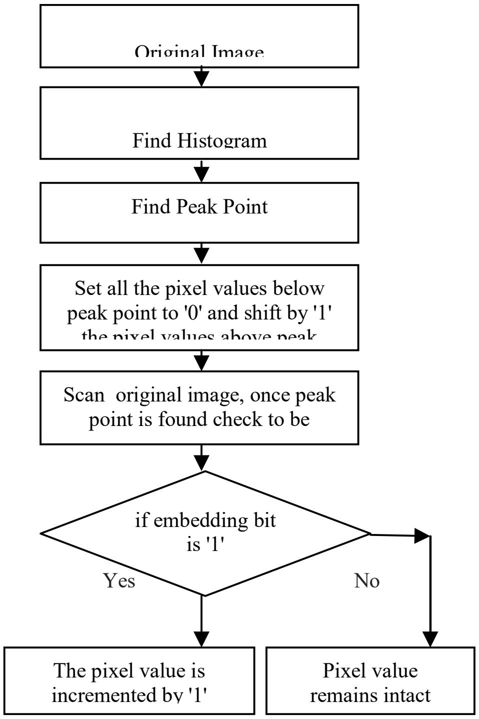

Original Image
Find Histogram
Find Peak Point
Set all the pixel values below peak point to '0' and shift by '1' the pixel values above peak
Scan original image, once peak point is found check to be
if embedding bit is '1'
Yes
No
The pixel value is incremented by '1'
Pixel value remains intact

Fig 3: Histogram Algorithm

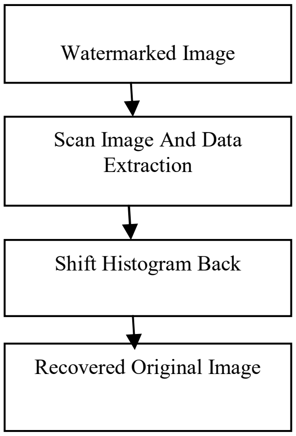


Fig 4: Extraction Algorithm

E. Advanced Encryption Standard

AES describes Rijndael algorithm which is a symmetric cipherblock used to process a block of 128 bit data using cipher key key length of 128, 198 and 256 bits. The initial process consists of add round key followed four steps: They are substitute byte, shift rows, mix columns and add round key. In the proposed method the key length of 128 bit is used. Hence the four steps are repeated for 10 times, where in, in the tenth round the mix column step is not performed. The decryption is performed by reversing the encryption process. The AES encryption algorithm is shown in the figure below:

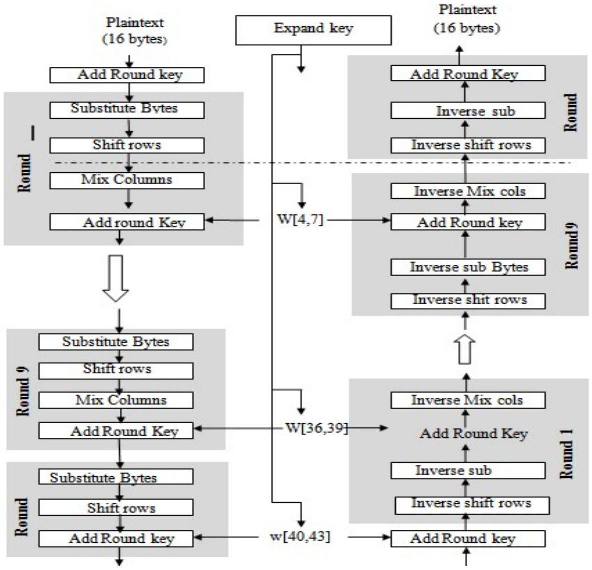


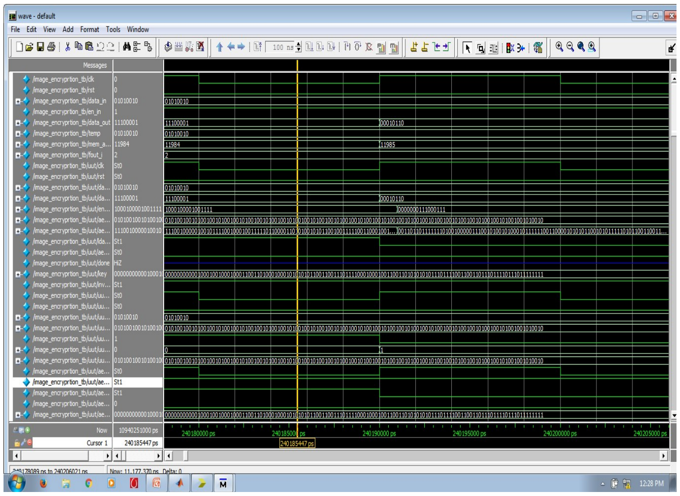
Fig 5: AES Algorithm

IV. EXPERIMENTAL RESULTS

The design was implemented on FPGA Artix 7 board using Xilinx 14.7 software. The simulation results are shown below.

A. Simulation Output

Figure shows the simulation output of encrypted image in which secret image in binary form is embedded into original image.



```
/image_encryprtion_tb/clk          0
/image_encryprtion_tb/rst          0
/image_encryprtion_tb/data_in      01010010
/image_encryprtion_tb/en_in        1
/image_encryprtion_tb/data_out     11100001
/image_encryprtion_tb/temp         01010010
/image_encryprtion_tb/mem_a...     11984
/image_encryprtion_tb/fout_i       2
/image_encryprtion_tb/uut/clk      St0
/image_encryprtion_tb/uut/rst      St0
/image_encryprtion_tb/uut/da...    01010010
/image_encryprtion_tb/uut/da...    11100001
/image_encryprtion_tb/uut/en...    1000100001001111
/image_encryprtion_tb/uut/ae...    010100100101001001
/image_encryprtion_tb/uut/ae...    111001000001001011
/image_encryprtion_tb/uut/lda...   St1
/image_encryprtion_tb/uut/ae...    St0
/image_encryprtion_tb/uut/done     HiZ
/image_encryprtion_tb/uut/key      000000000001000100
/image_encryprtion_tb/uut/inv...   St1
/image_encryprtion_tb/uut/uu...    St0
/image_encryprtion_tb/uut/uu...    St0
/image_encryprtion_tb/uut/uu...    01010010
/image_encryprtion_tb/uut/uu...    010100100101001001
/image_encryprtion_tb/uut/uu...    1
/image_encryprtion_tb/uut/uu...    0
/image_encryprtion_tb/uut/uu...    010100100101001001
/image_encryprtion_tb/uut/ae...    St0
/image_encryprtion_tb/uut/ae...    St1
/image_encryprtion_tb/uut/ae...    St1
/image_encryprtion_tb/uut/ae...    0
/image_encryprtion_tb/uut/ae...    000000000001000100
Now        10940251000 ps    240180000 ps    240185000 ps
Cursor 1   240185447 ps      240185447 ps
240178089 ps to 240206021 ps     Now: 11,177,370 ns  Delta: 0
```

Fig 6: Simulation Output

B. Output Image

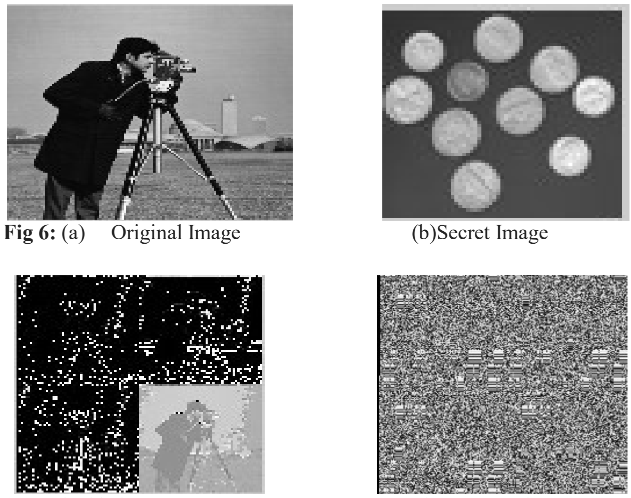
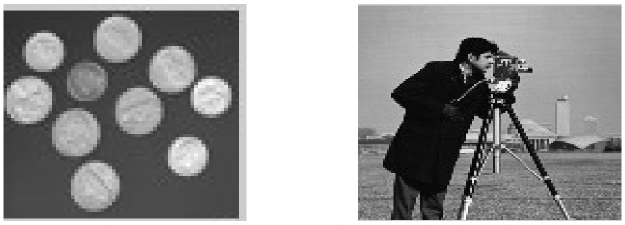


Fig 6: (a) Original Image (b)Secret Image

(c) Embedded Image In IWT Output (d) Decrypted Image



(e)Extracted Secret Image (f)Extracted Original Image

Figure 6 shows original image which is subjected to IWT and encrypted and vice versa the encrypted image is decrypted, secret image is extracted from original image and inverse IWT is applied to obtain original image.

The performance parameter for different images were calculated and compared with previous work to prove the efficiency of implemented image as shown in table 1. The design was implemented on FPGA Artix 7 board producing throughput of 343.5 MHz which is good throughput.

TABLE I
COMPARISION BETWEEN PROPOSED and PREVIOUS WORK for DIFFERENT IMAGES WITH RESPECT TO PSNR

Images	PSNR of Previous Work	PSNR of proposed Work
Cameraman	29.72	34.2
Lena	22.17	36.78
Couple	28.79	31.78

V. CONCLUTION

In this paper the histogram modification method used to hide data into integer wavelet transfer coefficient is proposed. Histogram method increases the embedding capacity as compared to all other embedding algorithm. Moreover, this algorithm suits all types of images like gray scale, colour, real time and even biomedical images because of its reversible nature. In the proposed algorithm secret data bits are hidden in sequential order. Also the number of bits to be embedded depends upon number of pixels associated with the peak point without effecting the quality of image. AES algorithm is used to maintain the privacy of embedded data. The experimental results showed that algorithm yields better PSNR ratio.

ACKNOWLEDGEMENT

We would like to thank our college management who patronized throughout our career and for the facilities provided to carry out this work successfully. We would also like to thank our teaching and non-teaching staff members who have helped us directly or indirectly.

REFERENCES

[1] Kaushik Deb, Md. Sajib Al-Seraj, Mir Md. Saki Kowsar and Iqbal Hasan Sarkar, "A Joint DWT-DCT Based Watermarking Technique for Avoiding Unauthorized Replication," 7th International Forum on Strategic Technologies, pp.1-5, IEEE, 18-21 September 2012.

[2] Sumalatha Lingamgunta, Venkata Krishna Vakulabaranam and Sushma Thotakura, " Reversible Watermarking for Image Authentication using IWT", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 6, No. 1, February 2013.

[3] Anjana Joshy and Neenu Suresh, "A Dual Security Approach for Image Watermarking using AES and DWT," International Journal of Digital Application & Contemporary research, vol. 3, Issue 1, August 2014.