High Speed DCT Based Image Steganography Implementation on FPGA

Rajeesh U. R
Department of Electronics & Communication Engineering
Rajagiri School of Engineering & Technology
Kochi, India

Rooha Razmid Ahamed, Asst.Professor
Department of Electronics & Communication Engineering
Rajagiri School of Engineering & Technology
Kochi, India

***Abstract*— FPGA implementation of a high-speed DCT architecture which is appropriate for digital image steganography. The architecture contain a digital clock manager (DCM) which is present inside modern field-programmable gate arrays (FPGA) for generating the sub clocks with increasing or decreasing frequency from the system clock. The DCM is used for generating a sub clock having frequency 8 times that of system clock. This sub clocks are used to drive the Discrete cosine transform (DCT) block. The proposed architecture uses only 5 adders and 4 multipliers for implementing DCT which have a throughput of 8 pixels per clock. The proposed design is coded in Verilog HDL. Xilinx ISE 14.1 is used to simulate and synthesis the design on Spartan-3 FPGA.**

Keywords*— *Steganography; DCT; DCM; FPGA.

I. INTRODUCTION

Steganography comes from the Greek words Steganos (Covered) and Graptos (Writing). Steganography is the art and science of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. There are lot of algorithms available for encrypting secret information such as DES (Data Encryption Standard) [1], AES (Advanced Encryption Standard) [2] and RSA [3]. The data encrypted in these ways are not in understandable format, so hackers can easily understand that these are secret data. Here comes the need of steganography. Here the secret data is embedded into a cover data without modifying the appearance of cover data, so that it cannot be observed.

In digital image steganography, secret image is embedded into another digital cover image to produce the modified cover image named stego image. The cover image is modified in such a way, with minimum distortion as possible.

Many steganography algorithms are presented in recent years. Out of these methods, substitution systems and transform domain techniques are most commonly used techniques now a days. In substitution system such as Least Significant Bit (LSB) method, the cover image pixel bit values are modified for embedding the secret information. In LSB steganography the cover image pixel's LSB bits are replaced with secret data bits for hiding secret information. So they are very simple in processing, fast and easy to implement. At the same time, the size of secret information carried depends on the size of cover image used. These can be increased by increasing the number of bits replaced in cover image by secret data, but this will affect the originality of image and results low peak signal-to-noise ratio (PSNR). Also it is easy to decode the secret data from stego image and due to this lack of secrecy, the substitution systems are not used widely.

The transformation domain techniques are other kind of steganography method, where cover image is converted into frequency domain for embedding secret information. These have the advantage of high PSNR and secrecy compared to other methods. There are several power level transformation methods to convert an image into frequency domain. Some of them are Discrete Fourier transformation technique (DFT), Discrete cosine transformation technique (DCT), Discrete Wavelet transformation technique (DWT). Each approach has its advantages and disadvantages. DWT based steganography methods enable good spatial localization and have multi resolution characteristics. Also, it shows robustness to low pass and median filtering. However, it is not robust to geometric transformations. The DFT approach has one disadvantage that, it introduces round-off errors, which can lead to loss of image quality and cause errors in the time of extraction.

DCT is the most widely used technique in JPEG image compression. DCT method have higher compression ratios and secrecy. Most DCT hardwares are implementations using distributed arithmetic architectures. But they require large size of ROM and large number of multipliers. This paper focuses on reducing the number of adders and multipliers because they consume most of the area in DCT hardware. Different type of DCT architectures have been proposed in recent years to reduce number of multipliers. Among these, Loeffler [4] proposed a DCT algorithm having 11 multipliers and 29 adders. But when compared to Loeffler the proposed DCT hardware uses only 4 multipliers and 5 adders. Also these are optimized to realize a low power and fast processing DCT architecture. High-Performance multiplier (RPM) and carry select adder are being used as multipliers and adders respectively.

The DCM block is present in most of the modern FPGAs. This is used to multiply or divide the clock. Here the application of DCM is generating a sub clock having frequency 8 times that of system clock, which speed up the overall DCT system. By using this, the architecture have a throughput of 8 pixels per clock.

The paper is organized as follows: The theory of DCT present in section II. Section III discuses the proposed hardware architecture of DCT block and steganography implementation. Implementation details and simulated results are illustrated in the section IV. Finally, section V presents concluding remarks.

II. DISCRETE COSINE TRANSFORMATION

The Discrete Cosine Transform was introduced by Ahmed et al [5] in 1974. The DCT convert a signal into corresponding elementary frequency components, in which image pixels are represented as the sum of sinusoids of varying magnitudes and frequencies. This transform has found wide applications in image processing, data compression, filtering, and other fields. For an input image x, the transformed DCT output image X is given by (1) as shown below. Where x is the input image having N pixels, x(k) is the intensity of pixel of the image and X(k) is the DCT coefficient.

$$X(n) = c_n \sum_{k=0}^{N-1} \cos \frac{2\pi n(2k+1)}{4N} x(k) \qquad (1)$$

$$For\ 0 \leq n \leq N-1$$

Where,

$$C_0 = {}^{1}/_{\sqrt{N}} \qquad for \quad n = 0$$

$$C_n = {}^{2}/_{\sqrt{N}} \qquad for \quad 1 \leq n \leq N-1$$

And the inverse DCT is given by,

$$x(k) = \sum_{n=0}^{N-1} \cos \frac{2\pi n(2k+1)}{4N} c_n X(n) \qquad (2)$$

The DCT can also be calculated by multiplying DCT coefficient matrix and image pixel matrix together, which is given below (3).

$$\text{DCT = D.X} \qquad (3)$$

Where X is the image matrix and D is the DCT coefficient matrix. An 8x8 DCT matrix is given by,

$$\begin{matrix}
0.35 & 0.35 & 0.35 & 0.35 & 0.35 & 0.35 & 0.35 & 0.35 \\
0.49 & 0.41 & 0.27 & 0.09 & -0.09 & -0.27 & -0.41 & -0.49 \\
0.46 & 0.19 & -0.19 & -0.46 & -0.46 & -0.19 & 0.19 & 0.46 \\
0.41 & -0.09 & -0.49 & -0.27 & 0.27 & 0.49 & 0.09 & -0.41 \\
0.35 & -0.35 & -0.35 & 0.35 & 0.35 & -0.35 & -0.35 & 0.35 \\
0.27 & -0.49 & 0.09 & 0.41 & -0.41 & -0.09 & 0.49 & 0.27 \\
0.19 & -0.46 & 0.46 & -0.19 & -0.19 & 0.46 & -0.46 & 0.19 \\
0.09 & -0.27 & 0.41 & -0.49 & 0.49 & -0.41 & 0.27 & -0.09
\end{matrix}$$

And the inverse DCT is given by,

$$\text{IDCT = D'.DCT} \qquad (4)$$

III. THE PROPOSED SCHEME

In our DCT based image steganoraphy, we first extract the DCT of cover image and secret image using our proposed architecture. For hiding the secret information, algorithms are applied to these DCT coefficients of secret image. Here we are hiding the data by multiplying it with a constant β. This make the secret information invisible from outsiders by reducing it's intensity. Here the image is first divided into blocks of 8x8 matrix. Then DCT of each blocks are computed separately.

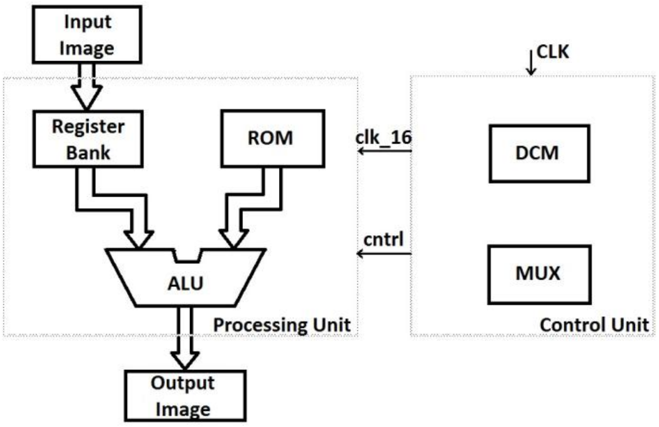

Fig. 1. System Architecture

The proposed system use only 5 adders and 4 multipliers. From DCT coefficient matrix, it can be seen that there are only maximum 4 values in a row, 2 values are repeating. So corresponding 2 values in the image columns can be added/ subtracted first and then it can be multiplied with the DCT coefficient matrix values to obtain the final DCT result.

There are only 7 fixed values in DCT coefficient matrix, and these values are repeating in each row with sign change. So it needs only 7 locations in ROM for storing these values. Also in every row, the first value and last value are equal, second value and second last value are equal and so on. So it can grouped into 4 groups having same values. Also the column values of the image matrix can be grouped into 4 groups in similar way. The sign of these values are then changed according to the sign of corresponding coefficient matrix row values, with the help of multiplexer in control unit. These image matrix values in each group are added together using first 4 adders.

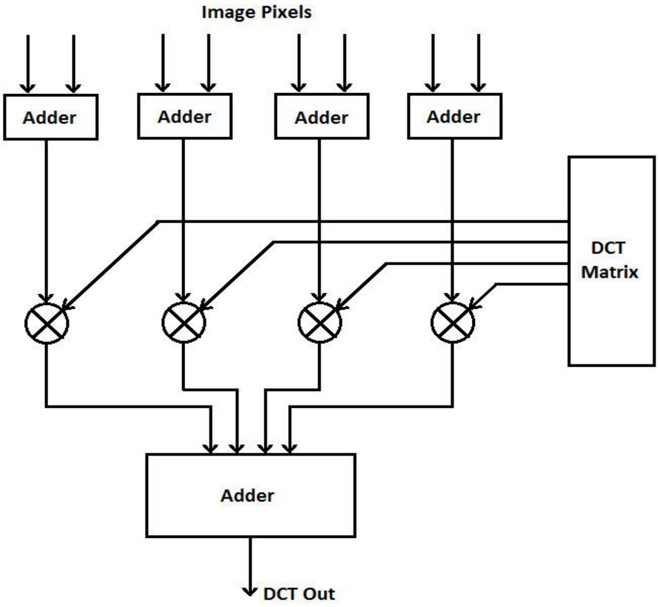

Fig. 2. Proposed DCT block

The results are then multiplied with DCT coefficients in order to perform matrix multiplication. The final adder add all these values together to form the DCT result. The DCM block in the control unit generate a sub clock having frequency of 8 x system clock, hence it outputs 8 pixels per system clock or have a throughput of 8 pixels per clock. Which thereby, reduces the processing time.

After computing the DCT of both cover image and secret image, the DCT values of secret image is multiplied with a constant β in order to hide it. This reduces the intensity of secret image which depends on the value of β. Then this new secret data is embedded into cover image DCT.

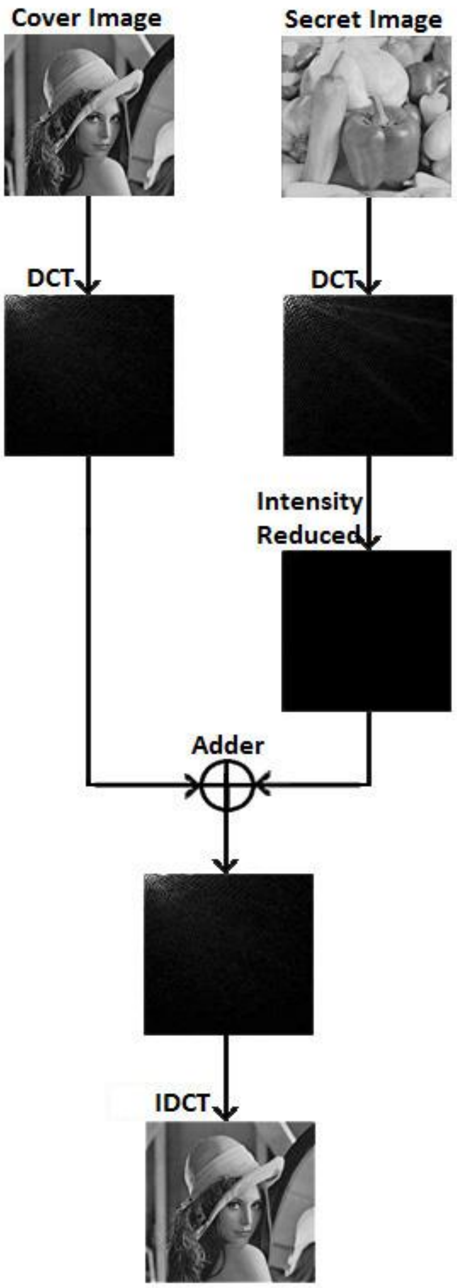

Fig. 3. Steganography flow diagram

A. Embedding Procedure

The steps of embedding secret image is as follows,

- Read the cover image.
- Splitting the cover image into blocks of 8 x 8 matrixes.
- Compute the DCT of each matrix.
- Read the secret image.
- Splitting the secret image into blocks of 8 x 8 matrixes.
- Compute the DCT of each matrix.
- Reduce the intensity of secret data by multiplying it with a constant β.
- Add DCTs of cover image and resultant secret data.
- Taking the IDCT gives the stego image.

B. Extraction Procedures

The steps of extracting secret image is as follows,

- Read the stego image.
- Splitting the stego image into blocks of 8 x 8 matrixes.
- Compute the DCT of each matrix.
- Read the original cover image.
- Splitting the cover image into blocks of 8 x 8 matrixes.
- Compute the DCT of each matrix.
- Subtract cover DCT from stego.
- Increase the intensity of resultant data by dividing it with a constant β.
- Taking the IDCT gives our initial secret image.

IV. SIMULATION AND RESULTS

The proposed architecture was modeled using verilog and simulated in Xilinx ISE 14.1. Images are converted into text file using MATLAB. These text files are used as inputs and outputs in verilog. The implementation was done and tested on a Xilinx Spartan 3 XC3s200 FPGA. The cover image and secret image used are lena image and peppers image having size of 80 x 80 pixels. It takes 1,600 clock cycles to complete the steganography. The stego image having a β value 0.01 is shown in fig.4. The secrecy will increase with lower values of β.

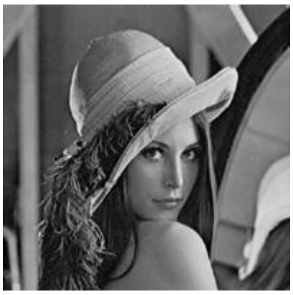

Fig. 4. Stego Image

The image metrics were computed for the produced stego image and are illustrated in table.1, which also lists the metrics of earlier methods. The results show that the proposed system has good PSNR and small error results.

TABLE I. COMPARISON OF IMAGE METRICS

Scheme	Size	Capacity	MSE	PSNR
LSB[6]	6400	800	6.0	40.3
HDWT[7]	6400	2432	28.5	33.58
DWT[8]	6400	1750	2.10	44.90
DCT	6400	6400	0.18	55.41

V. CONCLUSION

A new architecture is present in this paper to perform simultaneous compression and encryption. The modified DCT algorithm is an optimized model in terms of number of arithmetic operations which uses only 4 multipliers and 5 adders. The arithmetic operators used in DCT model are also optimized in order to increase the throughput and to decrease the power consumption. The FPGA implementation of this architecture shows improvement in terms of pixel throughput of 8 pixels per clock, area saving when compared to existing methods.

REFERENCES

[1] Akerkar, R. A.; Lingras, P. (2008). *An Intelligent Web: Theory and Practice*, 1st edn. Johns and Bartlett, Boston.

[2] Albert, R.; Jeong, H.; Barab´asi, A.-L. (1999): Diameter of the world-wide Web. Nature, **401**, pp. 130–131.

[3] Berry M. W., Dumais S. T., O'Brien G. W. (1995): Using linear algebra for intelligent information retrieval, SIAM Review, **37**, pp. 573-595.

[4] C. Loeffler and A. Lightenberg and G.S.Moschytz , "Practical fast I-D DCT algorithm with 11 multiplication", IEEE, ICAPSS, pp. 988-991, May 1989.

[5] N. Ahmed, T. Natarajan, and K. R. Rio, "Discrete Cosine Transform," IEEE Transactions on Computer, Vol. C-23, Jan. 1974, pp. 90-93.

[6] Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh and Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method," 978-1-4673-1550-0/12 ©2012 IEEE.

[7] B. Lai and L.Chang, "Adaptive Data Hiding for Images Based on Haar Discrete Wavelet transform," Lecture Notes in Computer Science, Vol 4319, 2006.

[8] P. Chen, H. Lin, "A DWT Based Approach for Image Steganography." International Journal of Applied Science and Engineering,Vol. 4, No. 3, pp. 275-290, 2006.