International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010
1793-8201

A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking

Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma

***Abstract*-- Data authentication and data security are the primary requisites in present day communication systems. In image processing, data authentication is implemented by using watermarking techniques. Nevertheless, whatever be the technique of watermarking, one of the important factors to be considered is robustness. In this paper we discuss about a novel robust method for digital watermarking in spatial domain. The method deals with an image in the spatial domain which is watermarked at different intensity subsections. Further, we have analyzed the performance of the proposed method by implementing the method using Verilog HDL & Matlab. A comparison of the proposed novel spatial domain method with the frequency domain method is also given here. We have implemented a frequency domain DCT/IDCT based digital watermarking as in [1] and [2]. We also compare the PSNR that can be obtained using the proposed spatial domain watermarking and the DCT/IDCT based watermarking.**

***Index Terms*—Watermarking, Spatial domain, Frequency domain, PSNR, Watermark.**

I. Introduction

Watermarking techniques can be broadly classified into two categories. They are spatial domain watermarking and frequency domain watermarking. Both have their own advantages and disadvantages. Majority of the present day watermarking techniques make use of the frequency domain. This is due to high robustness and ease of compression when compared to spatial domain. Frequency domain watermarking involves computation of the DCT/DWT of the pixel matrix of both the image as well as the watermark to be embedded on it. Then both the DCT/DWT coefficients are scaled and added. Finally the resulting DCT/DWT coefficients are subjected to IDCT/IDWT computation. Here we can observe that in frequency domain watermarking, lot of complex logic is involved.

Both DCT and DWT involve a lot of matrix multiplications and additions. This requires a large number of multipliers and adders. The power consumption in such a complex circuit will be humongous. Here we are proposing a novel method which involves watermarking in the spatial domain. In recent times spatial domain image watermarking is not much in use due to the low Peak Signal to Noise Ratio (PSNR) achieved by this method. But the method that we propose is different from the conventional spatial domain watermarking and has a PSNR comparable to that of frequency domain watermarking.

The first section of the paper brings a comparison of the two domains of digital image watermarking which are the frequency domain and the spatial domain. The next section is the novel robust method of watermarking that we suggest in the spatial domain. The next part of the paper depicts the implementation and the results which prove the proposed method to be robust. We have also included the watermarked images that were obtained by the proposed spatial domain watermarking technique and the PSNR that can be obtained using this method and the frequency domain watermarking method is compared for the same images. The standard 'Lena' and 'Cameraman' images are used as the base images for testing the proposed spatial domain watermarking technique.

Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma are with the Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, Kerala, India (email:.rajeshm@amritapuri.amrita.edu, mithun34@ieee.org, rahul44@ieee.org, enkatkrishnan.b@gmail.com, vineethisalways4u@gmail.com).

II. Motivation

The watermarking techniques in frequency domain that are used nowadays involve complex logic. Consequently, calculations are found to be rather tedious. Unlike conventional frequency domain computations, calculations in spatial domain are often simpler. Hence the referred spatial domain techniques could be used to implement a novel effortless watermarking technique.

III. Related Works

The watermarking techniques gained importance in information security after the Kerckhoff's Principle, Shannon's Approach and Diffie-Hellman's Terminology. These are the cryptanalytic approaches as in [6] and are based on three key articles: Kerckhoffs [7], Shannon [8], and Diffie-Hellman [9]. The watermarking has been done in many ways using a classical transform such as the discrete cosine transform (DCT), discrete wavelet transform (DWT), fast Fourier transform (FFT), Fourier Mellin etc. Apart from these methods the watermarking can be implemented in spatial domain also. Some common techniques are described in the following sections.

Kerckhoff's Principle: This principle gained significance because of the similarity of the Watermarking with Cryptography. In watermarking, it is assumed that the opponent knows the watermarking algorithm. Hence, for a given design and implementation of an algorithm, the security stems from the secrecy of the key.

Shannon's Approach: The methodology that Shannon exposed for studying the security of encryption schemes is here transposed to watermarking. The watermarking technique is perfectly secured if and only if no information about the secret key leaks from the observations. If it is not the case, the security level is defined as the number of observations that are needed to disclose the secret key. The bigger the information leakage is, the smaller the security level of the watermarking scheme will be.

Diffie-Hellman's Terminology: According to the context of the attack, the opponent may have access to several kinds of data. The opponent has at least access to watermarked content, but in some cases, he might also observe the hidden messages (for instance, the name of the author in copyright protection or the status of a movie in copy protection) or to the original data (for instance, imagine DVD movies are watermarked for copy protection; the original version of old movies were not protected). This implies that a security level is assessed for a given context.

Our earlier paper [2], discuss in detail, a pipelined hardware implementation of DCT/IDCT based watermarking scheme. The elementary motive of the scheme is aimed at increasing the speed of the system with a concurrent decrease in complexity. The requisite in amount of multipliers and adders comparitively decreased to 32 and 24 respectively. A conventional 2D DCT computing algorithm demands 64 and 56 multipliers and adders respectively. An 8x8 block of the concerned images were taken and added in frequency domain by applaying the wieghts as given below.

Resultant=.97*DCT(watermark)+.17DCT (parentimage)

Blockwise DCT was accomplished via series of steps. Steps are done as shown in Fig. 4. The foremost step is to calculate the row wise 1D DCT of a block of data as given by the equation.

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (4)$$

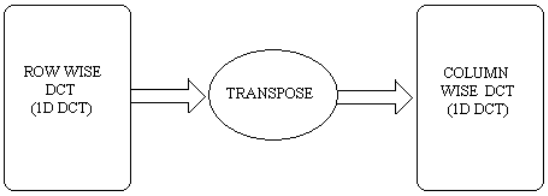

Figure 1. steps to compute 2D DCT

$$\begin{bmatrix} y0 \\ y1 \\ y2 \\ y3 \\ y4 \\ y5 \\ y6 \\ y7 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} c4 & c4 & c4 & c4 & c4 & c4 & c4 & c4 \\ c1 & c3 & c5 & c7 & -c7 & -c5 & -c3 & -c1 \\ c2 & c4 & c6 & -c2 & -c2 & -c6 & c6 & c2 \\ c3 & -c7 & -c1 & -c5 & -c5 & c1 & c7 & -c3 \\ c5 & -c1 & c7 & c3 & -c3 & -c7 & c1 & -c5 \\ c6 & -c2 & c2 & -c6 & -c6 & c2 & -c2 & c6 \\ c7 & -c5 & c3 & -c1 & c1 & -c3 & c5 & -c7 \end{bmatrix} \begin{bmatrix} x0 \\ x1 \\ x2 \\ x3 \\ x4 \\ x5 \\ x6 \\ x7 \end{bmatrix}$$

Figure 2. Matrix relation for 1D DCT

The equation can be easily replaced by the matrix relation shown in Fig.2 for eight element data vector

Where,

$$C(x) = \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (5)$$

The subsequent step is the computation of transpose of the resultant 1D DCT. The first step is repeated for the traspose too. The resulatant would be a 2D DCT.

After superimposing the parent and the watermark, IDCT of the image is estimated. The matrix relation for the IDCT is shown in figure 6

Correspnding values of x0,x1,x2…x7 are evaluated by solving the simultaneous linear equations obtained. Eg. x0+x7= o1 and x0-x7=o2, then x0 is given by (o1+o2)/2 and x7 is given by (o1-o2)/2.

The logic of the scheme was efficiently HDL coded so as to increase speed and decrease complexity. The image was the input data to the system. The pixels were extracted from the image using MATLAB. This was imported to HDL environment in the form of text file. The design flow is given in Fig. 4.

IV. Types Of Watermarking Schemes

The algorithms adopted for watermarking are as given below. Both frequency domain and spatial domain watermarking are discussed in detail.

$$\begin{bmatrix} x0+x7 \\ x1+x6 \\ x2+x5 \\ x3+x4 \\ x0-x7 \\ x1-x6 \\ x2-x5 \\ x3-x4 \end{bmatrix} = 2 \times \begin{bmatrix} y0 \\ y1 \\ y2 \\ y3 \\ y4 \\ y5 \\ y6 \\ y7 \end{bmatrix} \begin{bmatrix} c4 & c4 & c4 & c4 & 0 & 0 & 0 & 0 \\ c2 & c6 & -c6 & -c2 & 0 & 0 & 0 & 0 \\ c4 & -c4 & -c4 & c4 & 0 & 0 & 0 & 0 \\ c6 & -c2 & c2 & -c6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c1 & c3 & c5 & c7 \\ 0 & 0 & 0 & 0 & c3 & -c7 & -c1 & -c5 \\ 0 & 0 & 0 & 0 & c5 & -c1 & c7 & c3 \\ 0 & 0 & 0 & 0 & c7 & -c5 & c3 & -c1 \end{bmatrix}^{-1}$$

Figure 3. matrix relation for IDCT

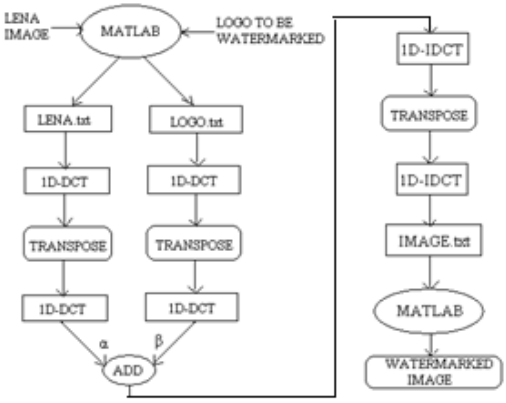

Figure 4. Design flow

A. Watermarking in Frequency Domain

Watermarking in frequency domain is the most common method of digital image watermarking. This can be done using different transforms like Discrete Cosine Transform (DCT), Discrete Sine Transform (DST), Discrete Hartley Transform (DHT) and Discrete Wavelet Transform (DWT) [2]. In the frequency domain watermarking the two images, that is the image to be watermarked and the image on which

the watermark should be laid are transformed to the frequency domain. The frequency domain of the two images is added in different proportions using equation (1). The inverse transform of the output is taken to get the watermarked image.

$$V_i' = V_i * (1 + \alpha * (X_i + \beta * W_i)) \quad (1)$$

Where Vi' is the result of the added DCT of the two images. Xi is the DCT value of the image on which the watermarking is done and Wi is the DCT of the logo which is watermarked on the image. The constants α, β, decides the visibility of the watermark. If the value of β is very less we obtain invisible watermark and as its value increase the visibility also increases. For the extraction of watermark the value of α and β has to be known. So the extraction of the watermarking cannot be done by anyone who does not know the values. To increase the security there are also methods where in the values of α and β are varied for each

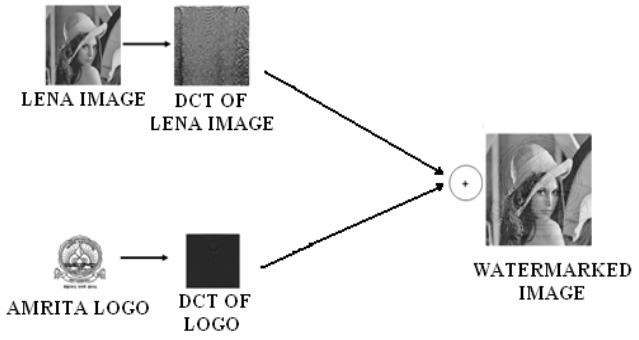

Figure 5. DCT/IDCT based digital watermarking.

block and these values are known only to the owner, which is the principle used in image authentication or copyright [2]. Suppose we choose α to be 0.97 and β to be 0.27 we get a watermark of average visibility. The visibility of the watermark can be decreased by decreasing the value of β to 0.17. When it is decreased further we find that invisible watermark can be obtained.

Considering any image, bulk of its information is embedded in the lower frequencies. These lower frequency components are referred to as detail coefficients. These coefficients have very little correlation between them. While computing the DCT or DWT more importance is given to the low frequency components than the high frequency components. Fig.5 shows the implementation of digital watermarking in frequency domain using Discrete Cosine Transform.

B. Watermarking in Spatial Domain

Conventional Spatial domain watermarking is generally not in use due to its least reliability. In the spatial domain, pixels in randomly selected regions of the image are modified according to the signature or logo desired by the author of the product. This method is as simple as modifying the pixel values of the original image where the watermark should be embedded. Fig. 6 shows the block diagram of a spatial-domain data embedding system. Randomly selected image data are dithered by a small amount according to a predefined algorithm which may vary in complexity in practical systems. The algorithm defines the intensity and the position of the watermark on the original image. One of the major disadvantages of the conventional watermarking is that it can be easily extracted from the original image which makes this technique unsuitable for copyright authentication.

There are three factors that determine the parameters of the algorithm that is used in the spatial domain watermarking. The three factors are:

- The information associated with the signature-The signature is the watermark that we embed on

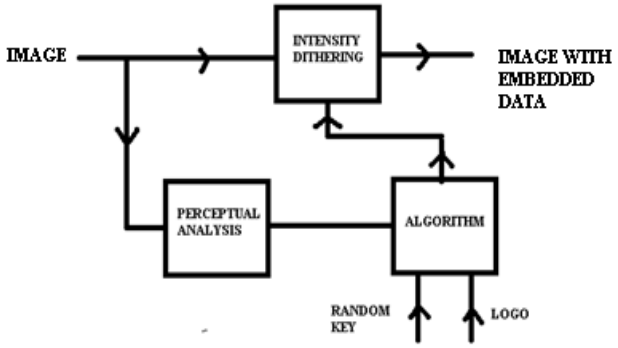

Figure 6. Spatial domain data embedding system.

the original image. The information of the signature is closely related to the size and quality of the signature

- The secret random key- The secret key may be included in the process of watermarking to improve the security during transmission. If a key is also included, only the receiver who knows the key can extract the watermark and not any intruders.
- The masking property of the image- The masking property of the image is also related to the quality and composition of the image which signifies the clarity of the watermark on the original image.

One form of the data embedding algorithm is given by the equation (2),

$$\hat{y} = y + \alpha I \quad (2)$$

Where y(i,j), is the original image intensity at pixel position (i,j), $\hat{y}$ is the marked image, and αI represents the embedded data in the form of small changes in intensity levels. The author of the watermark holds two keys:

- One is the regions of the image where the mark is hidden and
- The information in the watermark, αI.

Given the marked image, the original owner will be able to recover the watermark by comparing the marked image with the original. In the reconstruction of the embedded watermark, the following computation is made,

$$I = (\hat{y} - y)/\alpha \quad (3)$$

This is the simplest watermarking technique that can be used.

V. DIVERSIFIED INTENSITY MATRIX

The pixel values of a gray scale image varies from 0 to 255. The pixel intensity matrix of the original image is compared with four predetermined constant terms. These constants for 8-bit encoded pixel data are 63,127,191 and 255. The four diversified pixel intensity matrices are named

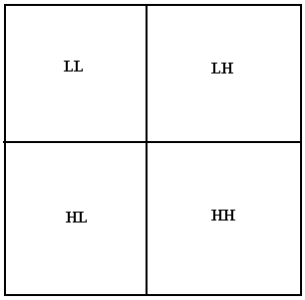

Figure 7. Diversified pixel intensity matrices

TABLE I. DIVERSIFIED INTENSITY MATRICES

Category	Pixel value range (P)	Diversified intensity matrix
1	$0 < P \leq 63$	LL
2	$64 \leq P \leq 127$	LH
3	$128 \leq P \leq 191$	HL
4	$192 \leq P \leq 255$	HH

as lowest intensity matrix(LL), Intermediate Intensity Matrix(LH) ,Higher Intensity Matrix(HL) and Highest Intensity Matrix(HH) as shown in Fig 7.

Each pixel value is compared with these four constants and sorted into corresponding matrices that is given in Table I. The matrices thus obtained have one fourth the size of the original image matrix.

VI. NOVEL METHOD FOR SPATIAL DOMAIN WATERMARKING

The methodology that we used in the spatial domain watermarking involves the following steps. The first step involves the computation of the four diversified pixel intensity matrices for the original image, as well as the watermark, I to be embedded as shown in Fig 8. This is done by the comparator technique mentioned in the previous section. Once these eight matrices have been obtained, the four diversified pixel intensity matrices of the watermark is scaled by a constant, α.

Similarly the four diversified intensity matrices of the original image to be watermarked is scaled by another factor β. Once these scaled matrices are obtained, one can do both visible as well as invisible watermarking.

A. Visible Watermarking

The eight matrices obtained after scaling are added together to obtain the Watermarked Image, ŷ. The visibility of the watermark can be varied by changing the value of α and β. Prior to the above addition, the values of the scaling factors, α and β were experimentally determined to be 0.12 and 0.97 respectively. This is in no way different from conventional spatial domain watermarking. The technique that could be used to make data embedding step easier is by

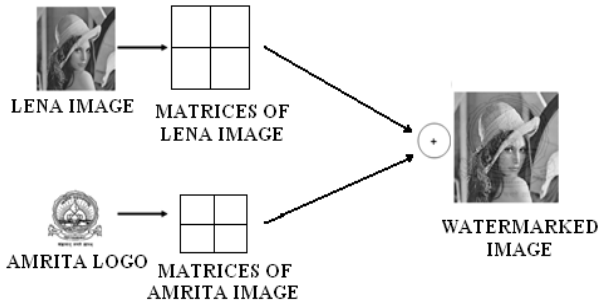

Figure 8. Spatial domain digital watermarking with two images.

discarding the lowest intensity matrix of the watermark (matrix LL). In this way the amount of data in the final image will get reduced, thereby achieving a finite amount of compression.

A. Invisible Watermarking

The advantage of this type of watermarking is that one cannot identify the watermark that is embedded in the image. This is most commonly used for secret communication . For the process of invisible watermarking the scaling factors, α and β were experimentally found to be 0.005 and 0.97. One can decrease the complexity of the method by adopting the step described above in section *A*.

B. Robustness of the Watermarking Technique

Digital image watermarking can be done for copyright authentication or secret communication. The former can be achieved by the invisible watermarking done by the novel method proposed. The latter should be tested for its robustness and hence we used Pseudo Random Noise for the purpose of security. This noise was added to the watermarked image as a key with the intention of bringing about a variation in the pixel values. Robustness was checked by adding random noise along with the scaled and added versions of the diversified intensity matrices and then transmitted. To check the security aspect, we tried the extraction of the watermark without using the key, which was not possible. The normal watermark can be extracted out from the conventional spatial domain watermarked image just by subtracting the original image (Lena image) from the watermarked image. The security is ensured by the fact that direct subtraction of the original image from the watermarked image by an eavesdropper results in an unrecoverable blurred image with no resemblance to that of the watermark. Only the intended user can extract the watermark by using the same key at the receiver end. So this would prevent any eavesdropper from extracting the information embedded in the watermark, which makes the method suitable in security aspect as well.

Robustness of this watermarking technique can also be verified by use of pseudo random noise with the watermarked image. In this case an intruder who does not know the proper key that is multiplied with the image cannot extract the watermark.

C. Retrieval of the watermarked image

If the lowest intensity matrix is not sent, then it should be notified to the receiver and the receiver should act accordingly. The reconstruction of the watermark could be done by assuming zeros in those pixel values which are not sent. This method of compression would work if the image is a pure black and white image. In this case, the retrieved image would have a considerably high PSNR. Otherwise, that is if the image contains all the colour shades, the receiver will have to retrieve the image with a lower PSNR. To avoid this scenario, the image is watermarked as such, that is, without any compression. But if it is a pure black and white image then its lowest intensity matrix need not be sent. This could be used for compression in black and white text images or other similar images.

VII. IMPLEMENTATION

The method of digital image watermarking that we have introduced is entirely different from the conventional spatial domain watermarking techniques. The proposed method of implementation is verified in MATLAB and then implemented in Verilog HDL. Then the simulation is done using Modelsim 6.2c. We also synthesized this design using Xilinx ISE 10.1. We have compared the conventional spatial domain watermarking with our method. It can be seen that the proposed method of watermarking is more secure than the conventional watermarking technique.

In the design proposed, we have used four comparator modules to classify the pixels into the diversified intensity matrices. The first stage in the implementation is the comparison of the pixel values and the classification of the values into four intensity groups. Out of the four matrices LL, LH, HL and HH, the lowest intensity pixels are classified into the HH matrix (that is with lowest pixel values). The similar classification of the four matrices is done in the image to be watermarked, using comparators. So now that the two images are divided into four blocks based on the difference in the pixel values, watermarking of the image can be done by adding the corresponding matrices with varying proportions. The proportion of the image to be added can be decided by the degree of visibility that is required in the watermarking. The results and analysis of this implementation is discussed in the next section of this paper.

VIII. PROCEDURE

At first MATLAB is used for generating the bit files of the intensity matrices or the pixel values for both the original image and the image to be watermarked. Then these bit files are taken as input to the implemented hardware block and the watermarked image is received at the output of the hardware module.

In the hardware, which is implemented using Verilog HDL, the different intensity matrices are computed and they are added. After the corresponding matrices have been added, the resultant matrix is converted into the bit file. This is the pixel values of the watermarked image. The bit file output is read into Matlab and is converted into the image, which is the watermarked image. The watermark or the signature can be retrieved by using the same tool and its PSNR to the original image can be calculated.

IX. RESULTS

Fig.9 shows the results of implementation using the standard 'Lena' image which is the original image used andThe image to be watermarked which is the logo of our university, Amrita Vishwa Vidyapeetham. Fig.9 (c) shows the watermarked 'Lena' image using the proposed methodology of watermarking. For this visible watermarking we have used the α-value to be 0.9 and β-value to be 0.12. Fig.9 (d) shows the result of the invisible watermarking done where we chose α value to be 0.9 and β value to be 0.005.

The invisible watermarking is implemented by adding a different scaled version of the image to be watermarked to the original image. Finally it is retrieved by using a secret floating point number. The algorithm is implemented in Verilog HDL. The applicability of this method for any image is also verified using another standard image, which is the 'Cameraman' image. The watermarking is done using 'Lena' image as the base image and 'Cameraman' image is watermarked onto it. Results obtained are as shown in Fig.10. Here the original image is again the 'Lena image'. The robustness and the usability of the method is guaranteed only if there is a high Peak Signal to Noise Ratio for the retrieved watermark with the original watermark.

X. PSNR CALCULATION

The robustness of the method is given by the Peak Signal to Noise Ratio (PSNR) value of the retrieved image with respect to that of the original image. The value of PSNR for the proposed method is found out experimentally. The digital image watermarking was done by the proposed method and noise was added to it. We did the retrieval of the watermark from the watermarked image and the mean square error and the PSNR is found out. The Mean Square error, M.E and the PSNR of the retrieved image can be calculated by using the following equations (4) and (5).

$$M.E= (1/(m*n))*\sum i \sum j (I_1(i,j)-I_2(i,j))^2 \quad (4)$$

$$PSNR=10*\log (\max(I_1(i,j))^2)/M.E) \ dB \quad (5)$$

where m and n are the pixel dimensions of the image, I1 and I2 are the original and retrieved images respectively.

The results of the calculations for the proposed spatial domain watermarking and a standard frequency domain watermarking using DCT are as given in Table I. It can be seen that the PSNR value of the proposed method is comparable to the PSNR that can be obtained by the frequency domain watermarking which is most commonly used. The DCT based watermarking could give a PSNR of 33.16 and the novel spatial domain gives a PSNR of 29.66 dB which shows that our method is reliable and robust. The comparison is made with the implementation done using DCT algorithm [1].

From Table II it is clear that the proposed method of digital image watermarking is reliable to a good extent since it gives a PSNR value comparable to the PSNR value that can be obtained by the frequency domain watermarking for the same set of images used.

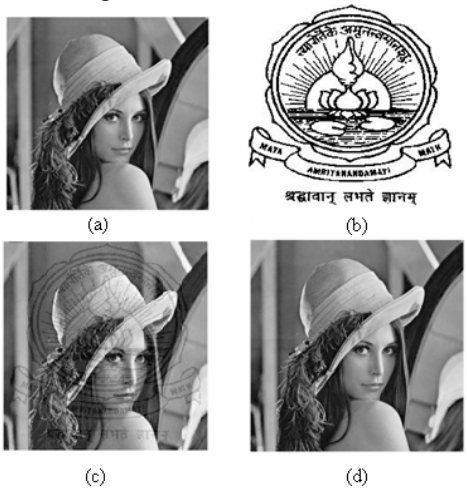

Figure 9. The figure shows (a) the original Lena image (b) the logo to be watermarked (c) visible watermarked image and (d) invisible watermarked image

Figure 10. The figure shows (a) the Lena image (b) the original Cameraman image to be watermarked (c) visible watermarked image and (d) the retrieved cameraman image.

TABLE II. COMPARISON OF PSNR VALUES IN SPATIAL AND TRANFORM DOMAINS FOR FIGURE 9.

Domain	PSNR (dB)
Spatial	29.66
Frequency(DCT)	33.16

TABLE III. COMPARISON OF PSNR VALUES IN SPATIAL AND TRANFORM DOMAINS FOR FIGURE 10.

Domain	PSNR (dB)
Spatial	318.02
Frequency(DCT)	25.72

Assume that we are using the same method for watermarking the set of images in Figures 9 and 10. The PSNR values for both the retrieved images are found. The cameraman image in Figure 10 is having less PSNR compared to amrita logo in Figure 9.

The decrease in the PSNR value for the second set of figures is due to the fact that the image used for watermarking consists of more shades between white and black. This means that the intensities of this image are not well within a finite range. Thus the method is well suitable for both compression and watermarking for those watermarks which are of the type Fig. 9 (b). Of course most of the watermarks are for data authentication and does not require high resolution images. Hence this method is well suitable for watermarking.

But if the watermarking is done without compression, that is by using all the matrices then the PSNR value is very good. This makes the method robust.

XI. DEVICE UTILIZATION

As mentioned in the beginning of the paper, the complexity of spatial domain logic is less compared to that of the frequency domain. Hence the device utilization of the spatial domain should be less. This result is observed from the design summary of the synthesis done in the Xilinx ISE. The compared results are as shown in the table.

It's obvious from TABLE IV that, the issue of complexity is figured out efficiently. The number of slices was found to be just 217 as compared to frequency domain schemes which demanded 2059 slices. The device selected was Spartan3E of Xilinx ISE 10.1.The amount of flip flops required aggregated to 169 instead of 2228. The multipliers used were hardly 11% of complete device utilization compared to 53% in Frequency domain scheme.

TABLE IV. DEVICE UTILIZATION COMPARISON

Type of Device Utilization (total number)	Spatial Domain		Frequency Domain	
	Number	Percentage utilization	Number	Percentage utilization
Number of Slices (33280)	217	0	2059	6
Number of slice flip flops(66560)	169	0	2228	3
Number of 4 input LUT's(66560)	398	0	2094	3
Number of IO's	153		820	
Number of bonded IOB's(633)	152	24	628	99
Number of MULT18X18 s(104)	12	11	56	53
Number of GCLK's(8)	1	12	1	12

The limiting factors for any VLSI design are the delay, area and power consumption. The considerable decrease in number of flip flops would effectively decrease dynamic power and area of the system.

XII. CONCLUSION

The novel spatial domain watermarking is implemented using Verilog HDL in Xilinx FPGA. The image to bit file conversion and the bit file to image conversion is done using Matlab. We have also implemented the frequency domain watermarking as mentioned in [1] & [2]. The PSNR of the proposed algorithm is found and is compared to the PSNR of the frequency domain algorithms used at present. Compression could be introduced for some image files. The watermarked images and the PSNR obtained using the proposed method ensures robustness and quality of the watermarked image. Hence the method can serve as a suitable substitute for other algorithms available at present.

ACKNOWLEDGMENT

We gratefully acknowledge the Almighty GOD who gave us strength and health to successfully complete this venture. The authors wish to thank Amrita Vishwa Vidyapeetham, in particular the Digital library, for access to their research facilities and for providing us the laboratory facilities for conducting the research.

REFERENCES

[1] Rajesh Kannan Megalingam, Vineeth Sarma.V , Venkat Krishnan.B , Mithun.M, Rahul Srikumar, Novel Low Power, High Speed Hardware Implementation of 1D DCT/IDCT using Xilinx FPGA

[2] Rajesh Kannan Megalingam, Venkat Krishnan.B, Vineeth Sarma.V, Mithun.M, Rahul Srikumar, Hardware Implementation of Low Power, High Speed DCT/IDCT Based Digital Image Watermarking

[3] Khurram Bukhari, Georgi Kuzmanov and Stamatis Vassiliadis, DCT and IDCT Implementations on Different FPGA Technologies.

[4] S. An C. Wang, Recursive algorithm, architectures and FPGA implementation of the two-dimensional discrete cosine transform

[5] Cayre F, Fontaine C, Furon T. Watermarking security: theory and practice. IEEE Transactions on Signal Processing, 2005, 53 (10) :3976-3987.

[6] W. N. Cheung, Digital Image Watermarking In Spatial and Transform Domains.

[7] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," Signal Process., vol. 83, no. 10, pp. 2069–2084, Oct. 2003, to be published.

[8] A. Kerckhoffs, "La cryptographie militaire," J. Des Sci. Militaires, vol.9, pp. 5–38, Jan. 1883.

[9] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst.Tech. J., vol. 28, pp. 656–715, Oct. 1949.

[10] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[11] Liu Jun, Liu LiZhi, An Improved Watermarking Detect Algorithm for Color Image in Spatial Domain, 2008 International Seminar on Future BioMedical Information Engineering.

[12] B. Smitha and K.A. Navas, Spatial Domain- High Capacity Data Hiding in ROI Images, IEEE - ICSCN 2007

[13] Amit Phadikar Santi P. Maity Hafizur Rahaman, Region Specific Spatial Domain Image Watermnarking Scheme, 2009 IEEE International Advance Computing Conference (IACC 2009)

[14] Houtan Haddad Larijani, Gholamali Rezai Rad, A New Spatial Domain Algorithm for Gray Scale Images Watermarking, Proceedings of the International Conference on Computer and Communication Engineering 2008.

[15] Irene G. Karybali, Efficient Spatial Image Watermarking via New Perceptual Masking and Blind Detection Schemes, IEEE transactions on information forensics and security.

[16] Dipti Prasad Mukherjee, Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication, IEEE Transactions on multimedia.