22

Novel Variance Based Spatial Domain Watermarking and Its Comparison with DIMA and DCT Based Watermarking Counterparts

Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma
Amrita Vishwa Vidyapeetham, Amritapuri Campus
India

1. Introduction

Most computers and systems are dealing with huge volumes of digital data. Major part of these digital data deals with multimedia, images and videos. The storage and secure transfer of this class of data is a burden for both individuals and organizations. Data authentication, data security and data compression are the primary requisites for any class of digital data in communication systems. Due to widespread and unrestricted use of the internet, multimedia data are available to everyone. For the protection of the author copyrights, image authentication is extremely important in present-day day communication systems. In image processing, 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 chapter, novel methods for digital image watermarking and digital image compression are discussed. A novel method for digital watermarking in spatial domain, called as the (VB)2 (Variance Based Variable Block) Algorithm, will be discussed. The comparison in robustness of the spatial domain algorithm called as the DIMA (Diversified Intensity Matrix Algorithm) with our DCT-based frequency domain algorithm has been presented in [2]. The proposed work compares all watermarking techniques and determines the method with the highest robusteness. Additionally, a compression technique to address the problem of multimedia data storage and management is also proposed. This compression is brought about by a variance based algorithm.

2. Digital watermarking

Digital watermarking is about embedding digital information into another information/data, which can be reversible or irreversible. The information can be audio, video or images. Digital watermarking can be visible or invisible and the visibility of the watermark can be varied according to the wish of the owner. Major applications of watermarking include copyright protection and steganography. In steganography, people communicate secretly with their information embedded in digital signals, which have been in use for a long time. Watermaking can be done using software or hardware. But the efficiency of the watermarking technique is found out with the capacity, robustness and perceptibility of the method. Watermarking that we have done is purely image watermarking, both visible and invisible and this finds its

potent applications in copyright authentication. Any method in frequency domain can be used for watermarking which can be based on Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Hartley Transform (DHT), etc. Watermarking can also be done using the conventional spatial domain techniques. In this chapter, we discuss an improved version of the spatial domain watermarking.

While working with images, there comes another dilemma of dealing with copyright protection. Due to the widespread accessibility of Internet, multimedia data (or images) are available everywhere with minimum effort. It becomes easier for anyone to tamper with any image according to their whims and fancies. Therefore, it becomes mandatory to provide authors of images with appropriate copyright protection. One of the methods to provide image copyright protection is to embed a watermark in the parent image. Such methods are broadly called as watermarking schemes.

3. Compressed variance-based block type spatial domain watermarking technique

Images form an integral part of all information systems. Visual information perceived by the eyes are easily registered and recollected by the brain in contrast to other sources of information. Thus, transmitting, receiving, storing and processing images become extremely important. At the same time, images require higher bandwidths for transmission and greater memory for storage. Therefore, any technique that can bring forth a significant reduction in the memory requirement of images without affecting their integrity would be extremely useful in both transmission and storage of images. Such methods are broadly known as compression methods.

3.1 Compression

Compression is the process of reducing the number of pixels in an image without affecting the overall information content. As a result, the amount of memory required to store an image is reduced significantly. In our proposed work, a novel and efficient method for compression is discussed.

In this method, an $M=2^a$ x $N=2^b$ image is divided into X blocks, each of size $P=2^c$ x $Q=2^d$, where

$$X = \frac{M*N}{P*Q} = 2^{a-c+b-d} \tag{1}$$

If the image matrix and the block matrix are square matrices, i.e., $M = N = 2^a$ and $P = Q = 2^b$, the equation can be simplified as below

$$X = 2^{2a-2b} = 2^{2(a-b)} \tag{2}$$

The next step involves computation of mean and variance of each of the X number of blocks. This step enables identification of the blocks, having the least variance values. Small value of variance in a particular block signifies the fact that pixels of the corresponding block are closely related in magnitude and that the information content in the block is less. Thus, replacing the original pixel values of various blocks with their respective mean values will not distort the image significantly. i.e., the image can be recovered efficiently. Therefore, it suffices to transmit the mean value of a block instead of the entire block itself, thereby providing unparalleled compression in the image.

After the blocks with the smallest set of variance are identified, a threshold variance V_t is chosen. Those pixels of blocks having a variance V less than V_t , are replaced by their corresponding means and transmitted. The pixels of blocks having a variance V greater than V_t , are kept unchanged from that of the parent image and transmitted. The transmitted image is recovered and its integrity to that of the parent image is measured, using a parameter called the PSNR (Peak Signal to Noise Ratio). The PSNR is a measure of the robustness of an image and its resemblance to the parent image.

In the proposed image compression technique, an instance of a 512*512 Lena Image was used. During the first analysis, this image was divided into 64 blocks each of size 64*64. The next step involved the computation of mean and variance for the 64 blocks and replacing the blocks having the minimum set of variance with their corresponding mean values. The reconstructed image showed minimum distortion as the chosen threshold value for variance was decreased. The first analysis brought about a conclusion that higher the size of each block formed during the division of an image, higher will be the chances of distortion in the reconstructed image.

In order to overcome the distortion effects, we decided to delve deep into the block division process. This enabled us to come up with an idea to construct blocks of much smaller sizes. Therefore, a compression method involving blocks of size 16*16 was devised. After forming 16*16 blocks from the Lena Image, the mean and consequently the variance of each block were computed. The analysis was done by choosing threshold variances, V_t = 10, 20, 50, 100, 200 and 300 respectively, and transmitting only the means of those blocks whose variances were less than V_t while transmitting the other blocks unchanged. The reconstructed Lena images, with compressed blocks whose variances were less than V_t , are given in Fig. 1.

Fig. 1. Reconstructed Lena images with compressed 16*16 blocks with different threshold variances V_t.

The PSNR between the original and compressed reconstructed images for varying threshold variances, V_t are tabulated in Table 1.

Compression type(Variance)	PSNR b/w original and compressed(Lena) in dB
10	49.0054
20	44.5549
50	39.5507
100	36.0901
200	33.2333
300	31.7445

Table 1. PSNR between original and reconstructed images for different values of V_t.

The amount of compression achieved from this variance based compression technique is tabulated in Table 2.

Compression type(Variance)	Percentage compression (%)
10	10.35
20	20.11
50	33.88
100	45.41
200	55.27
300	59.86

Table 2. Amount of compression achieved for varying V_ts.

By scrupulous analysis of the findings in Tables 1 and 2, it can be inferred that at V_t= 300, the compression obtained is ~60% and the PSNR is also quite high (31.74). However, if one needs to bring in more clarity in the reconstructed image, V_t = 100 can be chosen. This gives a compression of 45.5% and a PSNR of 36.1, which indicates high amount of robustness in the received image.

From Tables 1 and 2, it is possible to derive a 2nd order regression equation with PSNR as the dependent and percentage compression as the independent variable. The equation can be formulated using the following equations.

$$PSNR = a * (\%\ Compression)^2 + b * (\%\ Compression) + c \tag{3}$$

Performing summation on both sides of equation (3), we get

$$\sum PSNR = a * \sum(\%Compression)^2 + b * \sum(\%\ Compression) + c * N \tag{4}$$

Multiplying $\sum(\%\ Compression)$ on both sides of equation (3), we get

$$\begin{aligned} &\sum(\%\ Compression) * PSNR = \\ &a * \sum(\%Compression)^3 + b * \sum(\%Compression)^2 + c * \sum \%Compression \end{aligned} \tag{5}$$

Multiplying $(\sum \%\ Compression^2)$ on both sides of equation (3), we get

$$\sum\left(\%\ Compression^2\right)*PSNR = a*\sum(\%Compression)^4 + b*\sum(\%Compression)^3 + c*\sum(\%Compression)^2 \quad (6)$$

By determining the values of the various summation factors and solving equations (4), (5) and (6), the parameters a, b and c are obtained as follows.

a = 1.95*10^ (-3); b = - 0.48 ; c = 53.613.

Therefore, equation (3) can be re-written as

$$PSNR = 1.95 * 10^{-3} * (\%\ Compression)^2 - 0.48 * (\%\ Compression) + 53.613 \quad (7)$$

The above equation is a theoretical approximation of the dependence of % compression on PSNR of images subjected to compression derived from the findings in Tables 1 and 2.
This equation can be used to estimate the PSNR in dB of the compressed Lena image to that of the original image for any percentage compression. A compression of 60% gives a PSNR of 31 dB.

3.2 Watermarking

The process of embedding an image or text into another image for the purpose of copyright protection, security or data authentication is known as watermarking. The image into which another image is embedded is called the parent image and the image used for the embedding process is called the watermark.

Fig. 2. Watermarked images for varying compression rates defined by the threshold variances (V_t).

Consider the image to be watermarked, I and the watermark, W. In our work, we have used the Lena Image (I) as the image to be watermarked and an Amrita Logo (W) as the watermark. In the technique of watermarking, both the image and the watermark are scaled by factors α and β such that the intensity of the original image is significantly prominent (α > β) when compared to that of the watermark. The values of α and β were obtained by trial and error method to be 0.97 and 0.15 respectively. The Image obtained after watermarking would be a linear combination of scaled I and scaled W represented as given below.

$$Watermarked\ Image = 0.97 * I + 0.15 * W \quad (8)$$

The watermarked image is transmitted and then received. After reception of the watermarked image, α*I is subtracted from the received image and multiplied by (1/ β) to obtain the watermark. The watermarking process is repeated using compressed images for all the afore-mentioned threshold variances (V_t) from 10 to 300 in the previous section. The robustness of the retrieved watermark is measured using the PSNR (Peak Signal to Noise Ratio).

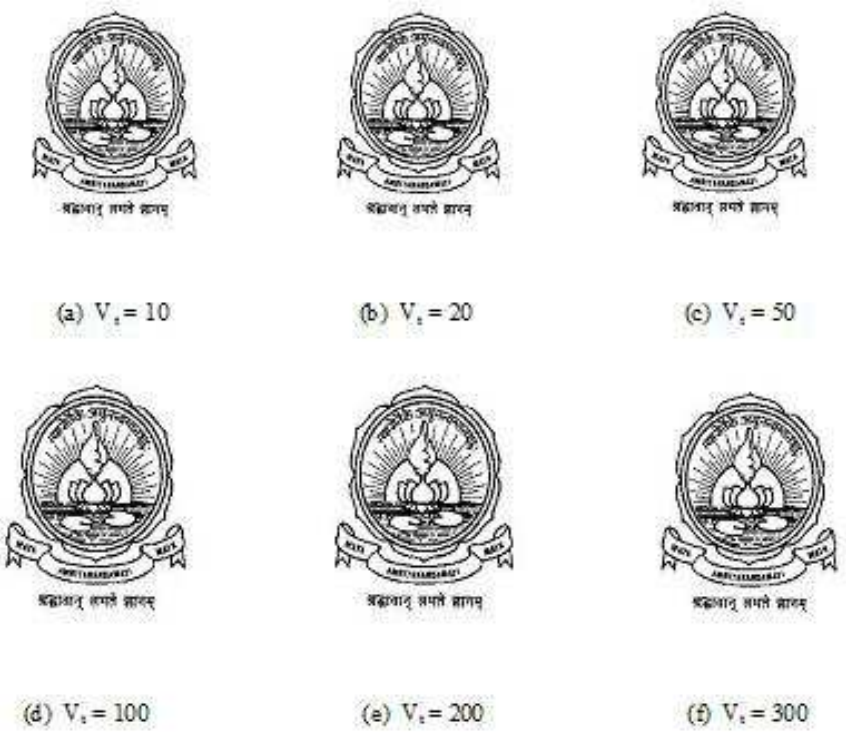

Fig. 3. Reconstructed watermarks for varying watermarking schemes compressed using threshold variances, V_t = 10, 20, 50, 100, 200 and 300.

Table 3 tabulates PSNR between original and compressed Lena images for varying threshold variances V_t.

Compression type (Variance V_t)	PSNR between original and Compressed Images (Amrita Logo)(dB)
10	57.0258
20	56.5360
50	52.6592
100	50.6900
200	47.8014
300	46.0550

Table 3. PSNR between original and compressed watermark images for varying V_ts.

Table 4 shows PSNR between original and reconstructed watermarks for varying threshold variances V_t.

Compression type(Variance V_t)	PSNR b/w original and reconstructed Images(Amrita Logo)(dB)
10	49.1933
20	49.1086
50	48.1102
100	47.3150
200	45.7512
300	44.5842

Table 4. PSNR between original and reconstructed watermarks for varying V_ts.

By heedful analysis of Tables 3 and 4, it can be observed that, as the threshold variance for compression is increased, the dip in PSNR is found to be decreasing. At V_t = 300, the dip in PSNR is about 1.47 dB (46.0550 - 44.5842). This enables us to arrive at a conclusion that at higher compression rates using the proposed method, the PSNR dip is almost insignificant. In other words, the proposed method helps to achieve high rates of compression without compromising PSNR, a technique of very high robustness and significant compression.

4. DCT based watermarking

Several frequency domain methods can be used in watermarking which can be based on Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Hartley Transform (DHT), etc. The discrete cosine transform (DCT) and the inverse discrete cosine transform (IDCT) are substantial performance bottlenecks in image watermarking, since the time taken to watermark the image depends on the time required to get the DCT/IDCT of the images.

4.1 Two dimensional DCT

A DCT expresses finite number of data points in terms of sum of cosine functions oscillating at different frequencies. The method that we used for digital image watermarking is based

on DCT, where the 2D DCT of the images are determined and added to watermark an image. This needs the 2-dimensional DCT of the images for the watermarking to be performed. 2-D DCT is represented by the equation (1), where n1 and n2 vary from 0 to 7 for a 8x8 block of data. The value of the constants k1 and k2 also vary from 0 to 7.

$$X(k1,k2) = \sum_{n1=0}^{N1} \sum_{n2=0}^{N2} x(n1,n2) Cos\left(\left(\left(\frac{\pi}{N1}\right) + 0.5\right) k1\right) Cos\left(\left(\left(\frac{\pi}{N2}\right) + 0.5\right) k2\right)$$

There are many methods for finding the 2D DCT of which the transpose method is the most common method.

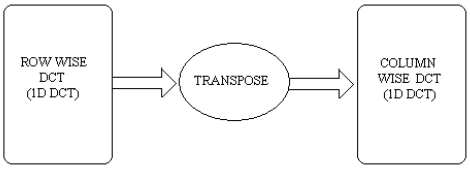

Fig. 4. 2D-DCT using 1D-DCT

The digital data of the image is made into several 8X8 blocks and the 1D DCT of each block is found out. Then the transpose of the 8x8 block is taken and again the 1D DCT is found out, which when applied to all the blocks of the image gives the 2D DCT of the whole image. In other words, the row wise block DCT is first found, followed by the column wise DCT which gives the 2D DCT. Suppose that the image under consideration is of size 512x512, and then the image, when divided into 8x8 blocks gives, 4096 blocks. The block wise DCT is found out for each block. The "Fig.1" illustrates the method of finding the 2D DCT of an 8x8 block of data. The same procedure is repeated for all the 8x8 block of data.
From the above explanation it is quite evident that the implementation of digital watermarking needs an efficient algorithm to find the 2D DCT/IDCT, for which we need the implementation of 1D DCT. So the implementation of 1D DCT has been discussed in the next section.

4.2 One dimensional DCT implementation

The 1-D DCT of a sequence of length N is given by

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\pi(2x+1)u / 2N\right] \quad (10)$$

For u=0, 1, 2, 3….. (N-1) and in the similar way the 1-D IDCT is defined as

$$f(x) = \alpha(u) \sum_{u=0}^{N-1} \alpha(u)\, C(u) \cos\left[\pi(2x+1)u / 2N\right] \quad (11)$$

For x=0, 1, 2, 3…. (N-1) and for both the equations

$$\alpha(u) = (1/N)^{0.5} \quad \text{for } u = 0$$

$$= (2/N)^{0.5} \quad \text{for } u \neq 0$$

Here we consider an 8X8 block of data and for this we will have to find the 1D-DCT for each row of 8 elements and each column of 8 elements separately. The major concern in finding the 1D DCT/IDCT is the number of multipliers and the adders that had to be used.

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

Fig. 5. Matrix method of implementing 1D-DCT/IDCT

4.3 Watermarking

Watermarking of an image can be done using the DCTs of the images to be used. The DCT of both the images are taken and the intensity of the image that has to appear as the water mark, can be varied by the proportion in which the DCT is added. The basic process that takes place, is the addition of DCTs followed by the IDCT of the result, which gives the watermarked image.

$$V_i' = V_i * (1 + \alpha * (X_i + \beta * W_i)) \quad (13)$$

Where Vi' is the result of the added DCT of the two images. X_i is the DCT value of the image on which the watermarking is done and W_i is the DCT of the logo, which is watermarked on the image. The constants α, β, affect the visibility of the watermark. For very small β value, a watermark is invisible and as the visibility increases by growth of β value. For extraction of a watermark, the values of α and β have to be known and hence the extraction of the watermarking cannot be done by anyone who does not know these values. To increase security, there are methods where in the values of α, β are varied for each block, which are known only to the owner. This is the principle used in image authentication or copyright.

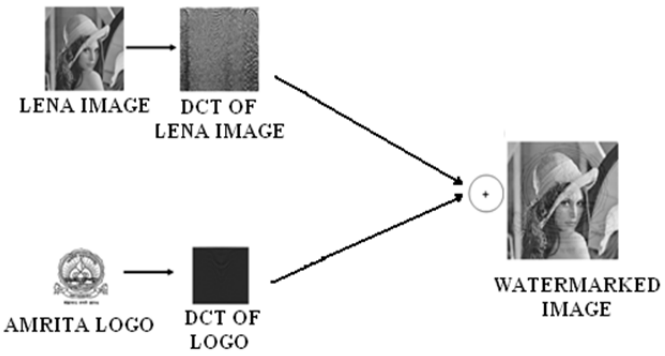

Fig. 6. DCT/IDCT based digital watermarking.

Fig. 7. (a) Lena image (b) logo to be watermarked

Fig. 8. The images obtained after watermarking (a) for α=.97 and β=.07 (b) for α=.97 and β=.17 (c) for α=.97 and β=.27 (d) invisible watermarking

5. 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 involves modifying the pixel values of the original image where the watermark should be embedded. Fig. 2 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, whose complexity may vary 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 applied in the spatial domain watermarking. The three factors are:

- The information associated with the signature. Basically, the signature is the watermark embedded on 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.

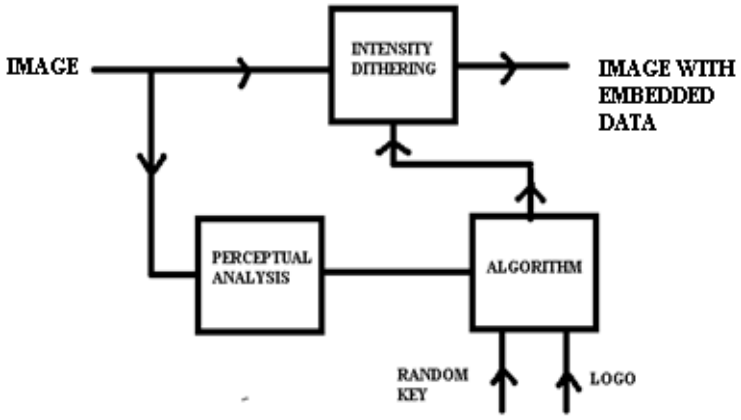

Fig. 9. Spatial domain data embedding system.

One form of the data embedding algorithm is given by the equation (14),

$$\hat{y}=y+\alpha I \tag{14}$$

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

- The region of the image where the mark is hidden and
- The information in the watermark, aI.

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,

$$I= (\hat{y}-y)/\alpha \tag{15}$$

This is the simplest watermarking technique that can be used.

5.1 Diversified intensity matrix

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 as lowest intensity matrix(LL), Intermediate Intensity Matrix(LH) ,Higher Intensity Matrix(HL) and the Highest Intensity Matrix(HH), as shown in Fig 3.

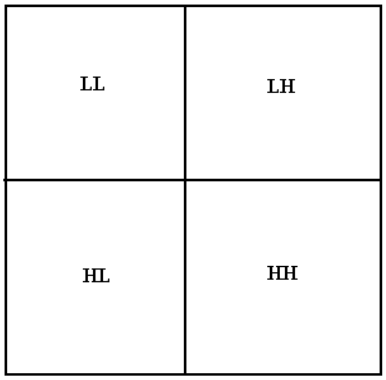

Fig. 10. Diversified pixel intensity matrices

Each pixel value is compared with these four constants and sorted into corresponding matrices as given in Table 5. The matrices thus obtained have one fourth the size of the original image matrix.

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

Table 5. Diversified Intensity Matrices

5.2 Novel spatial domain watermarking algorithm

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 to be embedded as shown in Fig. 11. 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, a.

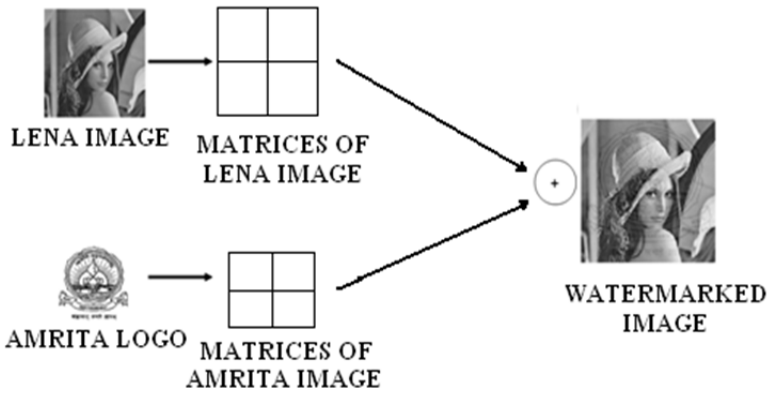

Fig. 11. Spatial domain digital watermarking with two images.

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, $\hat{y}$. The visibility of the watermark can be varied by changing the value of a and β. Prior to the above addition, the values of the scaling factors, a and β were experimentally determined to be 0.12 and 0.97 respectively.

B. 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.

C. 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 security purpose. 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 to extract 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.

5.3 Results

Fig.5 shows the results of implementation, using the standard 'Lena' image, which is the original image used and the the logo of our university, Amrita Vishwa Vidyapeetham, the watermark used. Fig.6 (c) shows the watermarked 'Lena' image using the proposed methodology of watermarking. For visible watermarking we have used $\alpha = 0.9$ and $\beta = 0.12$. Fig.6(d) shows the result of the invisible watermarking done where we chose $\alpha = 0.9$ and $\beta = 0.005$.

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. The results thus obtained are as shown in Fig.7. Here the original image is again the 'Lena image'. Since similar results are obtained for both set of images, we can conclude that this method guarantees an average PSNR for any image that we consider.

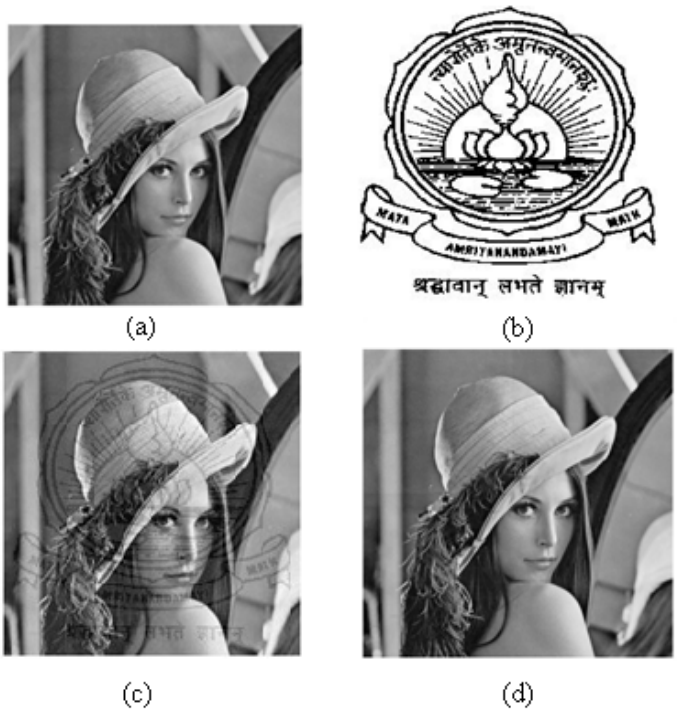

Fig. 12. The figure shows (a) the original Lena image (b) the logo to be watermarked (c) visible watermarked image and (d) invisible watermarked image.

Fig. 13. 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.

Domain	PSNR (dB)
Spatial	29.66
Frequency	33.16

Table 6. Comparison Of PSNR Values In Spatial And Transform Domains

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) & (5).

$$M.E= (1/(m*n))*\sum i \sum j (I_1(i,j)-I_2(i,j))^2 \quad (16)$$

$$PSNR=10*\log (\max(I_1(i,j))^2)/M.E) \ dB \quad (17)$$

where m and n are the pixel dimensions of the image, and 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 1. 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 2 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.

6. Comparison and results

From the above results, it can be concluded that the Compressed Variance-Based Block Type Spatial Domain Watermarking Technique is having the required amount of robustness and is able to give a good amount of compression.
The digital image watermarking using diversified intensity matrices and using discrete cosine transform is also robust. But higher robustness can be achieved using the present method as per the requirements by using equation (7). If watermarking demands a minimum robustness of X dB, put X in equation 7 and find the maximum compression that can be achieved and then do the watermarking. Hence, this is a flexible and efficient method capable of doing significant compression and robust watermarking.

7. 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.

8. 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 International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010.

[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.
[17] D.W. Trainor J.P. Heron" and R.F. Woods," Implementation of the 2D DCT using a XILINX XC6264 FPGA, "0-7803-3806-5/97.
[18] S. Musupe and is Arslun, Low power DCT implementation approach for VLSI DSP processors, 0-7803-5471 -0/99.
[19] S. An C. Wang "Recursive algorithm, architectures and FPGA implementation of the two- dimensional discrete cosine transform", The Institution of Engineering and Technology 2008.
[20] Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, " A New Robust Digital Image Watermarking Technique Based On Joint DWTDCT Transformation", Third 2008 International Conference on Convergence and Hybrid Information Technology.
[21] A.Aggoun and I. Jalloh "Two-dimensional DCT/SDCU architecture", 2003 IEE proceedings online no. *20030063*, *DO/:* 10.1049/ip-edt:20030063.
[22] Syed Ali Khayam, "The Discrete Cosine Transform (DCT): Theory and Application", Department of Electrical & Computer Engineering, Michigan State University.
[23] Kuo-Hsing Cheng, Chih-Sheng Huang and Chun-Pin lin "The Design and implementation of DCT/IDCT Chip with Novel Architecture" , ISCAS 2000 - IEEE international symposium on circuits and systems, may 28-31, 2000, Geneva, Switzerland.

[24] Christoph Loeffler, Adriaan Lieenberg, and George s. Moschytz, "Practical fast 1-d DCT algorithms With 11 multiplications ", ch2673-2/89/0000-0098.
[25] Archana Chidanandan, Joseph Moder, Magdy Bayoumi "Implementation of neda-based DCT architecture using even-odd decomposition of the 8 x 8 DCT matrix", 1-4244-0173-9/06.
[26] Archana Chidanandan, Magdy Bayoumi, "Area-efficient neda architecture for the 1-D DCT/IDCT", 142440469x/06/.

Applications of MATLAB in Science and Engineering

Edited by Prof. Tadeusz Michalowski

ISBN 978-953-307-708-6
Hard cover, 510 pages
Publisher InTech
Published online 09, September, 2011
Published in print edition September, 2011

The book consists of 24 chapters illustrating a wide range of areas where MATLAB tools are applied. These areas include mathematics, physics, chemistry and chemical engineering, mechanical engineering, biological (molecular biology) and medical sciences, communication and control systems, digital signal, image and video processing, system modeling and simulation. Many interesting problems have been included throughout the book, and its contents will be beneficial for students and professionals in wide areas of interest.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma (2011). Novel Variance Based Spatial Domain Watermarking and Its Comparison with DIMA and DCT Based Watermarking Counterparts, Applications of MATLAB in Science and Engineering, Prof. Tadeusz Michalowski (Ed.), ISBN: 978-953-307-708-6, InTech, Available from: http://www.intechopen.com/books/applications-of-matlab-in-science-and-engineering/novel-variance-based-spatial-domain-watermarking-and-its-comparison-with-dima-and-dct-based-watermar

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821