IMPLEMENTATION OF DIGITAL IMAGE WATERMARKING

Nirav Patel
Master of Engineering ,ECE Department, Bhabha Engineering Research Institute, Bhopal, India
Email: nirav.kadi@gmail.com

Abstract-**Today, Internet is increasingly used to transfer data from one end to another end. Due to advancement of Digital technologies, copying of digital data over the internet is become faster. So, copying and distributing data over the internet from unauthorized person is increased. To protect form unauthorized copying and distributing of digital media, Digital watermarking techniques are developed. It is the process of combining digital mark into the digital media using some algorithm. The two algorithms, spatial domain LSB algorithm and transform domain sub band DCT algorithm are simulated using matlab and compared.**

I. INTRODUCTION

Watermarking is the process of hiding the Information into the digital media which can be extracted later by using some algorithm. Digital Watermarking means embedding Digital stream of bits into Multimedia file. Multimedia file can be an image, video, audio or text. It describes the methods and technologies to hide the information in digital form in the digital media. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copyright, license, tracking and authorship etc.

II. GENERAL FRAMEWORK OF WATERMARKING

Digital Image Watermarking describes methods and technologies that hide information, for example a number or text, in images. Information hiding is the process of embedding a message into digital media. Figure 1 shows simple watermarking process.

security of the information is main issue while transferring the information data over the internet. There are many ways to hack the information and it is possible to copy the data and distribute this data over the internet by unauthorized person. So to withstand against such attacks and for security purpose Digital Watermarking come into the picture. Nowadays, Digital watermarking has many applications like owner identification, broadcast monitoring, copy control, data authentication etc. The digital watermarks can be a visible watermarks or Invisible watermarks. The visible watermarks are used to mark a digital image in a clearly detectable way so it can avoid unauthorized use of digital image. The visible watermark cannot be removed without any degradation of original image. So if unauthorized person try to remove the visible watermark, it removes the commercial value of the original image. While the invisible watermarks are used to authenticate the content, to detect and to prevent unauthorized copy of the data [3][5].

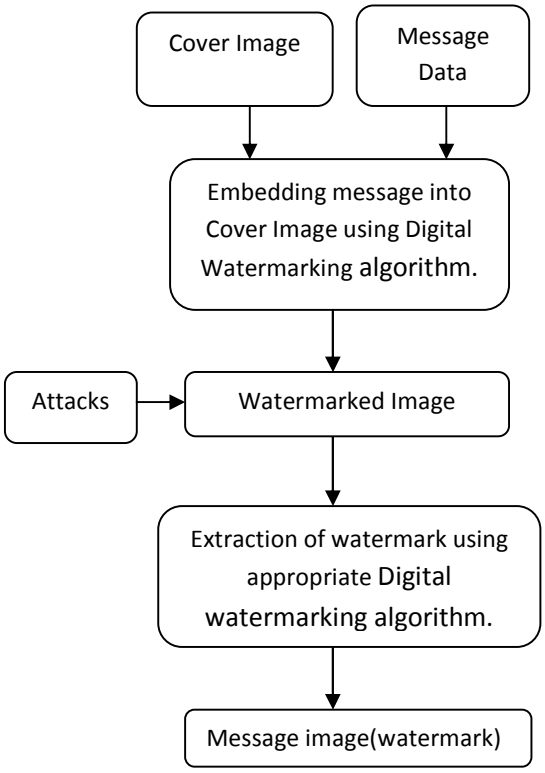


Figure 1 Simple Watermarking Process [9].

While in the Non-Blind Digital Watermarking algorithms, the original image is required to compare and extract the watermark [4]. According to domain Digital watermarking can be divided into Spatial Domain algorithms and Transform Domain algorithms. In spatial domain the watermark is embedded by manipulating the pixel values of the original

image. While In Transform domain the image is converted into another domain like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) and then the watermark is embedded in that domain.

III. CLASSIFICATION OF WATERMARKING TECHNIQUES

Digital watermarking is used to various applications according to the requirement. The properties of watermarking like robustness, security, complexity, imperceptibility are very much important while selecting the Digital watermarking technique. Basically, there are two main types of digital watermarking. First one is Spatial domain watermarking techniques and second one is Transform domain watermarking techniques [3], [5].

A. *Spatial domain watermarking techniques:* In the spatial domain image watermarking techniques, the watermark is embedded in the pixel domain using some algorithm. In this techniques the image is not transform to the another domain, but the actual pixel values are changed according to watermarking bit. Modification of bits can include the flipping of lower bits of the pixel values. The embedding process of the watermark in the cover image is based on the simple operation on the pixel values of the cover image according to the watermark bit. The watermark can be extracted from the watermarked image by correlating the expected pattern. The main advantages of spatial domain watermarking techniques are its simplicity and less complexity. But the measure disadvantages of these techniques are its robustness and security. It can survive against simple attacks like rotation or noise addition, but it cannot survive geometrical attacks like zooming, shrinking, filtering, cropping etc. Lossy compression can defeat the watermark.

B. *Transform Domain Techniques:* Transform domain methods are more widely used for watermarking as compared to spatial domain methods because its robustness against different attacks. In the transform domain methods, the original image is converted to frequency domain using discrete cosine transform (DCT), discrete Fourier transform or discrete wavelet transform (DWT). After converting the image in spectral coefficients using any one of the method mentioned above, the watermark is embedded in this domain by changing the coefficients of the transform domain. The reason for choosing frequency domain is that the characteristics of human visual system (HVS) are better understood using spectral coefficients. For example, HVS is more sensitive to low frequency coefficients while it is less sensitive to the high frequency coefficients [5]. Also in the lossy compression the high frequency coefficients are removed due to its less sensitivity. So for embedding the watermark in transform domain method choosing the coefficients is very important. Mostly, middle level coefficients are selected for watermark embedding because low frequency coefficients are more sensitive and high frequency coefficients are considered insignificant. After embedding the watermark, the inverse transform is apply to get watermarked image.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

we are going to compare spatial domain and transform domain methods. P. Kr Sharma and Rajni [7] proposed a Blind watermarking method based on Least Significant Bits. In this method they embed the watermark into the spatial domain by changing the Least Significant Bits of the Cover Image. Z. Rui-mei, L. Hua, P. Hua-wei, H. Bo-ning [13] proposed a blind watermarking technique based on the modified AC coefficient based in the subband DCT domain. We simulate these methods using Matlab and compare both methods by calculating the Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Normalized Cross correlation (NC) parameters. The MSE and PSNR are two error matrix used to compare Image quality. This ratio is often used to measure the quality between original Image and watermarked Image. The lower the value of the MSE lower will be the error. The MSE is given by the equation [7]:

$$MSE = \frac{\sum_{i=1}^{k}\sum_{j=1}^{k}[I(i,j) - I'(i,j)]^2}{k \times k} \qquad (1)$$

Where $I(i,j)$ is the original Image without watermark embedding, $I'(i,j)$ is the watermarked Image and k is the size of the Image. The PSNR represents measure of the Peak error. The PSNR is given by the equation [13]:

$$PSNR = 10log_{10}\frac{255 \times 255}{\sum_{i=1}^{k}\sum_{j=1}^{k}[I(i,j) - I'(i,j)]^2} \qquad (2)$$

Where $I(i,j)$ is the original Image without watermark embedding, $I'(i,j)$ is the watermarked Image and *k* is the size of the Image. The Normalized Cross correlation is used to detect the similarity between original watermark and extracted watermark. The Normalized Cross correlation (NC) is given by the equation [13]:

$$NC = \frac{\sum_{i=1}^{L}\sum_{j=1}^{L}[W(i,j)\times W'(i,j)]}{\sqrt{\sum_{i=1}^{L}\sum_{j=1}^{L}W(i,j)^2}\sqrt{\sum_{i=1}^{L}\sum_{j=1}^{L}W'(i,j)^2}} \quad (3)$$

Where $W(i,j)$ is the original watermark, $W'(i,j)$ is the extracted watermark and L is the size of the watermark.

A.*Spatial domain algorithm*

The proposed algorithm by P. Kr Sharma and Rajni [7] is based on the LSB substitution by the watermark bits in the Cover Image. The steps for proposed algorithm are as following:

Step 1: Convert Cover Image from RGB to Gray-scale Image.

Step 2: Find out size of the Cover Image and Watermark.

Step 3: In the first pixel of cover Image, replace LSB of the Cover Image with the MSB of first pixel of the watermark.

Step 4: Repeat step 3 until all watermark bits are embedded in the Cover Image.

B.*Transform domain algorithm*

Z. Rui-mei, L. Hua, P. Hua-wei, H. Bo-ning [13] proposed a sub band DCT based blind watermarking algorithm in which watermark is embedded in the AC coefficients of the each block. The proposed algorithm is robust against some digital image attacks, like JPEG compression, noise, filtering and shearing. They were embedded 2-bit watermark image but I simulated this algorithm by using binary watermark. The watermarking steps of the proposed algorithm by ZHAO Rui-mei, LIAN Hua, PANG Hua-wei, HU Bo-ning are as following:

C. *Watermark Embedding*

Step 1: The 2-bit watermark image W is transformed into W' by using Arnold transform. The W' is scanned on-line and then transformed into one-dimensional sequence. A of size LxL. Where L is the size of W. The Arnold transform is given by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ L) \quad (4)$$

Where x and y are pixel coordinates of the W and x' and y' are pixel coordinates after Arnold Transform.

Step 2: The original Image(Cover Image) is divided into 8x8 blocks and each block is transformed into DCT coefficients.

Step 3: The DCT coefficients are scanned by means of Zig-Zag and the one dimensional sequence $Z_i(m)$ ($m = 1,2,\ldots,64$) is getted. AV of all $Z_i(m)$ is calculated which os given by

$$AV = \frac{\sum_{i=1}^{L\times L}|Z_i(m)|}{L\times L} \quad (5)$$

Step 4:The sequence A embeds in $Z_i(m)$ of each block by the following formula

$$Z_i(\mathrm{m}) = \begin{cases} -|AV-\Delta| & a_i = 1\ and\ Z_i(m) > 0 \\ -|AV+\Delta| & a_i = 1\ and\ Z_i(m) < 0 \\ |AV+\Delta| & a_i = 0\ and\ Z_i(m) > 0 \\ |AV-\Delta| & a_i = 0\ and\ Z_i(m) < 0 \end{cases} \quad (6)$$

Where $\Delta = \big||Z_i(m)| - AV\big|/10$.

Step 5: The Watermark image I' is achived after each block is transformed into IDCT data.

D.*Watermark Extraction*

Step 1: The watermarked Image I' is divided into 8x8 blocks and each block is transformed into DCT coefficients. The DCT coefficients are scan by means of Zig-Zag. A one dimentional sequence B ($B = \{b_i\}, i = 1,2,\ldots L\times L.$) is getted. The value of b_i is given by

$$b_i = \begin{cases} 1 & Z_{i(m)} > 0 \\ 0 & Z_{i(m)} < 0 \end{cases} \quad (7)$$

Step 2: The one-dimentional sequence *B* is recognized into two-dimensional image watermark *W'*.

Step 3: The image watermark *W'* is obtained by inverse Arnold transform.

V.SIMULATION RESULTS

The comparison of spatial domain LSB algorithm with transform domain subband DCT domain algorithm uder different conditions. In the LSB algorithm the watermark used is of size 256x256 and in the subband DCT domain the watermark size is 64x64. Figure 2 shows the results of applying LSB algorithm to embed the binery cameramen Image as a watermak in the 8-bit Baboon Image.Image as a watermak in the 8-bit Baboon Image.

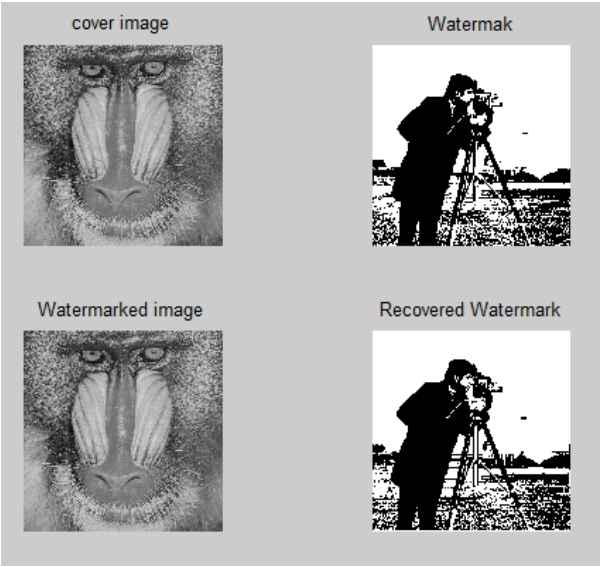


Figure 2 Output Result of using spatial domain LSB algorithm

Figure 3 shows the result of applying to hide 64x64 binery watermark in the 8-bit gray-scale baboon Image using subband DCT algorithm.

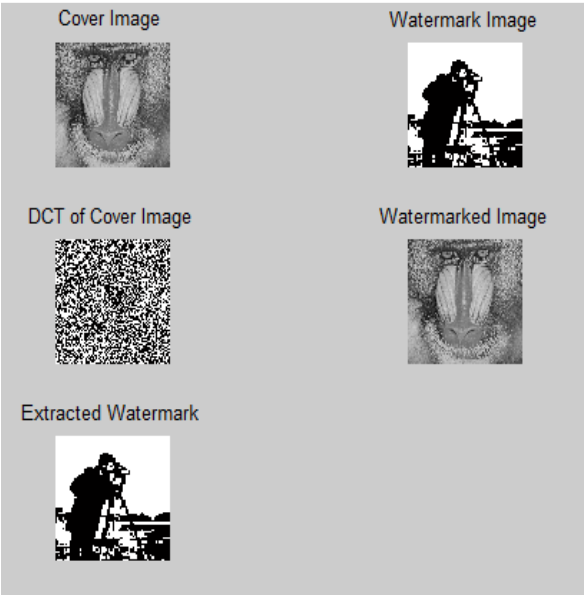


Figure 3 Output Result of using sub band DCT algorithm

Table 1 shows the results of both algorithms without any attacks on the watermarked Image. Results shows that LSB algorithm provide good MSE but the Normalised crosscorrelation factor is not so good as compared to subband DCT algorithm. The NC of LSB algorithm is 0.8987 while it is 1 in case of subband DCT. The results of both methods under the salt and pepper noise is shown in the Table 2. In this condition also the PSNR and NC of subband DCT is good. Table 3 shows the results of applying this algorithms under the gaussian filtering. From the results we can see that in case of LSB algorithm the watermark is not recognised while it is perfectly extracted with good PSNR and NC factor. The PSNR in this case for subband DCT algorithm is 34.3954 and the NC is 0.9996 while in case of LSB algorithm it is 35.1402 and 0.5433 respectively.

Table 1 Comparison table of two methods without any attacks.

Without any attacks the value of MSE,PSNR and NC of both methods are	
LSB algorithm	**Subband DCT algorithm**
Watermark Size is 256x256	Watermark Size is 64x64
MSE :- 0.2024 **PSNR** :- 55.0691 **NC** :- 0.8987	**MSE** :- 8.4033 **PSNR** :- 38.8863 **NC** :- 1

Table 2 Comparison table of two methods under the salt & pepper noise.

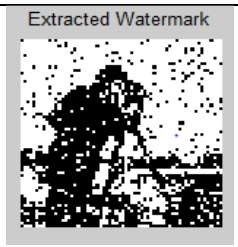
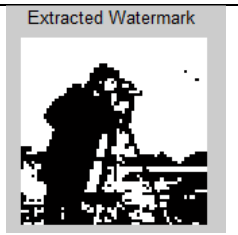
Under the salt & pepper noise of 0.01 strength	
LSB algorithm	**Subband DCT algorithm**
Watermark Size is 256x256	Watermark Size is 64x64
MSE :- 1.4943 **PSNR** :- 46.3864 **NC** :- 0.8952	**MSE** :- 9.6366 **PSNR** :- 38.2916 **NC** :- 0.9268

Table 3 Comparison table of two methods under the Gaussian filtering.

Under the Gaussian Filtering with sigma 0.5.	
LSB algorithm	**Subband DCT algorithm**
Watermark Size is 256x256	Watermark Size is 64x64

MSE :- 19.9096 **PSNR** :- 35.1402 **NC** :- 0.5433	**MSE** :- 23.6349 **PSNR** :- 34.3953 **NC** :- 0.9996

Table 1 Comparison table of two methods by extracted watermark.

	LSB algorithm	**Subband DCT algorithm**
Without any attacks the extracted water-mark		
Under the salt & pepper noise of 0.01 strength		
Under the Gaussian Filtering with sigma 0.5.		

VI.CONCLUSION

The advantages of spatial domain is its simplicity and it can provide robustness against some simple attacks like noising or shearing, but it cannot provide the robustness against geometric attacks, JPEG compression or filtering. On the other hand transform domain algorithms are robust against such type of attacks. The transform domain algorithms are complex as compared to spatial domain algorithms but it can provide better robustness as compared to spatial domain algorithms. simulation results of two algorithms we can conclude that sub band DCT domain algorithm is more robust and has good correlation and noise resisting factor as compared to spatial domain LSB algorithm.

VII.FUTURE WORK

In Future, these algorithms which are simulated using Matlab can be simulated using DSK-6713. The comparison can be done by finding different performance parameters DSK-6713.

REFERENCES

[1] Harpuneet Kaur, "Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data," 2006.

[2] Darshana Mistry, "Comparison of Digital Water Marking methods," *International Journal on Computer Science and Engineering*, vol. 2, no. 9, pp. 2905-2909, 2010.

[3] Song Han and Elizabeth Chang Vidyasagar M. Potdar, "A Survey of Digital Image Watermarking Techniques," , 2005, pp. 709-716.

[4] Sonika Jindal and Sunny Behal Manpreet Kaur, "A STUDY OF DIGITAL IMAGE WATERMARKING," *International Journal of Research in Engineering & Applied Sciences*, vol. 2, no. 2, pp. 126-136, February 2012.

[5] C. M. Wolak, "Digital Watermarking," *IEEE transactionson Industrial Electronics*, vol. 48, no. 5, pp. 875-882, October 2001.

[6] Lin Liu, "A Survey of Digital Watermarking Technologies," Department of Electrical and Computer Engineering, State University of New York at Stony Brook, NY 11794-2350, 2005.

[7] Puneet Kr Sharma and Rajni, "Information security through Image Watermarking using Least Significant Bit Algorithm," *Computer Science & Information Technology*, vol. 2, no. 2, May 2012.

[8] Rosziati Ibrahim and Mohd. Najib Mohd. Salleh Abdullah Bamatraf, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," *JOURNAL OF COMPUTING*, vol. 3, no. 4, April 2011.

[9] Florence Denis and Atilla Baskurt Fadoua Drira, "Image watermarking technique based on the steerable pyramid transform," in *International Society for Optical Engineering-Wavelet Applications In Industrial Processing, Philadelphia,Pennsylvania,USA*, 2004, pp. 165-176.

[10] Santi Prasad Maity and Malay Kumar Kundu, "Robust and Blind Spatial Watermarking in Digital Image," in *3rd Indian Conf. on Computer Vision, Graphics and Image Processing*, 2002, pp. 388-393.

[11] P Nagaraju, Vinay J, Kavya N Bhushan, Naren S Vasanad Thanuja T C, "Hardware Implementation of a Robust Modulo Watermarking Algorithm," *MES Journal of Technology and Management*, vol. 2, no. 1, pp. 51-56, 2011.

[12] Lian Hua, Pang Hua-wei and Hu Bo-ning Zhao Rui-mei, "A Watermarking Algorithm by Modifying AC Coefficies in DCT Domain," in *International Symposium on Information Science and Engineering*, December 2008, pp. 850-853.

[13] Martín Amado and Fernando Pérez-González Juan R. Hernández, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 56-68, January 2000.

[14] Chandra Mohan B and Srinivas Kumar S., "Robust Multiple Image Watermarking Scheme using Discrete Cosine Transform with Multiple Descriptions," *International Journal of Computer Theory and Engineering*, vol. 1, no. 5, pp. 47-51, December 2009.

[15] Franco Bartolini, Vito Cappellini and Alessandro Piva Mauro Barni, "A DCT-domain system for robust image watermarking," *Signal Processing*, vol. 66, no. 3, pp. 357-372, May 1998.

[16] Mr.Navnath S. Narawade and Dr.Rajendra D.Kanphade, "DCT Based Robust Reversible Watermarking For Geometric Attack," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 1, no. 2, pp. 27-32, August 2012.