Journal of Science Research

Volume 9, 2010

Journal of Science Research (2010) Vol. 9: 33-41 *ISSN 11179333*

Digital Watermarking of Still Images with Colour Digital Watermark

Zubair A.R., Fakolujo O.A. and Rajan P.K.

Abstract Digital Watermarking is a popular tool for copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication. In this paper, a method of embedding a colour image as digital watermark into a host image is proposed. The watermark is first converted from the Red-Green-Blue (RGB) colour space to an index image. The index image is decomposed into a series of binary digital images for implementation as multiple watermarking. Experimental results show that the proposed method is robust to reasonable image processing operations and the lossy compression techniques such as the Joint Photographic Experts Group (JPEG) compression. Furthermore, application of democratic approach in signal sampling is found to produce better signal to noise ratio compared with uniform quantization approach.

Keywords: Watermarking, Copyright Protection, Secret Communication, Sampling, Compression.

Introduction

The rapid expansion of the Internet and the increased availability of digital data recording and duplicating devices have increased the availability of digital data such as text, audio, images and videos to the public. Copyright owners are concerned about illegal duplication and distribution of their data and work. A solution for this is to use digital watermarking to protect intellectual property of creators, distributors or owners of such data.

Digital watermarking is applied for copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication. Digital watermarking is the hiding of a secret message or information within an ordinary message and its extraction at its destination[1,2,3,4,5,6,7,8,9]. The secret message is the digital watermark.

An effective watermarking scheme must successfully deal with the triple requirements of imperceptibility, robustness and capacity [1,3,5,8]. Imperceptibility requires that the host data and the watermarked data be perceptually undistinguishable. Robustness requires that the watermark be reliably detectable after alterations or corruption of the watermarked data. Capacity is the size of watermark [1]. Small size may enhance both robustness and imperceptibility.

Various forms of digital watermarks can be found in the literature [13]. One-dimensional and two-dimensional digital watermarks are common. These have less perception and information of copyright ownership compared with a three-dimensional watermark. The three-dimensional watermark considered in this paper is essentially another RGB colour image.

The 3-D watermark is first pre-processed by converting it from the RGB colour space to an index image. The resulting index image has a 2D matrix and a colour map. The colour map is stored and is available as part of the watermark extraction key. The 2D matrix is essentially a 2D gray-scale image which is decomposed into a series of binary digital images using stack filter's threshold decomposition technique [8]. The resulting binary digital images are then used to implement multiple watermarking in the spatial domain. Due to its higher dimensionality, copyright ownership is more secret and robust in multiple watermarking [8].

Pre-Processing of the Watermark

The watermark is a RGB colour image w(m x n x 3) where each pixel is represented by 24 bits. First, w is converted to an index image w_i which is fully represented by a 2D matrix y(m x n) and a colour map p(256 x 3). The values of pixels in y range from 0 to 255. For example, if the value of a pixel in y is I, the actual red, green and blue intensities of this pixel are located at p(I+1,1), p(I+1,2) and p(I+1,3) respectively.

Zubair A.R.
Department of Electrical/Electronic Engineering, University of Ibadan, Ibadan, Nigeria.

Fakolujo O.A. and Rajan P.K.
Department of Electrical and Computer Engineering, Tennessee Technological University (TTU), USA.

This conversion can be thought of as signal (colour) sampling, selecting 256 colours to represent an image with possible 2^{24} colours. Not all the possible colours are present in a given image. Also a particular colour may occur more than once. Furthermore, some colours are so close to each other that the human eye cannot distinguish between them. Therefore, it is possible to choose 256 colours without introducing a large quantization error. The conversion is also a form of image compression where y and p are represented by (mn + 256x3) pixels while w is represented by 3mn pixels. As long as mn is greater that 384, which is usually the case, (mn + 256x3) is less than 3mn.

Signal reconstruction can be easily carried out by recovering the image w_r(m x n x 3) from y and p. To evaluate the error introduced by the sampling, we may use the values of peak signal to noise ratio (psnr) and normalized cross-correlation (NC) [10,11,12,13,14]. The psnr and NC are given by Eqns (1) and (2) to 1, the better is the signal sampling process.

$$psnr = 10\log_{10}\left[\frac{255^2}{\frac{1}{3mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{t=1}^{3}(w(i,j,t)-w_r(i,j,t))^2\right]}\right] \quad (1)$$

and NC is expressed as

$$NC = \frac{\left[\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{t=1}^{3}w(i,j,t)w_r(i,j,t)\right]}{\left[\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{t=1}^{3}(w(i,j,t))^2\right]} \quad (2)$$

where i, j and t are row, column and colour variables

The types of sampling approaches considered in this paper are described next.

Uniform Quantization Approach

The image is scanned from pixel to pixel. The colour of the first pixel is selected and included in the colour map p. The colour of every other pixel I_p is compared with the already selected colour I_s in the colour map. Initially, k is chosen as 1. The inequality in (3) is checked for the three colour components of I_P.

$$(I_s - k) \le I_p \le (I_s + k) \quad (3)$$

If Eqn. (3) is true for the three colour components of I_P, the exact colour I_P of the pixel concerned is discarded and approximated as the already selected colour I_S in p. If Eqn. (3) is false for at least one component of I_P, the colour of the pixel concerned is compared with yet another already selected colour in p. If Eqn. (3) is false after comparing with all the colours in colour map p, then the colour of the pixel is selected and included in p.

If the number of selected colours in p is more than 256, k is increased by 1 and the process is repeated until the number of selected colours in p is just equal to or less than 256.

Democratic Approach

In the uniform quantization approach described above, for large size images, k is often greater than 10 and the quantization error is quite significant. Therefore, the approach is modified to take into consideration the frequency of occurrence of colours. The selection of colours in this case is democratic.

Step 1: Select 256 most frequently occurring colours

The process in section II A is carried out with k=1. The selected colours are noted. The number of pixels associated with each selected colour is noted as well. The selected colours are arranged in descending order of frequency of occurrence. The most frequently occurring 256 colours are chosen as the selected colours in the colour map p.

Step 2: Associate all pixel colours with the selected colours

The pixels are re-scanned to associate all pixels with the nearest colour in p. For each pixel, k =1 is used and the pixel is compared with all the 256 colours in p. If Eqn (3) is false after comparing with all colours in p, then k is increased by 1 and the process is repeated till the pixel colour is associated with one of the selected 256 colours.

Step 3: Evaluating the process by calculating the psnr

The recovered image w_r obtained from index image y and the colour map p is compared with the original image w. psnr is evaluated.

Step 1 is repeated with the value of k increased by 1 and then steps 2 and 3 are repeated. This is done twenty times. psnr is plotted against values of k used in step 1. The situation that gives the highest psnr is selected as the optimum.

Step 1 is like dividing a population into constituencies and selecting 256 constituencies with the highest population. Step 2 is like fixing each individual in one of the 256 constituencies that is closest to him. Step 3 is like evaluating the dividend of democracy.

In the uniform quantization approach, k is the same for all pixels while in the democratic approach; k varies from pixel to pixel. The quantization error in each pixel

is directly proportional to k. The average quantization error in the democratic approach is found to be less compared with uniform quantization approach.

Decomposition of Gray-Level Image

The matrix y(m x n) obtained is treated as a gray-level image. The gray-level image is decomposed into a series of binary digital images b(m x n x 8) using stack filter's threshold decomposition technique [8]. The technique converts each pixel in y to binary as illustrated in Figure 1. y(1,1) is 201_{10} which is 11001001_2. y(2,1) is 15_{10} which is 00001111_2. A single gray-level image becomes 8 binary images: $b_1, b_2, ..., b_7$ and b_8.

Watermarking Procedure

Figure 2 shows the overall watermarking system. The RGB to index converter and the stack filter have been discussed. The parallel to serial converter converts the binary images to a single bit stream, b. The digital watermarker embeds the bit stream into the host image, h. In the transmission channel or storage, the watermarked image, h_{mkd} may be attacked or corrupted [3,8,15]. The watermark extractor detects and actually extract bit stream, b_r. The host image and a key are required for the extraction.

The bit stream is converted back to binary images: $b_{r1}, b_{r2}, ..., b_{r7}$, and b_{r8}. The inverse stack filter converts the binary images to gray-level image y_r. Finally, y_r and colour map, p are converted to RGB colour recovered watermark, w_r.

Embedding Stage

The host image, h(M x N x 3) is an RGB colour image with MN pixels but there are 3MN possible locations for embedding watermark bits. In other words, the red, green and blue components of h are treated as separate images to host bits. The watermark, w(m x n x 3) has mn pixels and will lead to 8mn bits in the bit stream, b.

Each of the 8mn bits is encoded r times. r is greater than 1 to achieve better robustness. A "1" bit is encoded by adding a coding constant cc to the host pixel intensity and a "0" bit is encoded by subtracting cc from the host pixel intensity. To achieve better robustness cc must not be too small. For better imperceptibility, cc must not be too large. The value of cc should be such as to obtain less than just noticeable difference (JND) between the watermarked image and the host. The peak signal to noise ratio, psnr of watermarked image should be equal or greater than 40dB for better imperceptibility [2]. The normalized cross correlation, NC between watermarked image and host should be close to 1. This also requires that some of the host pixels should be left free in the embedding process. The values of r, cc and the information on the actual pixels carrying watermark bits constitute part of the extraction key.

The Extraction Stage

The corrupted or attacked image is taken as a test image. The host image and the key must be available. Each bit carrying pixel is examined for the presence of a "1" or "0" bit. A decision has to be reached whether the pixel carries a "1" or "0" bit. The r pixels carrying the same bit are compared before deciding whether it is a "1" or "0" bit. Rare cases where the decision reached is doubtful are noted. The percentage of such doubtful cases is evaluated as a measure of reliability of the process and is represented as error in Eqn. (4). Very small error indicates high reliability.

$$error = \frac{no\ of\ times\ decision\ is\ doubtful\ x\ 100}{total\ no\ of\ times\ decision\ is\ made}\ \% \quad (4)$$

The recovered bit stream b_r is eventually converted to recovered watermark w_r. The appearance of w_r, its psnr and the normalized cross correlation (NC) compared with w will show without doubt if the watermark is present in the test image or not. Matlab programs were developed as implementation of the subsystems or blocks. Results of experiments conducted are discussed next.

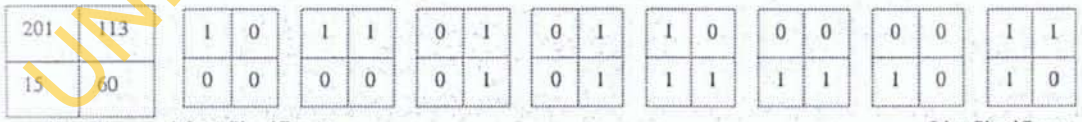


Figure1 Stack Filter's Threshold Decomposition of Gray-Level Image to Binary Images

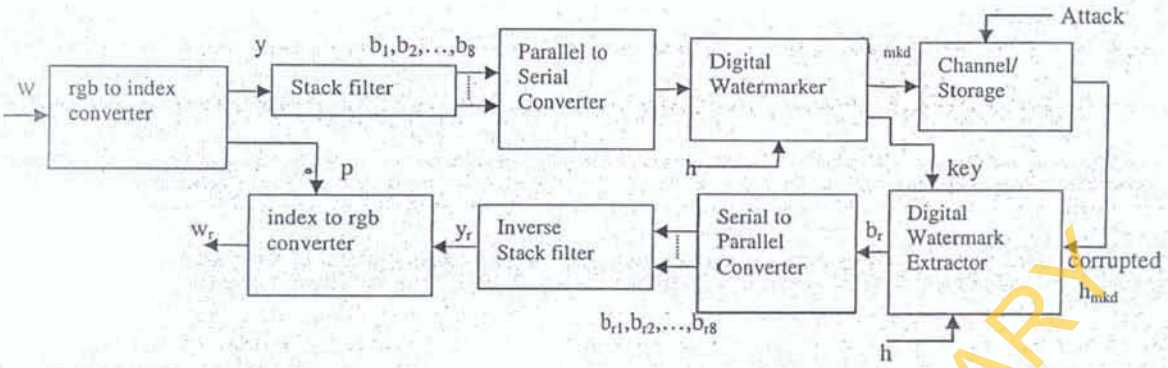


Figure 2 Overall Watermarking System

Results and Discussion

Pre-processing

The algorithm developed for the conversion of RGB image to index image was tested with three images: Mazuda, Goldhill and Baboon [8]. Figure 3 shows the graph of psnr against k (used in step1 of the democratic approach) for the three images. For each image the value of k (step1) that gives the highest psnr is obtainable from Figure 3 and is included in Table 1.

Table 1 and Figure 4 give the comparison of results obtained with the uniform quantization approach and democratic approach for the three images. Democratic approach gave better appearance and higher psnr compared with uniform quantization approach. Furthermore, it is observed that the highest psnr is obtained for Mazuda and the lowest psnr is obtained for Baboon. To account for this trend, concept of frequency estimate is hereby introduced.

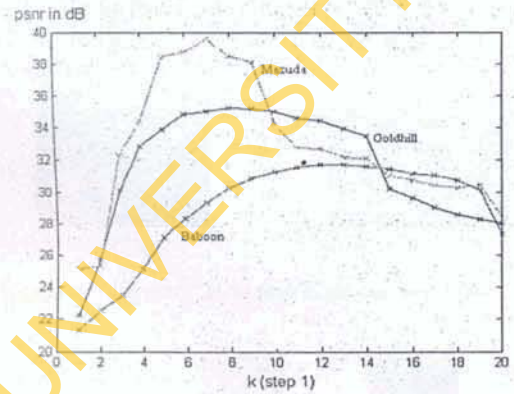


Figure 3 psnr for Different Colour Distribution for Three Images: Mazuda, Goldhill and Baboon

A careful study of the three images reveal the fact that the rate of change of intensity (colour) decreases from Baboon through Goldhill to Mazuda. Therefore, Baboon has the highest spatial frequency while Mazuda has the lowest spatial frequency. For the purpose of comparing images, Eqn. (5) is proposed for the evaluation of frequency estimate of an RGB colour image.

$$freq = \frac{1}{3M(N-1)} f_{rows} + \frac{1}{3N(M-1)} f_{columns} \qquad (5)$$

where $f_{rows} = \sum_{i=1}^{M} \sum_{j=2}^{N} \sum_{t=1}^{3} \left| I(i,j,t) - I(i,j-1,t) \right|$

$$f_{columns} = \sum_{j=1}^{M} \sum_{i=2}^{N} \sum_{t=1}^{3} \left| I(i,j,t) - I(i-1,j,t) \right|$$

The frequency estimates of the three images are evaluated using Eqn. (5) and listed in Table 1. The higher the frequency estimate, the higher the psnr obtained.

Mazuda psnr = 39.55 dB | Goldhill psnr = 35.24 dB | Baboon psnr = 31.71 dB

(a) Democratic Approach Results

Mazuda | Goldhill | Baboon

(b) Original Images

Mazuda psnr = 32.73 dB | Goldhill psnr = 30.21 dB | Baboon psnr = 27.32 dB

(c) Uniform Quantization Approach Results

Figure 4Comparison of Pre-Processing Results Obtained with Democratic Approach and Uniform Quantization Approach

Watermarking

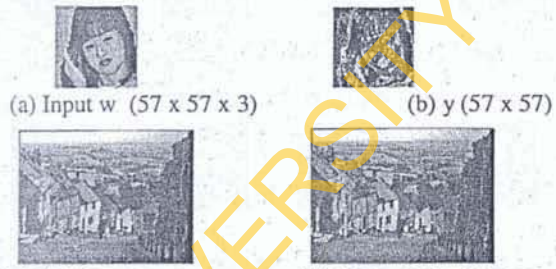
Figure 5(a) shows a watermark, w (57 x 57 x 3) which was converted to index image, w_i. w_i is made of two 2D matrices: gray-level image y (57 x 57) shown in Figure 5(b) and a colour map, p (256 x 3). The Goldhill image (576 x 787 x 3) shown in Figure 5(c) was used as host image in this work. Various watermarks were used for different tests discussed below. Various forms of watermark attacks were considered. The input image w of Figure 5(a) was used as watermark with cc=3 to obtain the watermarked image of Figure 5(d). The psnr of the watermarked image of Figure 5(d) is 41.75 dB and the normalized cross correlation is 0.9962.

Reliability Test

The watermarked image of Figure 5(d) was used as a test image to detect the presence of watermark. The detected watermark shown in Figure 6(a) has psnr of 39.67 dB, NC of 0.9999 and the error is virtually zero.

The host image itself was attacked by compression, zoom-out operation (interpolation) and zoom-in operation (sampling). The attacked host image was used as a test image to detect the presence of watermark. The detected watermark shown in Figure 6(b) has psnr of 9.07 dB, NC of 0.1633 and the error is 1.40%.

Another watermarked image carrying a watermark that is different from that of Figure 5(a) was used as test image to detect the presence of watermark. The detected watermark shown in Figure 6(c) has psnr of 9.42 dB, NC of 0.7271 and the error is virtually zero.



(a) Input w (57 x 57 x 3) (b) y (57 x 57)

(c) Host Image (d) Watermarked Image

Figure 5Watermark, Host and Watermarked Image

(a) psnr = 39.67dB (b) psnr = 9.07dB (c) psnr = 9.42dB

Figure 6 Reliability Test Results

These results confirm the presence of watermark in the first test image and the absence of watermark in the second and third test images. The overall system's performance is satisfactory and reliable.

Robustness against JPEG Compression Attack

The Joint Photographic Experts Group (JPEG) lossy compression is a type of watermark attack. The watermarked image is compressed. The degree of compression is indicated by the quality factor q. The lower the q value, the lower the image size and hence the higher the degree of compression: this is illustrated in Figure 7. Compressed watermarked images with different q values were tested for the presence of watermark. The results are summarized and presented in Figure 8 and Figure 9. The lower the q value, the lower the psnr of attacked watermarked image and detected watermark.

(a) Watermarked Image Original as in Figure5(d) (576x787x3) 799kB

(b) Watermarked Image Compressed **q100** (576x787x3) 454kB

(c) Watermarked Image Compressed **q75** (576x787x3) 86.4kB

Figure 7 Original Watermarked Image and Its Compressed Versions

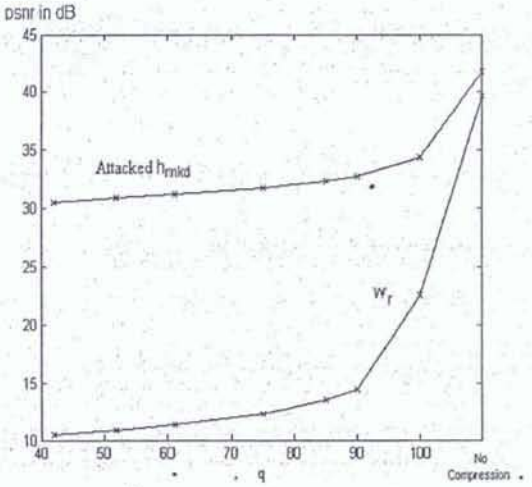


Figure 8psnr of Attacked h_{mkd} and Detected Watermark w_r for Different q Values

Robustness against Watermarked Image Spatial

Size Adjustment

JPEG is used to simulate the second form of attack. For example, the watermarked image spatial size is reduced (sampling) to 75% at q100 from (576 x 787 x 3) to (486 x 700 x 3) and then expanded (interpolation) back to normal spatial size (576 x 787 x 3) at the same q100. This is like zoom-in and zoom-out operation. If the adjustment is indicated as 120%, the watermarked image spatial size is expanded (interpolation) to 120% at q100 from (576 x 787 x 3) to (633 x 860 x 3) and then reduced (sampling) back to normal spatial size (576 x 787 x 3) at the same q100. Attacked watermarked images with different % spatial size adjustment were tested for the presence of watermark. The results are summarized and presented in Figure 10 and Figure 11. The lower the % (percent) spatial size adjustment the lower the psnr of attacked watermarked image and detected watermark.

Table 1 Comparison of pre-processing results obtained with democratic approach and uniform quantization approach

		Democratic Approach	Uniform Quantization Approach
Mazuda (270 x 288 x 3) Frequency Estimate = 3.16	k Psnr NC No of colours	7(for step1) 39.55 dB 0.9994 575	11 32.73 dB 0.9956 246
Goldhill (288 x 394 x 3) Frequency Estimate= 10.53	k Psnr NC No of colours	8(for step1) 35.24 dB 0.9977 925	15 30.21 dB 0.9883 236
Baboon (256 x 256 x 3) Frequency Estimate= 24.45	K Psnr NC No of colours	13(for step1) 31.71 dB 0.9985 668	20 27.32 dB 0.9895 244

Figure 9Detected Watermarks in Compressed Watermarked Images with Different q Values

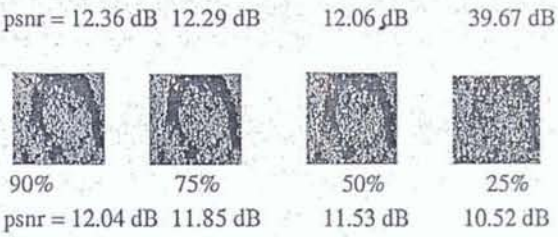


Figure 10 Detected Watermarks in Attacked Watermarked Images Subjected to Different % Spatial Size Adjustment

Effect of Coding Constant on Robustness

Five watermarked images were formed by embedding the watermark of Figure 5(a) in the host image of Figure 5(c) using five different values of coding constant cc. The five watermarked images were subjected to the same

attack; JPEG compression q90. They were screened for the presence of watermark. The results are summarized and presented in Table 2 and Figure 12. The lower the coding constant, cc, the higher the psnr of watermarked image, h_{mkd}; hence the higher the imperceptibility. The higher the coding constant, cc, the higher the psnr of detected watermark: hence the higher the robustness. cc=3 is a good compromise for good imperceptibility and robustness.

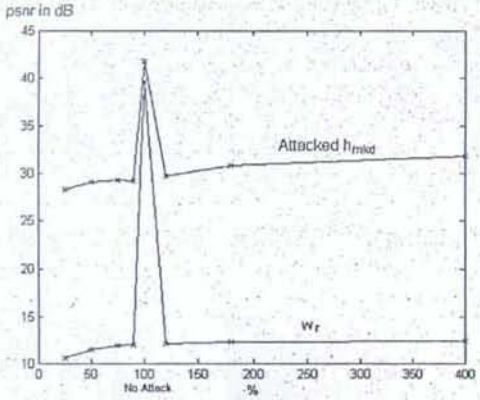


Figure 11 psnr of Attacked h_{mkd} and Detected Watermark w_r for Different % Spatial Size Adjustment.

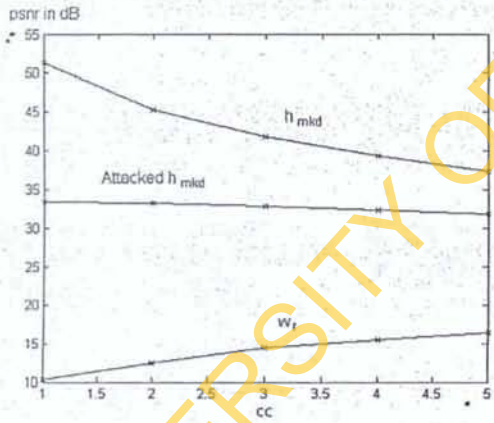


Figure 12 psnr of Watermarked Image, Attacked Watermarked Image and Detected Watermark for Different Values of Coding Constant, cc with **q90** JPEG Compression Attack.

Effect of Number of Watermark Image Pixels on Robustness

Various sizes of watermarks were used to generate watermarked images with cc=3. The watermarked images were subjected to the same attack: q100 JPEG compression. The attacked watermarked images were screened for the presence of watermark. The results are summarized and presented in Figure 13 and Figure 14. It is noticeable that the higher the number of pixels, the lower the imperceptibility and robustness. Better robustness obtained for smaller watermark size is due to higher value of r. Reasonable degree of imperceptibility and robustness limits the capacity: size of watermark.

Table 2 psnr of Watermarked Image, Attacked Watermarked Image And Detected Watermark for Different Values of Coding Constant, cc with **q90** JPEG Compression Attack

cc	psnr of h_{mkd}	psnr of Attacked h_{mkd}	psnr of w_r	Detected Watermark
1	51.25 dB	33.42 dB	10.30 dB	
2	45.25 dB	33.17 dB	12.49 dB	
3	41.75 dB	32.79 dB	14.43 dB	
4	39.27 dB	32.31 dB	15.52 dB	
5	37.34 dB	31.75 dB	16.40 dB	

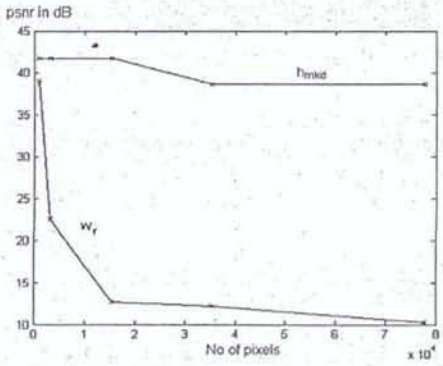


Figure 13 psnr of Watermarked Image Detected Watermark for Different Number of Watermark Image Pixels with **q100** JPEG.

Effect of Watermark Image Frequency on Robustness

Three watermarked images were formed by embedding the watermarks of Figure 15(a) in the host image of Figure 5(c) using cc=3. The three watermarked images were subjected to the same attack; JPEG compression q90. They were screened for the presence of watermark. The results are summarized and presented in

Figure 15(b). The lower the frequency estimate, the higher the robustness.

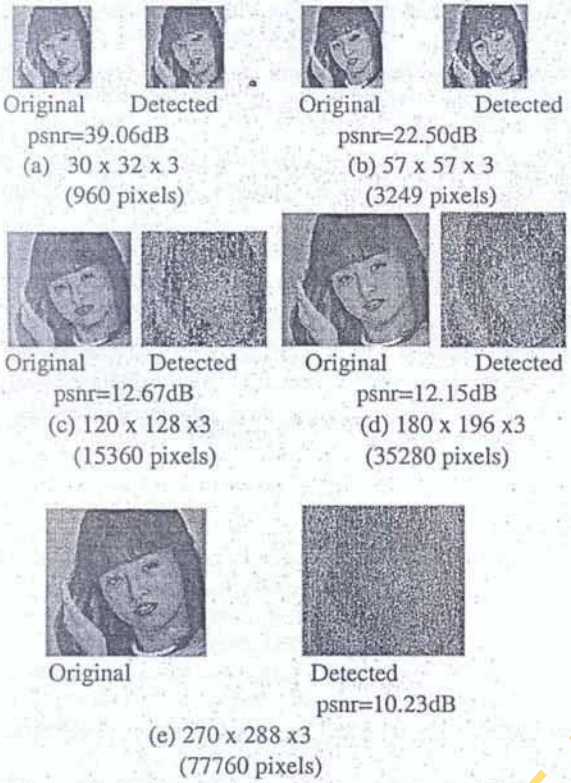


Figure 14 Different Sizes of Watermarks and Detected Watermarks (Different Number of Pixels) with **q100** JPEG Compression Attack.

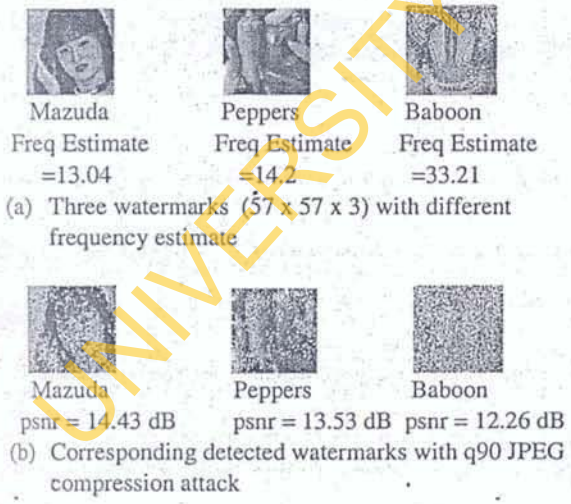
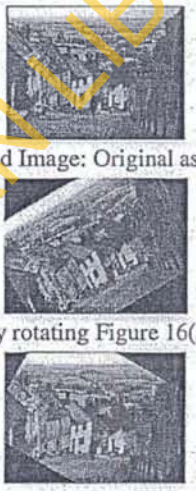


Figure 15 Robustness Against Watermark Image Frequency.

Robustness against Watermarked Image Rotation

Rotation of watermarked image is another form of attack. For example the watermarked image of Figure 16(a) was rotated through angle $\theta=30^{\circ}$ to give the image of Figure 16(b) which was rotated through angle $\theta=-30^{\circ}$ to give the attacked watermarked image of Figure 16(c). Matlab code 'imrotate' was used to simulate this attack. Attacked watermarked images formed using different values of θ were tested for the presence of watermark. The results are summarized and presented in Figure 17. The minimum psnr of detected watermark is 13.50dB.



(a) Watermarked Image: Original as in Figure 5(d)

(b) Obtained by rotating Figure 16(a) through 30°

(c) Obtained by rotating Figure 16(b) through -30° (Attacked Watermarked Image)

Figure 16 Original Watermarked Image and Its Rotated Versions

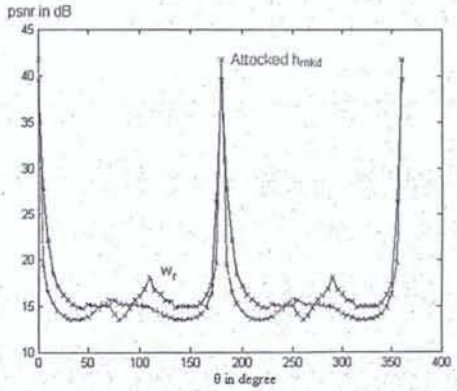


Figure 17 psnr of attacked watermarked image and detected watermark for different values of θ

Conclusions

In this paper, a method of embedding a colour image as digital watermark into a host image is presented. The watermark is first converted from RGB colour space to index image. The index image is decomposed into a series of binary digital images for implementing multiple watermarking.

Experimental results show that the proposed method is robust to reasonable image processing operations and the lossy compression techniques such as JPEG. Furthermore, application of democratic approach in signal sampling is found to produce better signal to noise ratio compared with uniform quantization approach. The results also illustrate the relationship between capacity, imperceptibility and robustness. The method can be applied for secret communication.

References

[1] Barni M., Bartolini F., Rosa A.D. and Piva A. Capacity of full frame DCT image watermarks, IEEE Trans. on Image Processing **9** (8) (2000). p. 1450-1455.

[2] Chen, B. and Wornell, G.W (1998). Digital watermarking and information embedding using dither modulation. *Proc. IEEE Second Workshop on Multimedia Signal Processing*, pp 273-278.

[3] Fei C., Kundur D., and Kwong R.H. Analysis and Design of secure watermark-based authentication systems, IEEE Trans. on Information Forensics and Security **1** (1) (2006). p. 43-55.

[4] Hernandez J.R and Gonzalez F.P. Statistical analysis of watermarking schemes, Proceedings of the IEEE **87** (7) (1999). p. 1142-1166.

[5] Hsu C.T. and Wu J.L. Hidden digital watermarks in images, IEEE Trans. on Image Processing **8** (1) (1999) p. 58-68.

[6] Lu C.S. and Liao H.Y.M. Multipurpose Watermarking for image authentication and Protection, IEEE Trans. on Image Processing **10** (10) (2001) p. 1579-1592.

[7] Mohanty, S.P., Ramakrishnan, K.R. and Kankanhalli, M.S. (2000). A DCT Domain Visible Watermarking Technique for Images. *Proc. of the IEEE International Conference on Multimedia and Expo*II, 1029-1032.

[8] Niu X.M., Lu Z.M., and Ho S.H. Digital watermarking of still images with gray-level watermark, IEEE Trans. on Consumer Electronics **46** (1) (2000). p. 137-144.

[9] Voyatzis G. and Pitas I. The use of watermarks in the protection of digital multimedia products. Proceedings of the IEEE **87** (7) (1999). p. 1197-1207.

[10] Canada, B. and Majumder, D.D. (2000). *Digital Image Processing and Analysis.* Prentice-Hall, Indian. 384p. ISBN 8120316185.

[11] Choy, S.S.O., Chan, Y. and Siu, W. (1996). An Improved Quantitiaive Measure of Image Restoration Quality. *Proc. IEEE International Confeence on Acoustics, Speech and Signal Processing (ICASSP'96)III, 1613-1616*

[12] Gonzalez, R.C. and Woods, R.E. (2002). *Digital Image Processing.* Addison-Wesley, Massachusetts: 793p. ISBN 0201 600781.

[13] Jain A.K. (2003). *Fundamentals of Digital Image Processing.* Prentice-Hall, India: 569p. ISBN 0133 361659.

[14] Weeks A.R. (1999). *Fundamentals of Electronic Image Processing.* Prentice-Hall, India: 576p. ISBN 0780 334108.

[15] Huang, C.H. and Wu J.L. (2001). Inpainting Attacks against Visible Watermarking Schemes *Proc. SPIE, the International Society for Optical Engineering* 4314, 376-384.

[16] USC-SIPI Image Database (2006), Standard Test Images Retrieved on October 5, 2006 from the database of Signal and Image Processing Institute of the University of Southern California, USA: http://sipi.usc.edu/database/index.html.