Color Image Watermarking Using DFT

Ningombam Jimson, Research Scholar, Department of Computer Science, Assam University, Silchar, India, Email: jimson123@gmail.com

Kattamanchi Hemachandran, Professor, Department of Computer Science, Assam University, Silchar, India, Email:khchandran407@gmail.com

Abstract — **Digital watermarking provide copyright protection and information security by adding an information to the cover image. In this paper, a color image watermarking is proposed using DFT in YC$_b$C$_r$ color space. The original RGB image is converted into YCbCr color space to get the luminance information Y and chrominance information (C$_b$, C$_r$). The watermark is embedded in the luminance information, Y. To insert the watermark into Y, first Y is divided into non-overlapping block of 8X8 and the blocks are transform using DFT. Using two pseudo-random noise sequences, the watermark is embedded in the mid and high frequency magnitude of the DFT obtained. To measure the robustness of watermarking scheme we used Peak signal to Noise ratio and Normalized correlation. In watermark extraction, the Watermarked RGB image is converted into YCbCr and luminance information Y is divided into block. The bit is extracted by comparing the correlation between the Pseudorandom Noise sequences with the magnitude block of Y. Experimental results shows that the watermarking scheme is robust against common watermarking attacks.**

Keywords* —RGB, YC$_b$*C$_r$*, *Discrete Fourier Transform (DFT), Peak Signal to Noise ratio (PSNR), Normalized Correlation (NC).

I. INTRODUCTION

The rapid development of computer network and internet has increase the rate in which the digital data in form of image, video and audio are share and duplicated flawlessly without the consent of the content owner, thus violating the copyright and intelligent property. Digital watermarking is considered to the possible solution for the copyright protection of the digital data by adding an extra bit of information to the digital data in such a way that the embedded information become part of the digital data. A digital watermarking consist of two main process—watermark embedding and watermarking extraction or detection. Mathematically, the watermark can be embedded into the cover image either by additive approach or my multiplicative approach as shown in equation (1) and (2). [1]

$$C' = C + \alpha W \qquad (1)$$

$$C' = C(1 + \alpha W) \qquad (2)$$

Where C$^{'}$ and C is the watermarked image and cover image respectively and α is watermark embedding strength.

A watermark can be embedded in spatial domain as well as in the transform domain [1] [2] [3]. In the spatial domain watermarking scheme the value of the image pixels are directly manipulated. Least significant bit substitution [4] [5], patchwork are some of the common watermarking scheme used in the spatial domain. Watermarking in transform domain are more robust than the spatial domain watermarking and the watermark is embedded in the frequency domain using some transformation like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) [1] [6] etc. Robustness, capacity and perceptibility are three important requirement of digital watermarking [3]. Robustness means a watermark should be able to survive malicious or accidental removal attacks. Capacity of the watermarking is the amount of information that can be added to the cover image. Transparency or perceptibility mean addition of watermark should not cause any visual degradation of the cover image in which it is embedded.

A watermark can be visible and invisible based on the nature in which the watermark is encoded to the cover image [1]. A watermark is said to be visible in which the watermark is perceptible along with the cover image. In case of invisible watermarking, the watermark embedded in not visible but can be decoded or extracted using an extraction algorithm. Based on the robustness, a watermark can be robust and fragile. Robust watermarking are those in which the watermark is difficult to remove or survive any watermarking attacks. In case of fragile watermarking, a slight change in the watermarked image results watermark to be destroyed or unreadable. Such kind of watermarking scheme is used for authentication of the digital data. There is blind and non-blind watermarking classified based on how the watermark is detected or extracted. In a blind watermarking, the original cover image or some kind of

DOI : 10.18231/2454-9150.2019.0070

information about the cover image is required for watermark detection whereas in non-blind watermarking scheme, no such information or cover image is required for watermark detection.

II. Theoretical Background

A. YC_bC_r Colour model

YC_bC_r colour model is widely used for video. In this model all the luminance information are store as a single component(Y) and chrominance information are stored as two colour difference components (C_b and C_r) . C_b is the difference between the blue component and reference value and C_r is the difference between the red component and reference value. The YC_bC_r values can be obtained from the RGB colour model using equation 2 [7] [8][13]

$$Y = w_R R + (1 - w_B - w_R) \times G + w_B \times B$$

$$C_b = \frac{0.5}{1 - w_B}(B - Y) \qquad 2$$

$$C_r = \frac{0.5}{1 - w_R}(R - Y)$$

The values for weight are given as $w_R = 0.299$, w_B=0.114, $w_G = 0.587$. The matrix transformation from RGB to YC_bC_r is given as

$$\begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.5 \\ 0.5 & -0.419 & 0.081 \end{pmatrix} \times \begin{pmatrix} R \\ G \\ B \end{pmatrix} \qquad 3$$

The reverse transformation from YC_bC_r to RGB is given as

$$R = Y + \frac{1 - w_R}{0.5} \times C_r$$

$$G = Y - \frac{w_B(1 - w_B) \times C_b - w_R(1 - w_R) \times C_r}{0.5(1 - w_B - w_R)} \qquad 4$$

$$B = Y + \frac{1 - w_B}{0.5} \times C_b$$

In terms of matrix transformation

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1.0 & 0.0 & 1.403 \\ 1.0 & -0.344 & -0.714 \\ 1.0 & 1.733 & 0 \end{pmatrix} \times \begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} \qquad 5$$

B. Discrete Fourier Transform (DFT)

The Fourier transform of an image decompose an image into its sine and cosine component. In Fourier transform each point corresponds to a two dimensional frequency component. Discrete Fourier transform F(u, v) of an image f(x, y) of size M×N is given by [8] [9]

$$F(u,v) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp^{-j2\pi(\frac{xu}{M} + \frac{yv}{N})} \qquad 6$$

An the inverse Fourier transform is given by

$$f(x,y) = \frac{1}{M \times N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) exp^{j2\pi(\frac{ux}{M} + \frac{vy}{N})} \qquad 7$$

The DFT of image produce a complex number value image and can be displayed using the real or the imaginary part of the complex output. The phase P and magnitude M of the DFT is given by

M (u, v) = |F (u, v)|

P (u, v) = ∠ F (u, v)

III. Proposed Scheme

A. Watermark embedding process

The cover image is first decomposed into YC_bC_r format and luminance component Y is used to embed the watermark. In order to embed the watermark, the Y component is divided into non overlapping block of 8X8. Two highly uncorrelated PN sequence (PN1 and PN0) using a secret key is generated and it is used for embedding the watermark into magnitude component of the DFT. A binary watermark is embedded into the Y component using the two pseudorandom noise generated using the following equation

$$C_w(u,v) = \begin{cases} C_o(u,v) + \alpha * PN, & u,v \notin F_L \\ C_o(u,v), & u,v \in F_L \end{cases} \qquad 8$$

Where α is the embedding strength and C_W and C are the watermarked magnitude component and original magnitude component of DFT of luminance component Y. F_L is the lower frequency component of the DFT magnitude. If the watermark bit is 1 then PN1 is used and if the watermark bit is 0 then PN0 is used. After the magnitude component is being modified using the PN sequences, performing the inverse Fourier transform of the modified magnitude and original phase yields new Luminance component Y'. Combining this modified luminance component Y' and original C_b and C_r we get the watermarked image.

B. Watermark Extraction

In the extraction process, we used the same key to generate the highly correlated pseudorandom noise sequences. The watermarked image is decomposed into YC_bC_r format. The luminance component Y is divided into non-overlapping block of 8X8. After the luminance component is divided into blocks, DFT of each block is found out. Correlation between the magnitude component and Pseudorandom noise sequence is component is computed. Suppose PN1 and PN0 are the two pseudorandom noise sequences generated, then the watermark bit is extracted as – if the correlation between PN1 and magnitude is greater than correlation between PN0 and magnitude, then watermark bit is encoded as 1 and vice versa. The scheme is a blind based watermarking scheme in which the original image is not required for watermark

DOI : 10.18231/2454-9150.2019.0070

extraction and the secret key used for generating the PN sequences can passed on as a secret key for the extraction of watermark.

IV. Experimental Results

We used PSNR and NC to measure the robustness of the presented scheme. PSNR is used to measure the invisibility of the watermark on the cover image and NC value is used to determine the similarity between the original and extracted watermark. PSNR is define as[10][11]

$$PSNR = 10\,log\left(\frac{255^2}{MSE}\right) \qquad 8$$

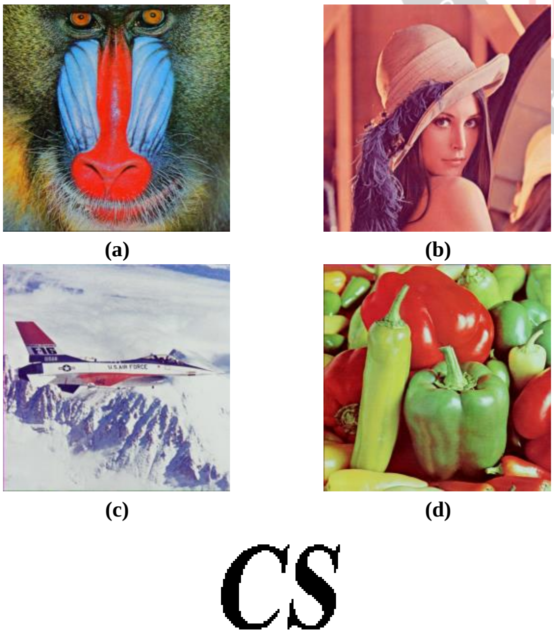
MSE is the mean square error and is calculated using equation 9

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[C(i,j) - C'(i,j)]^2 \qquad 9$$

Where C and C' are the original cover image and watermarked image of size MXN. The formula for calculating normalized correlation value is given by [11]

$$NC(w,w') = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j).w'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w'(i,j)^2}} \qquad 10$$

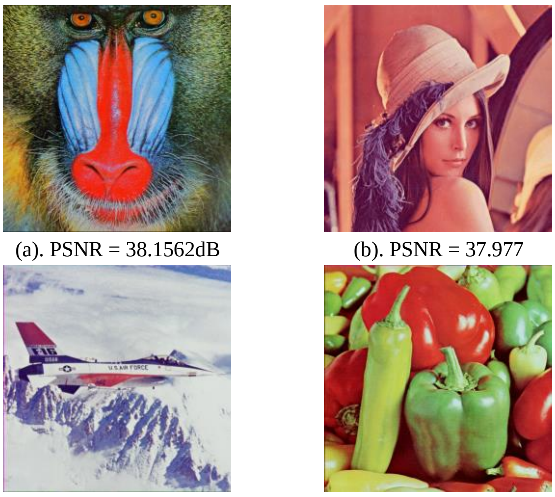
The NC value lies between 0 and 1 if the NC value is 1 then the original and extracted watermark are similar. Higher the NC value better the similarity between the extracted and original watermark. The cover images and watermark image are shown in Figure 1



(a) (b) (c) (d) (e)

Figure 1: Cover images (a-d) and watermark (e)

Keeping the embedding strength α =0. 25, we embed the binary watermark into the cover images used and resultant watermarked images are shown in Figure 2.

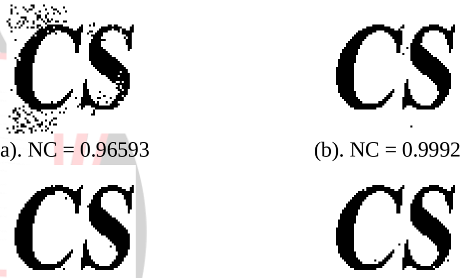


(a). PSNR = 38.1562dB (b). PSNR = 37.977

(c). PSNR = 37.6841 (d). PSNR=37.8873

Figure 2: Watermarked Cover images with PSNR value

Figure 3 shows the corresponding extracted watermark image from the cove images used.



(a). NC = 0.96593 (b). NC = 0.99922

(c). NC = 0.9989 (d). NC=0.99906

Figure 3: Extracted watermark from (a). Baboon (b). Lena (c) Airplane (d). Pepper.

From the results obtained, the watermarking scheme is able to maintain good perceptual quality of the watermarked image and NC value of the extracted watermark is almost 1. In the next part of the robustness testing, we used StirMark benchmarking tools [12] to simulate attacks on watermarked Lena image and corresponding NC value of the extracted watermark are shown in Table 1 below

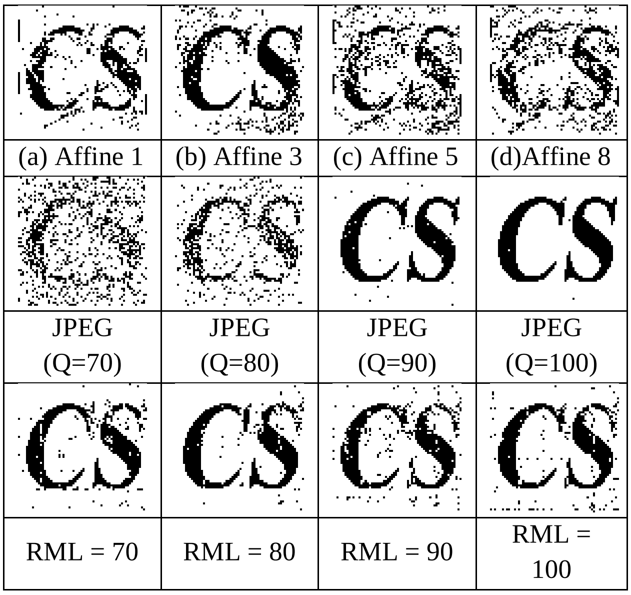
TABLE 1.
PERFORMANCE AGAINST ATTACKS SIMULATED BY STIRMARK BENCHMARKING TOOLS

Attack Type	NC
Affine 1	0.9385
Affine 2	0.8942
Affine 3	0.94146
Affine 4	0.89757
Affine 5	0.87133
Affine 6	0.86502
Affine 7	0.87554
Affine 8	0.87591
JPEG Compression(Q=60)	0.80547
JPEG Compression(Q = 70)	0.84721

DOI : 10.18231/2454-9150.2019.0070

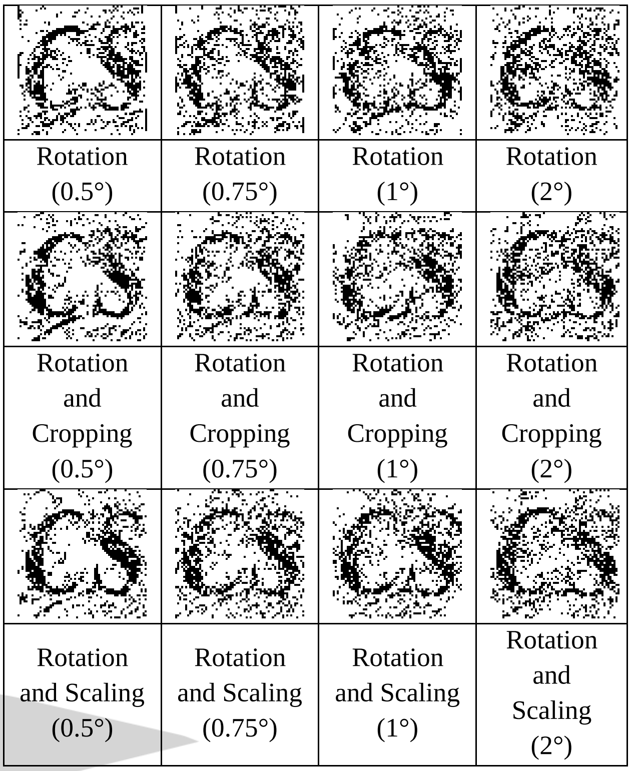
JPEG Compression(Q = 80)	0.91291
JPEG Compression(Q = 90)	0.9931
JPEG Compression(Q = 100)	0.99922
RML =50	0.96676
RML = 60	0.97108
RML = 70	0.97309
RML = 80	0.98077
RML = 90	0.96323
RML = 100	0.97182
Rescaling 75 %	0.92898
Rescaling 90 %	0.94346
Rescaling 110 %	0.99188
Rescaling 150%	0.97678
Rescaling 200%	0.98815
Rotation 0.5°	0.86479
Rotation 0.25°	0.91713
Rotation 0.75°	0.83815
Rotation 1°	0.84288
Rotation 2°	0.82001
Rotation and Cropping 0.5°	0.87796
Rotation and Cropping 0.25°	0.92187
Rotation and Cropping 0.75°	0.84969
Rotation and Cropping 1°	0.84141
Rotation and Cropping 2°	0.82568
Rotation and Scaling 0.5°	0.89249
Rotation and Scaling 0.25°	0.93024
Rotation and Scaling 0.75°	0.85434
Rotation and Scaling 1°	0.85408
Rotation and Scaling 2°	0.83722

From the results obtained as shown in the table, the presented scheme is able to survive most of the common attacks involve in watermarking system except for JPEG compression for which the quality is less than 60. The scheme is also able to survive rotation attacks for an angle up to 2°. The extracted watermark from the watermarked image after undergoing StirMark Benchmarking tool attacks are shown in figure below.


(a) Affine 1 | (b) Affine 3 | (c) Affine 5 | (d)Affine 8

JPEG (Q=70) | JPEG (Q=80) | JPEG (Q=90) | JPEG (Q=100)

RML = 70 | RML = 80 | RML = 90 | RML = 100


Rotation (0.5°) | Rotation (0.75°) | Rotation (1°) | Rotation (2°)

Rotation and Cropping (0.5°) | Rotation and Cropping (0.75°) | Rotation and Cropping (1°) | Rotation and Cropping (2°)

Rotation and Scaling (0.5°) | Rotation and Scaling (0.75°) | Rotation and Scaling (1°) | Rotation and Scaling (2°)

Figure 4: Extracted Watermark after the simulated Attacks using StirMark benchmarking tools.

We can increase the robustness of the watermarking scheme by increasing the embedding strength α. We test our scheme with embedding strength α = 0.25, but the scheme suffer from common image processing attacks like noise addition except Salt and Pepper noise addition. We increase the embedding strength α = 1 and got the PSNR value of watermarked Lena image 25.9916dB. Then we introduce common image processing attacks like salt and pepper, speckle, Gaussian noise addition in our watermarked image and results obtained are shown in Table 2 below

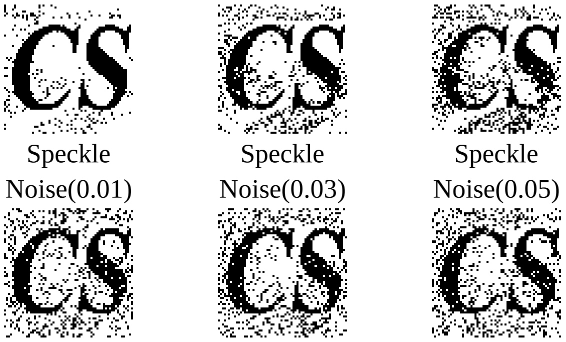
TABLE 2.
PERFORMANCE AGAINST NOISE ADDITION IN WATERMARKED LENA IMAGE.

Attacks	NC
Salt and Pepper Noise(0.01)	0.9653
Salt and Pepper Noise(0.03)	0.9016
Salt and Pepper Noise(0.05)	0.8444
Speckle Noise(0.01)	0.9649
Speckle Noise(0.03)	0.9126
Speckle Noise(0.05)	0.8803
Gaussian Noise(0.01)	0.8915
Gaussian Noise(0.03)	0.8862
Gaussian Noise(0.05)	0.8825

The extracted watermarks after the addition of noise in the watermarked Lena Image are shown in Figure 5

Salt and pepper (0.01) | Salt and pepper (0.03) | Salt and pepper (0.05)

DOI : 10.18231/2454-9150.2019.0070



Speckle Noise(0.01) Speckle Noise(0.03) Speckle Noise(0.05)

Gaussian Noise(0.01) Gaussian Noise(0.03) Gaussian Noise(0.05)

Figure 5: Extracted Watermark after addition of noise in Lena Image.

V. Conclusion

We proposed a color image watermarking scheme in which a binary watermark is embedding in a colored cover image. In the proposed scheme the colored cover image is converted from RGB to YCbCr color space and the watermark is embedded into the luminance component Y. The PSNR value of the watermarked image is directly dependent on the embedding strength using while encoding the binary watermark into the cover image. Increasing the value of the embedding factor decreases the PSNR value of the watermarked image. The scheme survive most of the common watermarking attacks except for the angular rotation as seen from the results obtained. The scheme also suffer from JPEG compression attack as the watermark bit is encoded in the middle and high frequency band of the magnitude of the DFT. Embedding the watermark in the lower component of the magnitude of DFT will affect the perceptual quality of the watermarked image. The scheme also survive noise addition like Salt and Pepper, Speckle Noise addition and Gaussian noise addition. Future work will focus on the making the scheme robust against geometric transformation like rotation with greater angle.

References

[1]. Shih, F. Y. (2017). *Digital watermarking and steganography: fundamentals and techniques*. CRC press.

[2]. Mohanty, S. P., Sengupta, A., Guturu, P., & Kougianos, E. (2017). Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection. *IEEE Consumer Electronics Magazine*, *6*(3), 83-91.

[3]. Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*, *10*, 0471443395.

[4]. Kurak, C., & McHugh, J. (1992, November). A cautionary note on image downgrading. In *[1992] Proceedings Eighth Annual Computer Security Application Conference* (pp. 153-159). IEEE.

[5]. Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE transactions on image processing*, *14*(2), 253-266.

[6]. Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.* (pp. 709-716). IEEE.

[7]. Gonzalez, R. C., & Wintz, P. (1977). Digital image processing(Book). *Reading, Mass., Addison-Wesley Publishing Co., Inc.(Applied Mathematics and Computation*, (13), 451.

[8]. Qidwai, U., & Chen, C. H. (2009). *Digital image processing: an algorithmic approach with MATLAB*. CRC press.

[9]. Ruanaidh, J. J. K. O., Dowling, W. J., & Boland, F. M. (1996, September). Phase watermarking of digital images. In *Image Processing, 1996. Proceedings., International Conference on*(Vol. 3, pp. 239-242). IEEE.

[10]. Voloshynovskiy, S., Pereira, S., Iquise, V., & Pun, T. (2001). Attack modelling: towards a second generation watermarking benchmark. *Signal processing*, *81*(6), 1177-1214.

[11]. Janthawongwilai, K., & Amornraksa, T. (2004, October). Improved performance of amplitude modulation based digital watermarking. In *Communications and Information Technology, 2004. ISCIT 2004. IEEE International Symposium on* (Vol. 1, pp. 318-323). IEEE.

[12]. Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: *Attacks on copyright marking systems*, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15–17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219–239.

[13]. S. Sridhar, (2011). *Digital Image Processing*. Oxford University Press.

DOI : 10.18231/2454-9150.2019.0070