

YCbCr Associated Digital Image Watermarking in the Discrete Cosine Transform Domain

Abdul Rasak Zubair¹, Elijah Oluwatomi Fakeye²

¹Department of Electrical and Electronic Engineering, University of Ibadan, Ibadan, Nigeria

²Department of Electrical and Electronics Engineering, University of Ilorin, Nigeria

(¹ar.zubair@ui.edu.ng, ²tomifakeye4real@gmail.com)

Abstract- The development of a digital watermarking scheme associated with YCbCr color space in the Discrete Cosine Transform (DCT) Domain is presented. The scheme embeds a rgb color watermark in a rgb host image. The Watermark is pre-processed such that it's converted from rgb color space to index image and then to binary bits. The watermark embedding is done only in the Y component of the host in YCbCr color space. The Y component is sub-divided into 8-by-8 blocks of pixels which are transformed to frequency domain using Discrete Cosine Transform (DCT). Hosting Pixels in the DCT 8-by-8 block are classified into regions: Low-Frequency, Middle-Frequency, High-Frequency, Low and Middle-Frequency and the whole 8-by-8 block. The watermarking scheme was subjected to image compression attack and Gaussian noise attack and found to be robust to both attacks. A coding constant $a=5$ is found to produce satisfactory compromise between imperceptibility and robustness. Highest robustness is recorded with watermarking in the Low-Frequency region. This study confirmed that information bits embedded in the Low-Frequency region are more immune to noise and interference. For Compression Quality factor Q less than 50%, the robustness is found to be poor. For Gaussian noise variance greater than 0.002, the robustness is found to be poor. The lower the watermark size the better the robustness. At lower watermark size, watermark bits are encoded more than once to enhance immunity against noise and interference. The proposed YCbCr associated DCT watermarking scheme is found to have a higher robustness, same level of imperceptibility but lower capacity compared with the Spatial Domain watermarking scheme.

Keywords- Color Spaces, Copyright Protection, Discrete Cosine Transform, Noise, Watermarking

I. INTRODUCTION

As illustrated in Fig. 1, Digital watermarking is defined as the hiding of a secret message or information known as watermark within another message known as host and the extraction of the secret message at its destination. Digital watermarking is an active area of research [1, 2, 3, 4, 5, 6, 7, 8,

9, 10, 11, 12]. The objectives of digital watermarking include copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication [13, 14]. Paper watermarking was used in the paper industry in the 18th century in America and Europe as a trademark and a method against counterfeiting. The most famous watermark can be detected holding a bank note against the light [15].

Both the watermark (w) and the host (h) can be audio, image, video or text. A secret key involved in the embedding process will enable the extraction of the watermark at the destination [16]. The host may be required for the detection or extraction of the watermark at the destination. The requirements of a good digital watermarking scheme are imperceptibility, robustness and capacity. Imperceptibility means that effective watermarking should not be perceptible to the observer. It implies that the quality of the watermarked message should not be degraded compared with the host.

A watermarking method is robust if the watermark data embedded into the host content cannot be damaged or removed without destroying the host data itself. Robustness is a measure of the immunity of watermark against various types of attacks [17]. Capacity is the amount of watermark data embedded into the host content. The lower the capacity the higher the imperceptibility and robustness [18]. Visible watermarking scheme where the watermark is visible to the observer is also possible for e-stamp, e-logo and e-label and e-signature [19].

Different watermarking schemes have been developed and are being developed. Cox *et al.* developed a Spread spectrum watermarking algorithm in the Discrete Cosine Transform (DCT) domain using a Gaussian sequence of pseudorandom real numbers of length 1000 as watermark [20]. Rawat *et al.* proposed a watermarking scheme in YCbCr for color host image with a gray scale watermark [21]. Xiong developed a watermarking algorithm which is based on quantization method in three dimensional DCT with a gray scale watermark [22]. Al-Gindy also implemented a watermarking algorithm for color host image in DCT domain with a hand written signature watermark [23]. Zubair, Fakolujo and Rajan proposed a method of embedding a color image as a digital watermark in spatial domain as illustrated in Fig. 2 [24].

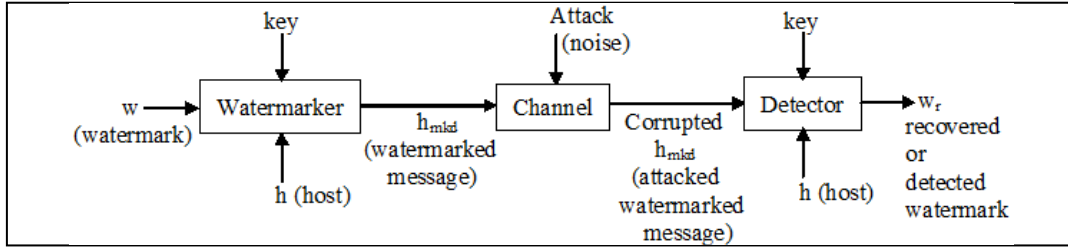


Figure 1. General Framework for Digital Watermarking

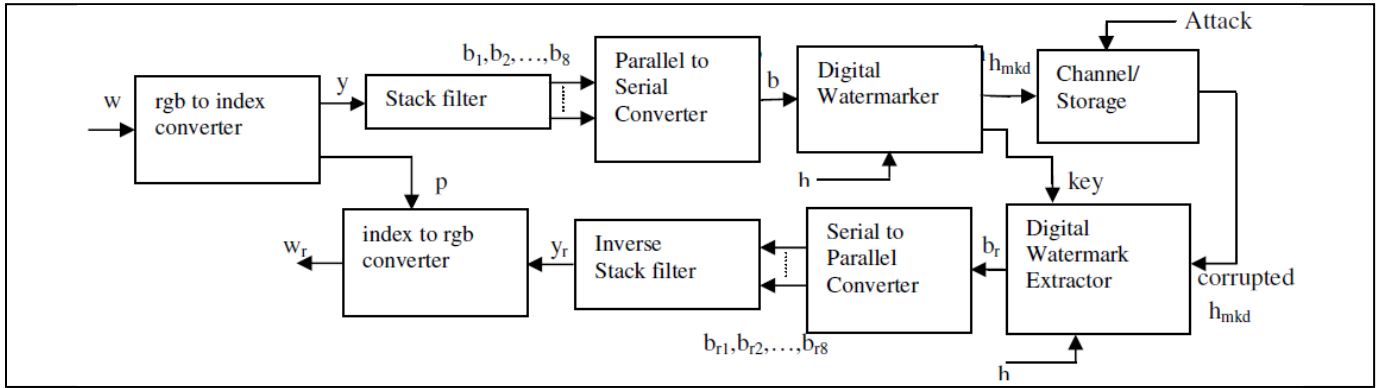


Figure 2. Overall Watermarking System proposed by Zubair, Fakolujo and Rajan [24]

In this work, the spatial domain watermarking scheme of Fig. 2 is subjected to tests in the frequency domain using the Discrete Cosine Transform (DCT). Frequency domain watermarking is considered to be more secured than spatial domain watermarking in the presence of noise [25].

All the blocks in Fig. 2 are implemented as discussed in Zubair, Fakolujo and Rajan (2010) except the Digital Watermarker and the Watermark Extractor which are redesigned to accommodate frequency domain DCT instead of spatial domain and to accommodate YCbCr color space instead of rgb color space. There is a better signal to noise ratio when working with YCbCr color space than with rgb color space [26]. In order to reduce the complexity of the image processing, embedding watermark bits in only the Y luminance component of YCbCr color space is recommended [27].

Color space is a set of rules to facilitate the specification of colors with numbers [27]. The Red-Green-Blue (rgb) color space is the simplest and the most natural color space. Each color is represented by three numbers which indicate the intensities of the primary colors; red, green and blue. rgb color space is an additive color space [28].

The YCbCr color space represents each color with three numbers; similar to the rgb color space. In YCbCr, Y is the brightness (luma) which is very similar to gray version of the original image, Cb is blue minus luma (B-Y) and Cr is red minus luma (R-Y) [29]. The Cb and Cr are the chrominance blue difference and the chrominance red difference respectively. The YCbCr color space focuses on exploiting the human eye properties. rgb can be converted to YCbCr using Eqn. (1) and YCbCr can be converted to rgb using Eqn. (2) [29].

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & 0.071 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} r \\ g \\ b \end{bmatrix} = \begin{bmatrix} 1.164 & 0 & 1.596 \\ 1.164 & -0.391 & -0.813 \\ 1.164 & 2.018 & 0 \end{bmatrix} \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} - \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \quad (2)$$

II. FREQUENCY DOMAIN WATERMARKING SCHEME

A. Watermark Pre-processing

The (m-by-n-by-3) watermark w is converted from rgb to (m-by-n) index image y and (256-by-3) color map p as shown in Fig. 2 [24]. Color map p must be available at the destination as part of the key for watermark extraction. The intensity values in the index image varies from 0 to 255 in decimal which is converted to 8 parallel binary bits b_1, b_2, \dots, b_8 using the stack filter [24]. The parallel bits to a single serial bit b which contains 8mn bits [24]. The serial bit b is used for frequency domain watermarking in the Digital Watermarker.

B. Digital Watermarker

The Digital Watermarker is described with the block diagram of Fig. 3. There are two inputs (h and b) and two outputs (h_{mkd} and key). The (M-by-N-by-3) input host image h is converted from rgb color space to YCbCr color space using Eqn. (1). The luminance component Y is further processed to

give embedded luminance component Y_e which recombines with the C_b and C_r components and gets converted back to rgb color space using Eqn. (2) to give the watermarked image h_{mkd} . Further processing of Y to obtain Y_e includes dividing Y into 8-by-8 blocks of pixels in B as illustrated in Fig. 4(a); transformation of the blocks in B from spatial domain to BB in Discrete Cosine Transform (DCT) frequency domain according to Eqn. (3) [30]; embedding the watermark bits b in the selected pixels in the blocks of BB to form BBe ; application of Inverse Discrete Cosine Transform (IDCT) on the blocks to transform BBe to Be according to Eqns. (4) and (5) [30]; and merging the blocks to give Y_e as illustrated in Fig. 3.

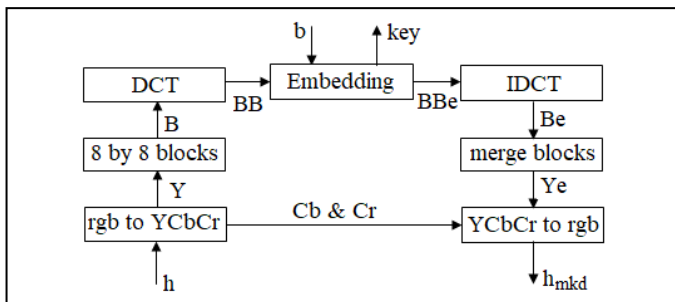


Figure 3. Digital Watermarker.

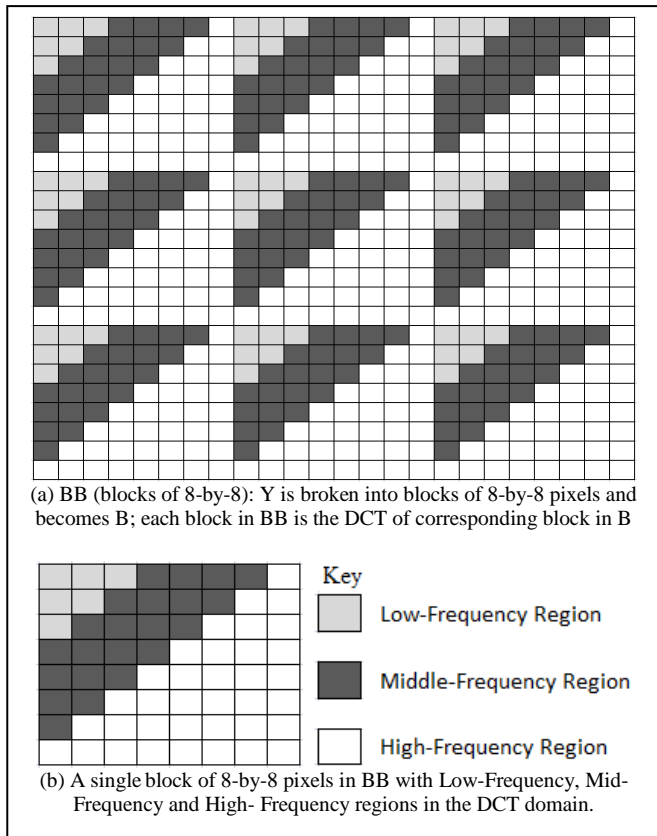


Figure 4. Dividing Y into 8 by 8 blocks of pixels to yield B and DCT version BB .

Each block in B is converted from spatial domain to DCT frequency domain in BB . Each block in BB (DCT frequency domain) has 6 pixels in the Low-Frequency region, 22 pixels in the Middle-Frequency region and 36 pixels in the High-Frequency region as illustrated in Fig. 4(b). Certain pixels in each block are selected to host the bits in the serial bit b ; one hosting pixel hosts one bit. Five combinations of hosting pixels are considered in this work as presented in Table I. There are $8mn$ bits in b . There are $MN/64$ blocks in BB . The number of bits that can be accommodated is given by Eqn. (6). The capacity of the watermarking scheme is given by Eqn. (7). Each bit in b is encoded r times. The higher the number of times the watermark bits is encoded, the greater is the robustness against attack. r is given by Eqn. (8).

TABLE I. FIVE COMBINATIONS OF PIXELS SELECTED TO HOST WATERMARK BITS IN EACH BLOCK

Option X	Description	(S) No of hosting Pixels / block
1	Low-Frequency Region	6
2	Middle-Frequency Region	22
3	High-Frequency Region	36
4	Low & Middle-Frequency Region	28
5	The whole 8-by-8 Block	64

$$BB(u, v) =$$

$$\sum_{x=1}^8 \sum_{y=1}^8 B(x, y) \cos \left[\pi (2x + 1) \frac{u}{16} \right] \cos \left[\pi (2y + 1) \frac{v}{16} \right] \quad (3)$$

$$Be(x, y) =$$

$$\frac{1}{64} \sum_{u=1}^8 \sum_{v=1}^8 \frac{BB(u, v)}{\alpha} \cos \left[\pi (2x + 1) \frac{u}{16} \right] \cos \left[\pi (2y + 1) \frac{v}{16} \right] \quad (4)$$

where

$$\alpha = \begin{cases} 4 & \text{if } u = 1, v = 1 \\ 2 & \text{if } u > 1, v = 1 \\ 2 & \text{if } u = 1, v > 1 \\ 1 & \text{if } u > 1, v > 1 \end{cases} \quad (5)$$

$$\text{No of spaces for bits} = \frac{M}{8} \frac{N}{8} S \quad (6)$$

$$mn \leq \frac{M}{8} \frac{N}{8} \frac{S}{8} \quad (7)$$

$$r = \frac{M}{8m} \frac{N}{8n} \frac{S}{8} \quad (8)$$

The encoding of each bit is described by Eqn. (9). For pixels not selected to host bits, the DCT coefficient in BBe is equal to the corresponding DCT coefficient in BB . For a pixel selected to host the k^{th} bit, the DCT coefficient in BBe is equal

to the corresponding DCT coefficient in BB plus a if b(k) is '1' or minus a if b(k) is '0'. k varies from 1 to 8mn. a is known as coding constant. For better robustness, a must not be too small. For better imperceptibility, a must not be too large [24].

$$BB_e(i, j) = \begin{cases} BB(i, j) + 2ab(k) - a & \text{for hosting pixels} \\ BB(i, j) & \text{for non hosting pixels} \end{cases} \quad (9)$$

The IDCT of Eqns. (4) and (5) are applied to each block in BB_e to convert it to B_e in the spatial domain. The blocks in B_e are merged to form the embedded Y_e which is recombined with C_b and C_r and converted from YCbCr color space to rgb color space with the help of Eqn. (2) to give the watermarked image h_{mkd}. The values of the watermark dimensions (m and n), the coding constant (a), option X, S and r constitute the key which is the second output from the Digital Watermarker. This key will be required in the watermark extraction or detection stage.

C. Attacks on Watermarked Image

The watermarked image (h_{mkd}) may be corrupted during transmission, storage or further processing. Image compression and Gaussian noise are two forms of attack considered in this work. Corrupted h_{mkd} is the result of the attack on watermarked image as illustrated in Fig. 1.

D. Digital Watermark Extractor

The Digital Watermark Extractor or Detector is described with the block diagram of Fig. 5. There are three inputs; the corrupted watermarked image, the host image and the key. The output is the recovered serial bit b_r. The corrupted watermarked image is converted from rgb color space to YCbCr color space using Eqn. (1). The luminance component Y1 is divided into 8-by-8 blocks in B1. The blocks in B1 are transformed to DCT coefficients in BB1. The host image h is also converted from rgb color space to YCbCr color space using Eqn. (1). The luminance component Y2 is divided into 8-by-8 blocks in B2. The blocks in B2 are transformed to DCT coefficients in BB2. BB1 and BB2 are compared for the extraction of recovered bits b_r from the hosting pixels according to information in the key and according to Eqn. (10). Eqn. (10) is applied to only the hosting pixels; the key provide information on the exact locations of the hosting pixels. The r pixels carrying the same bit are compared democratically before deciding if it's a '0' or a '1'. For example, if 2 out of 3 pixels hosting a particular bit result in a '1' and 1 out of 3 pixels hosting the bit results in a '0', the recovered bit is accepted as a '1'. The attack could affect the three hosting pixels differently.

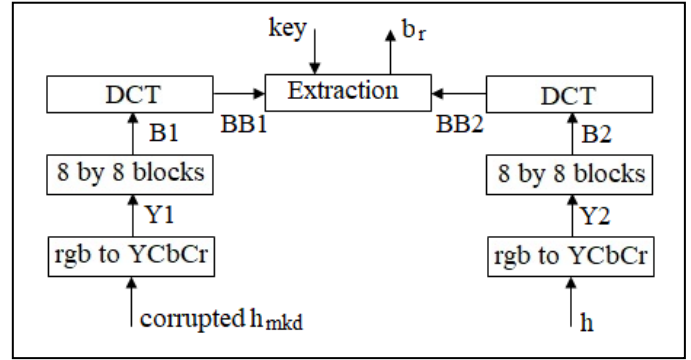


Figure 5. Digital Watermark Extractor.

$$b_r(k) = \begin{cases} 1 & \text{if } (BB1(i, j) - BB2(i, j)) > 0 \\ 0 & \text{if } (BB1(i, j) - BB2(i, j)) < 0 \end{cases} \quad (10)$$

E. Recovered Watermark Processing

After frequency domain watermark extraction in the Digital watermark extractor, the recovered serial bit b_r is converted to parallel binary bits b_{r1}, b_{r2}, ..., b_{r8} which are converted back to recovered (m-by-n) index image y_r. y_r is converted to recovered watermark w_r as illustrated in Fig. 2. The color map p is required in this process as shown in Fig. 2.

F. Performance Metric

The Peak Signal to Noise Ratio (PSNR) is a performance metric used to evaluate the error introduced in an image by an image processing procedure [24]. PSNR₁ of Eqn. (11) compares watermarked image h_{mkd} with the host image h; this is a measure of imperceptibility. The higher the PSNR₁, the higher is the imperceptibility of the watermarking scheme. PSNR₂ of Eqn. (12) compares recovered watermark w_r with the original watermark w; this is a measure of robustness. The higher the PSNR₂, the higher is the robustness of the watermarking scheme against attack. PSNR₃ of Eqn. (13) compares attacked watermarked image (Corrupted h_{mkd}) with host image h; this is a measure of the severity of attack. The lower the PSNR₃, the higher is the severity of attack. At zero or no attack, PSNR₃ is equal to PSNR₁.

All the steps described in section II are coded into computer sub-programs which constitute the developed digital watermarking scheme associated with YCbCr color space in the Discrete Cosine Transform (DCT) Domain. The scheme was subjected to tests.

$$PSNR_1 = 10 \log_{10} \frac{255^2}{\frac{1}{3MN} \sum_{i=1}^M \sum_{j=1}^N \sum_{t=1}^3 (h_{mkd}(i, j, t) - h(i, j, t))^2} \quad (11)$$

$$PSNR_2 = 10 \log_{10} \frac{255^2}{\frac{1}{3mn} \sum_{i=1}^m \sum_{j=1}^n \sum_{t=1}^3 (w_r(i, j, t) - w(i, j, t))^2} \quad (12)$$

$$PSNR_3 = 10 \log_{10} \frac{255^2}{\frac{1}{3MN} \sum_{i=1}^M \sum_{j=1}^N \sum_{t=1}^3 (Corrupted h_{mkd}(i, j, t) - h(i, j, t))^2} \quad (13)$$

III. RESULTS AND DISCUSSIONS

A. Optimum Coding Constant Experiment under no Attack

Digital watermarking and watermark extraction were carried out on five pairs of watermarks and host images with Option $X = 2$ (Middle-Frequency Region) and coding constant $a = 0.1, 0.5, 1, 2, 3, 4, 5,$ and 10 . The watermarked images were not attacked before watermark extraction was carried out. The results are summarised and presented in Table II. The detailed results for Anne (host) and Tosin (watermark) pair ($S/N = 5$ in Table I) are presented in Table III. $PSNR_1$ and $PSNR_2$ are

plotted against coding constant in Fig. 6 for Anne and Tosin pair. The higher the coding constant in Fig. 6, the lower the value of $PSNR_1$ which means the lower the imperceptibility. The higher the coding constant in Fig. 6, the higher the value of $PSNR_2$ which means the higher the robustness. Coding constant $a = 5$ is found to produce satisfactory imperceptibility and robustness. At $a = 5$, $PSNR_1$ is greater than 37 dB for $S/N = 1$ to 5 in Table II and there is perfect watermark recovery with $PSNR_2$ being infinity. $a = 5$ is therefore selected as the optimum coding constant for a trade off between imperceptibility and robustness.

TABLE II. CODING CONSTANT EXPERIMENTAL RESULTS UNDER NO ATTACK
















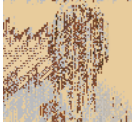












S/N	1		2		3		4		5	
Host										
	Auditorium (512-512-3)		Funke (512-512-3)		Funmi (512-512-3)		Bolu (512-512-3)		Anne (512-512-3)	
Watermark										
	Dami (32-32-3)		Yemi (47-57-3)		Henry (100-100-3)		Wuraola (52-64-3)		Tosin (39-56-3)	
Coding Constant a	$PSNR_1$ (dB)	$PSNR_2$ (dB)	$PSNR_1$ (dB)	$PSNR_2$ (dB)	$PSNR_1$ (dB)	$PSNR_2$ (dB)	$PSNR_1$ (dB)	$PSNR_2$ (dB)	$PSNR_1$ (dB)	$PSNR_2$ (dB)
0.1	52.17	14.90	52.12	7.41	52.26	12.50	52.36	9.60	51.98	8.81
0.5	51.02	23.75	50.93	16.17	51.08	15.44	51.23	16.44	50.93	9.43
1	48.39	∞	48.37	∞	48.58	40.62	48.55	∞	48.31	17.59
2	44.38	∞	44.50	∞	44.44	∞	44.59	∞	44.46	35.10
3	41.41	∞	41.53	∞	41.46	∞	41.61	∞	41.53	∞
4	39.11	∞	39.24	∞	39.14	∞	39.31	∞	39.26	∞
5	37.29	∞	37.41	∞	37.35	∞	37.49	∞	37.44	∞
10	31.46	∞	31.53	∞	31.55	∞	31.62	∞	31.59	∞

TABLE III. CODING CONSTANT EXPERIMENTAL RESULT DETAILS FOR ANNE AND TOSIN PAIR

Host		Watermarked Image		Watermarked Image	
					
Anne (512-512-3)		a=0.1; PSNR ₁ = 52.26dB		a=0.5; PSNR ₁ = 51.08 dB	
	Tosin (Original Watermark) w (100-100-3)		Recovered Watermark w _r PSNR ₂ = 12.50 dB		Recovered Watermark w _r PSNR ₂ = 15.44 dB
Watermarked Image		Watermarked Image		Watermarked Image	
					
a=1; PSNR ₁ =48.58 dB		a=2; PSNR ₁ = 44.44 dB		a=3; PSNR ₁ = 41.46 dB	
	Recovered Watermark w _r , PSNR ₂ = 40.62 dB		Recovered Watermark w _r , PSNR ₂ =∞ dB		Recovered Watermark w _r , PSNR ₂ = ∞ dB
Watermarked Image		Watermarked Image		Watermarked Image	
					
a=4; PSNR ₁ =39.14 dB		a=5; PSNR ₁ =37.35 dB		a=10; PSNR ₁ =31.55 dB	
	Recovered Watermark w _r , PSNR ₂ = ∞ dB		Recovered Watermark w _r , PSNR ₂ = ∞ dB		Recovered Watermark w _r , PSNR ₂ = ∞ dB

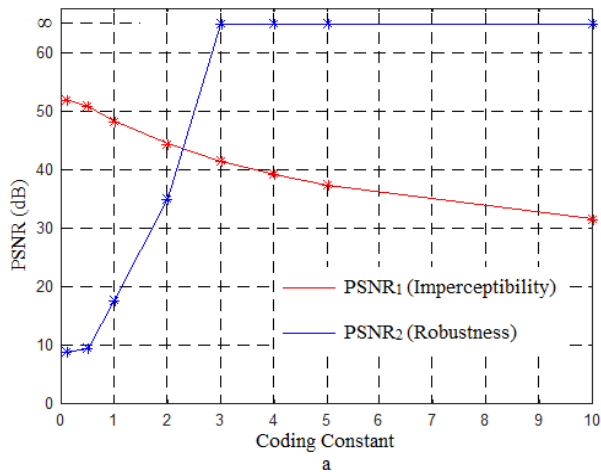


Figure 6. Variation of PSNR₁ and PSNR₂ with Coding Constant for Anne and Tosin pair

TABLE IV. ROBUSTNESS OF WATERMARKING USING THE FIVE REGIONS OF HOSTING PIXELS

Option X	1		2		3		4		5	
	Low-Frequency Region	Middle-Frequency Region	High-Frequency Region	Low & Middle-Freq. Region	The whole 8-by-8 Block	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	
Attack	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)
No Attack	42.59	∞	37.32	∞	39.55	∞	36.35	∞	32.87	∞
Compression Q100	41.10	∞	36.81	∞	38.74	∞	35.94	∞	32.67	∞
Compression Q80	36.17	∞	34.18	∞	36.89	14.90	33.70	∞	33.41	14.64
Compression Q70	34.93	44.20	33.75	22.22	35.58	14.90	33.25	31.28	33.15	14.27
Compression Q60	34.05	34.51	33.53	15.67	34.65	14.90	33.04	20.70	32.97	13.83
Compression Q50	33.42	21.70	33.25	13.20	33.90	14.90	32.80	15.96	32.75	13.57
Compression Q40	32.81	15.69	32.75	12.79	33.18	14.90	32.40	13.47	32.37	13.12
Compression Q20	30.66	12.95	30.70	12.73	30.83	14.90	30.54	13.22	30.53	12.60

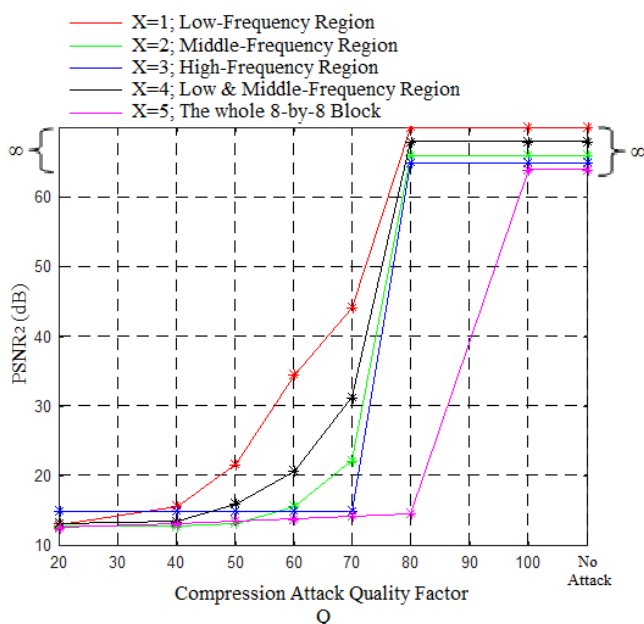


Figure 7. Comparison of PSNR₂ (Robustness against compression attack) for watermarking in the five regions

B. Robustness Against Compression Attack

The aim of Image compression is to reduce the size of an image before storage and or transmission. The benefit is reduction in the cost of bandwidth, storage and transmission. Image compression constitutes attack on watermarked image [31, 32].

Digital watermarking and watermark extraction were carried out with Blessing as host and Dami as watermark using coding constant $a=5$ and option $X=1, 2, 3, 4,$ and 5 . The watermarked images were subjected to image compression attack with Quality factor $Q=100, 80, 70, 60, 50, 40,$ and 20 before watermark extraction. The lower the Quality factor Q , the higher the degree of compression, the less the quality of the compressed image and the lower the image file size in kB. The results are summarised and presented in Table IV. PSNR₂ (Robustness) for watermarking in the five regions are plotted against Compression Quality factor Q as shown in Fig. 7.

Watermarking in the Low-Frequency region ($X=1$) recorded the highest robustness followed by Low & Middle-Frequency region ($X=4$). Robustness recorded in the Middle-Frequency region ($X=2$) is smaller compared with regions ($X=1$ and 4) but better than the other two regions ($X=3$ and 5). Low-Frequency region ($X=1$) watermarking has the lowest capacity as there are only six hosting pixels per 8-by-8 block. The capacity of the Low & Middle-Frequency region ($X=4$) watermarking is higher as there are twenty-eight hosting pixels per 8-by-8 block.

The detailed results of watermarking in the Middle-Frequency region ($X=2$) are presented in Table V and the corresponding graphs of Robustness (PSNR₂) and Severity of attack (PSNR₃) against Compression Quality factor Q are shown in Fig. 8. The higher the severity of attack the lower the robustness. For Compression Quality factor Q less than 50%, the robustness is poor.



















C. Robustness Against Gaussian Noise Attack

Gaussian noise attack adds statistical noise with different values of variance to the watermarked image to corrupt the watermarked image [31, 32]. Digital watermarking and watermark extraction were carried out with Blessing as host

using coding constant $a=5$ and Option $X=1$ (Low-Frequency region). Four watermarks of different sizes were used one after the other. The watermarked images were subjected to Gaussian noise attack with values of noise variance ranging from 0.001 to 0.009 before watermark extraction. The results are summarised and presented in Table VI. Robustness reduces as watermark size increases. The

improved robustness at lower watermark size is due to the fact that a watermark bit can be embedded more than once to increase the chance for detection of the bit in the presence of attack. With Dami as watermark, the graphs of Robustness ($PSNR_2$) and Severity of attack ($PSNR_3$) against Noise variance are shown in Fig. 9. For Gaussian noise variance greater than 0.002, the robustness is poor.

TABLE V. ROBUSTNESS RESULTS IN THE MIDDLE-FREQUENCY REGION ($X=2$).

Host		Watermarked Image		Attacked Watermarked Image	
					
	Dami (Original Watermark) w (32-32-3)		Recovered Watermark w_r $PSNR_2 = \infty$ dB		Recovered Watermark w_r $PSNR_2 = \infty$ dB
Attacked Watermarked Image		Attacked Watermarked Image		Attacked Watermarked Image	
					
	Recovered Watermark w_r $PSNR_2 = \infty$ dB		Recovered Watermark w_r $PSNR_2=44.20$ dB		Recovered Watermark w_r $PSNR_2 = 34.51$ dB
Attacked Watermarked Image		Attacked Watermarked Image		Attacked Watermarked Image	
					
	Recovered Watermark w_r $PSNR_2 = 21.70$ dB		Recovered Watermark w_r $PSNR_2 = 15.69$ dB		Recovered Watermark w_r $PSNR_2=12.95$ dB

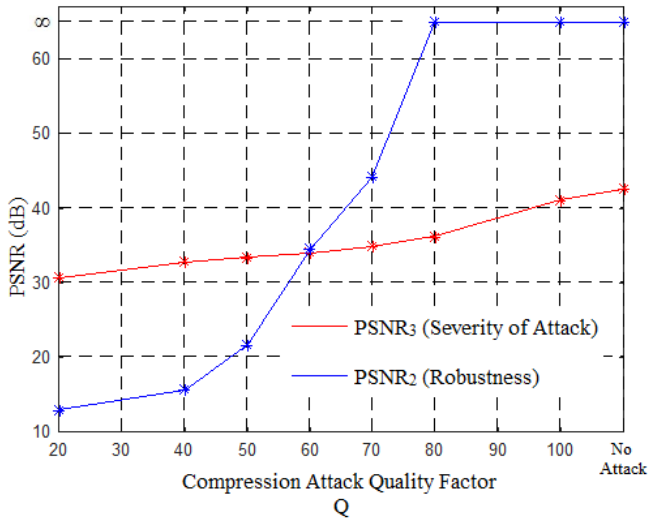


Figure 8. Severity of attack and Robustness against Compression Quality factor Q (Middle-Frequency Region X=2)

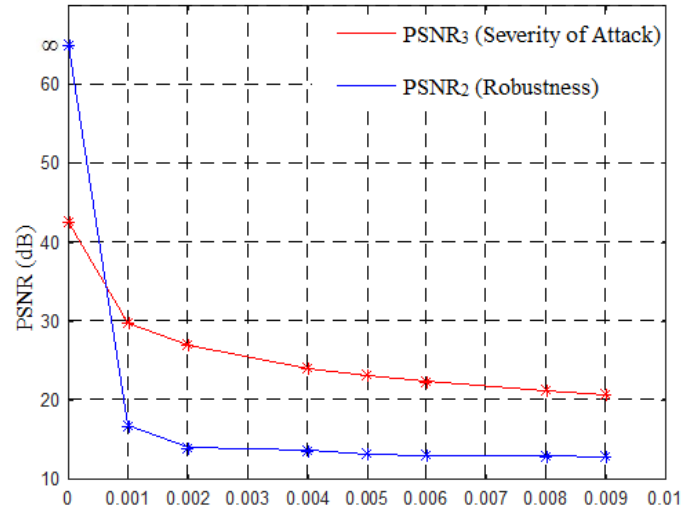


Figure 9. Severity of attack and Robustness against Gaussian noise variance with Dami as watermark

TABLE VI. ROBUSTNESS AGAINST GAUSSIAN NOISE ATTACK

Watermark size	Tope (4-4-3)		Kola (8-8-3)		Henry (16-16-3)		Dami (32-32-3)	
	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)	PSNR ₂ (dB)	PSNR ₃ (dB)
With no Attack	42.67	∞	42.57	∞	42.56	∞	42.59	∞
With Gaussian noise 0.001	29.84	∞	29.84	∞	29.83	25.49	29.84	16.77
With Gaussian noise 0.002	26.98	∞	26.98	∞	26.97	16.51	26.97	13.97
With Gaussian noise 0.004	24.09	∞	24.09	26.96	24.08	13.30	24.07	13.61
With Gaussian noise 0.005	23.17	∞	23.16	21.99	23.16	12.27	23.16	13.15
With Gaussian noise 0.006	22.41	∞	22.40	21.90	22.40	11.67	22.40	13.01
With Gaussian noise 0.008	21.23	∞	21.20	21.42	21.20	11.34	21.21	12.91
With Gaussian noise 0.009	20.74	19.88	20.74	21.18	20.72	11.31	20.73	12.83

D. Comparison between Spatial Domain and YCbCr Associated DCT Watermarking Schemes

The imperceptibility results for the Spatial Domain Watermarking [24] and the YCbCr associated DCT Watermarking schemes are compared in Table VII. The second column of Table VII is from the work of Zubair,

Fakolujo and Rajan [24]. The third column of Table VII is from Table II of this paper. The two schemes recorded approximately the same level of imperceptibility.

The robustness results for the Spatial Domain Watermarking [24] and the YCbCr associated DCT Watermarking schemes against compression attack are

compared in Table VIII. The robustness results for the Spatial Domain Watermarking scheme can be found in Fig. 9 in the work of Zubair, Fakolujo and Rajan [24]. The robustness results for the YCbCr associated DCT Watermarking scheme are from Table IV of this paper. The comparison is presented in graphical form in Fig. 10. The YCbCr associated DCT scheme recorded higher robustness compared with Spatial Domain scheme.

The capacity of the YCbCr associated DCT scheme is smaller than that of the Spatial Domain scheme. Two reasons are accountable for this. Firstly, the host in the Spatial Domain Scheme can host watermark bits in the three components (r, g, and b) while the host in the YCbCr associated DCT scheme can host watermark bits in the Y component only. Secondly, every pixel in the host in the Spatial Domain Scheme is a

potential hosting pixel for watermark bit while more than half of the pixels belonging to the high-frequency region can not host watermark bits in the YCbCr associated DCT scheme.

TABLE VII. COMPARISON OF THE IMPERCEPTIBILITY OF THE SPATIAL DOMAIN [24] AND THE YCbCr ASSOCIATED DCT WATERMARKING SCHEMES

Coding Constant a	Spatial Domain Scheme [24] Imperceptibility (dB)	YCbCr DCT Scheme Imperceptibility (dB)
1	51.25	48.39
2	45.25	44.38
3	41.75	41.41
4	39.27	39.11
5	37.34	37.29

TABLE VIII. COMPARISON OF THE ROBUSTNESS OF THE SPATIAL DOMAIN [24] AND THE YCbCr ASSOCIATED DCT WATERMARKING SCHEMES AGAINST COMPRESSION ATTACK

YCbCr DCT Scheme			Spatial Domain Scheme [24]	
Option X	X = 1	X = 4		
	Low-Frequency Region	Low & Middle-Frequency Region		
Compression Attack	Robustness (dB)	Robustness (dB)	Compression Attack	Robustness (dB)
Compression Q100	∞	∞	Compression Q100	22.50
Compression Q80	∞	∞	Compression Q90	14.43
Compression Q70	44.20	31.28	Compression Q85	13.55
Compression Q60	34.51	20.70	Compression Q75	12.27
Compression Q50	21.70	15.96	Compression Q61	11.39
Compression Q40	15.69	13.47	Compression Q52	10.90
Compression Q20	12.95	13.22	Compression Q42	10.40

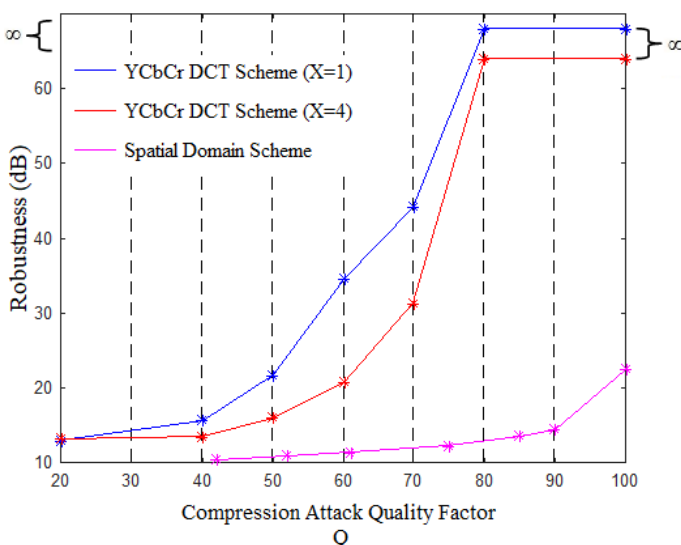


Figure 10. Comparison of the Robustness of the Spatial Domain [24] and the YCbCr associated DCT Watermarking schemes against compression attack.

IV. CONCLUSION

A digital watermarking scheme associated with YCbCr color space in the Discrete Cosine Transform Domain (DCT) has been developed. Both the host and watermark are rgb images. The scheme involves the conversion of the host from rgb color space to YCbCr color space. The Y (Luminous) component is grouped into 8-by-8 blocks which are transformed into frequency domain with Discrete Cosine Transform (DCT). Watermark is converted from rgb image to index image and then to binary bits. The watermark bits are embedded in certain hosting pixels in the frequency domain.

The proposed technique is found to be robust to image compression attack and Gaussian noise attack. A coding constant $a = 5$ is found to produce satisfactory compromise between imperceptibility and robustness. Experimental results show that highest robustness is recorded when watermark bits are embedded in the Low-Frequency region of the DCT 8-by-8 block of pixels. For Compression Quality factor Q less than 50%, the robustness is poor. For Gaussian noise variance greater than 0.002, the robustness is poor. The lower the watermark size the better the robustness.

The YCbCr associated DCT scheme is found to have higher robustness compared with Spatial Domain scheme. The capacity of the YCbCr associated DCT scheme is smaller compared with the digital watermarking scheme in the spatial domain. A sacrifice in capacity yielded improvement in Robustness. The two schemes recorded approximately the same level of imperceptibility.

REFERENCES

- [1] M. Abbasfard, "Digital Image Watermarking Robustness: A comparative Study," M.Eng. Thesis submitted to Computer Engineering Laboratory, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology Netherlands, 2009.
- [2] T. Hai, N. A. Ahmed, Z. J. Mohamad and L. Chongmin "Robust Image Watermarking Theories and Techniques: A Review," Journal of Applied Research and Technology, vol. 12, no. 1, pp. 123–129, 2014.
- [3] S. A. Indrebi and M. S. Sddiet, "Watermarking Digital images: A Hybrid approach," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 5, pp. 25–29, 2015.
- [4] K. Chaitanya, E. S. Reddy and K. G. Rao, "Digital Color Image Watermarking using DWT/DCT Coefficients in RGB Planes," Global Journal of Computer Science and Technology, vol. 13, no. 5, pp. 51–56, 2013.
- [5] H. Ensaf and A. Mohamed, "Digital Watermarking Technique, Application and Attacks applied to Digital media: A survey," International Journal of Engineering Research and Technology, vol. 1, no. 7, pp. 168–175, 2012.
- [6] D. Mohan and S. Devshiri, "A review paper on Digital watermarking," International Journal of Emerging Trends and Technology, vol. 3, no. 4, pp. 99–105, 2014.
- [7] S. P. Mohanty, Digital Watermarking : A Tutorial Review. 1999.
- [8] S. P. Mohanty, K. R. Ramakrishnan and M. S. Kankanhalli, "A DCT Domain Visible Watermarking Technique for Images," Proc. of the IEEE International Conference on Multimedia and Expo, pp. 1029–1032, 2000.
- [9] X. M. Niu, Z. M. Lu and S. H. Ho, "Digital Watermarking of Still Images with Gray-Level Watermark," IEEE Trans. on Consumer Electronics, vol. 46, no. 1, pp. 137–144, 2000.
- [10] C. S. Lu and H. Y. M. Liao, "Multipurpose Watermarking for image authentication and Protection," IEEE Trans. on Image Processing, vol. 10, no. 10, pp. 1579–1592, 2001.
- [11] C. Fei, D. Kundur and R. H. Kwong, "Analysis and Design of Secure Watermark-Based Authentication Systems," IEEE Trans. on Information Forensics and Security, vol. 1, no. 1, pp. 43–55, 2006.
- [12] J. R. Hernandez and F. P. Gonzalez, "Statistical Analysis of Watermarking Schemes," Proc. of the IEEE, vol. 87, no. 7, pp. 1142–1166, 1999.
- [13] P. Yusuf, P. Firoj and P. Asif, "An adaptive watermarking technique for the copyright of digital images and digital image protection," International Journal of Multimedia and Its Applications, vol. 4, no. 2, pp. 21–38, 2012.
- [14] D. Vaishnavi and T. S. Subashini, "Robust and Invisible image watermarking in RGB colour space using SVD," International Conference on Information and Communication Technology, vol. 46, no. 1, pp. 220–226, 2015.
- [15] J. Seitz, Digital Watermarking for Digital Media. London: Idea Group Inc., 2005.
- [16] C. Gunjan, "Information Hiding, Steganography and watermarking: A comparative study," International Journal of Advanced Research in Computer Science, vol. 4, no. 4, pp. 165–171, 2013.
- [17] K. Randeep and K. Kamaljit, "Gray scale image watermark," International Journal of Computers and Technology, vol. 3, no. 1, pp. 101–106, 2012.
- [18] M. Barni, F. Bartolini, A. De Rosa and A. Piva, "Capacity of full frame DCT image watermarks," IEEE Transactions on Image Processing, vol. 9, no. 8, pp. 1450–1455, 2000.
- [19] A. R. Zubair, "Digital Watermarking Algorithms for Visible Watermarks," African Journal of Computing & ICT., vol. 11, no. 2, pp. 24–36, 2018.
- [20] I. J. Cox, J. Kilian, T. Leighton and T. G. Shamoan, "Secure Spread Spectrum watermarking for multimedia," IEEE Transaction on Image Processing, vol. 1, no. 4, pp. 1673–1687, 1997.
- [21] S. Rawat and S. Tomar, "Digital watermarking scheme for authorization against copying or piracy of colour images," International Journal of Computer Science and Engineering, vol. 1, no. 4, pp. 295–300, 2010.
- [22] X. Xiong, "A new Robust Colour Image Watermarking Scheme based on 3D-DCT," World Journal of Engineering and Technology, pp. 177–183, 2015.
- [23] A. M. Al-Gindy, "Design and Analysis of Discrete Cosine Transform-Based Watermarking Algorithms for Digital Images," International journal of advanced research in computer Engineering and technology, Bradford, 2011.
- [24] A. R. Zubair, O. A. Fakolujo and P. K. Rajan, "Digital Watermarking of Still Images with Colour Digital Watermark," Journal of Science Research, vol. 9, pp. 33–41, 2010.
- [25] R. Hashita, K. Ashwani and K. Santendra, "Robust Digital Image watermarking scheme for copyright protection," International Journal of Computer Application, vol. 75, no. 18, pp. 27–32, 2013.
- [26] Y. Qing, L. Jiebo and J. Rajan, "Image processing method for reducing noise and blocking artifact in a digital Image," New York, USA: Google Patents, 2003.
- [27] N. John, A. Viswanath, V. Sowmya and K. P. Soman, "Analysis of various color space models on effective single image super resolution. Advances in Intelligent Systems and Computing," International Symposium on Intelligent Systems Technologies and Applications (ISTA-15) , vol. 384, pp. 529–540, 2016.
- [28] R. Gonzalo and L. P. Jose, Essential Guide to Image Processing, 2nd edition, University of Tennessee, Austin, Texas, 2005.
- [29] H. G. Schaathum, "The DCT domain and JPEG-CSM25 Secure Information Hiding," International Journal of Information of Computer Science and Its Application, pp. 28–33, 2009.
- [30] G. A. Jullien and V. Dimitrov, "Two-Dimensional Transforms Using Number Theoretic Techniques," In: Computer Techniques and Algorithms in Digital Signal Processing, London: Academic Press Limited, 155–210, 1996.
- [31] A. M. A. Hassan, "Robust Digital Image Watermarking Using Repetition Codes Against Common Attacks," A thesis report for the Degree of Master of Computer Science (Information Security), Universiti Tun Hussein Onn Malaysia, 2015.
- [32] C. Song, S. Sudirman, M. Merabti and D. Llewellyn-Jones, "Analysis of digital image watermark attacks," Proceedings of the 7th IEE in conference on Consumer Communications and Networking Conference, IEEE Press, pp. 941–945, 2010.

How to Cite this Article:

Zubair, A. R. & Fakeye, E. O. (2020). YCbCr Associated Digital Image Watermarking in the Discrete Cosine Transform Domain. International Journal of Science and Engineering Investigations (IJSEI), 9(101), 12-22. <http://www.ijsei.com/papers/ijsei-910120-02.pdf>

