I.J. Image, Graphics and Signal Processing, **2017, 9, 40-50**
Published Online September 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2017.09.05

An Improved DCT based Image Watermarking Robust Against JPEG Compression and Other Attacks

Soumik Das
Computer Science & Engineering, Jadavpur University, Kolkata, West Bengal - India
Email: soumikdas.techno@yahoo.co.in

Monalisa Banerjee and
Master of Computer Application, Techno India Salt Lake, West Bengal – India,
Email: monalisa_erjee@yahoo.com

Prof. Atal Chaudhuri
Computer Science & Engineering, Jadavpur University, Kolkata, West Bengal – India,
Email: atalc23@gmail.com

Received: 19 May 2017; Accepted: 11 June 2017; Published: 08 September 2017

***Abstract*—**Rapid growth of internet service attains better security of multimedia contents now a days. Heading this problem a DCT-based color image watermarking framework is proposed in this article. Many earlier works have suggested embedding watermark information in the low frequencies of the image to enhance the robustness against JPEG compression because low frequencies hold the most significant information of the image and not affected significantly by the quantization method of JPEG algorithm. Replacement of low-frequency components with watermark directly may incur undesirable degradation to the image quality. To preserve the visual quality of watermarked images, we are proposing a watermarking framework that adjusts the DCT low-frequency coefficients by scaled averaging. The security issue is well-taken care with double secret keys. Experimental result set demonstrates that the embedded watermark can be extracted efficiently from the JPEG-compressed images even after very high compression, re-watermarking, other image processing attacks. The extraction algorithm is blind i.e., neither host image nor the watermark is needed at the time of extraction.

***Index Terms*—**Image security, ownership, authentication, invisible watermarking, DCT, JPEG compression, re-watermarking

I. INTRODUCTION

Ownership authentication and copyright protection of image have achieved broad attention with the easy availability of internet services and technological advancements of peripherals. Illegal copying and misappropriation of digital image lead cyber crime. Digital watermarking is one of the valid solutions towards the problem of image copyright protection and ownership authentication. For last 20 years, a number of researchers have proposed several frameworks on this area of interest. The following points should be considered while designing an invisible image watermarking framework—

- In the watermarked image, the watermark should be perceptually invisible to human visual system (HVS).
- The watermarked image quality should not be degraded as such that could be revealed in HVS.
- The watermark should sustain image processing attacks, re-watermarking, compression etc.

Invisible image watermarking is a method for embedding information into a digital image without deteriorating the image quality. It provides a persistent connection between the authenticator and the image it authenticates [1]. The digital invisible image watermarking (hereinafter referred to as watermarking for rest of the paper) can be categorized mainly into two types with respect to watermarking domain— spatial and frequency domain watermarking [2]. Spatial domain watermarking is useful to determine the ownership integrity. But it is not suitable for copyright protection as it is very fragile in nature. A counterfeiter may not retrieve the watermark from watermarked image but the watermark can be destroyed if image processing filters are applied or JPEG compression is performed on the watermarked image even at a very low level. Frequency domain watermarking approaches are proven efficient to resist the different type of attacks and compression.

II. Related Work

In 1997 Cox et.al. have proposed a global DCT based watermarking technique for image watermarking [3]. They first suggested that the watermark could be embedded in the low-frequency bands. Although low-frequency coefficients are very sensitive to HVS but at the same time, it is also true that most compression techniques reduce the insubstantial parts of the image like— LSB in the spatial domain and high frequencies in the frequency domain. They proposed a spread spectrum watermarking technique where NxN DCT is performed on a NxN image to obtain NxN coefficients (Global DCT). At the encoding end, a NxN image D is taken and NxN DCT is performed to obtain NxN coefficients. They have chosen the watermark as a sequence of 1000 real numbers $X = x_1 \dots x_{1000}$. Each value of the watermark x_i is chosen independently with a normal distribution having zero mean and unity variance. Now out of NxN DCT coefficients 1000 largest low-frequency coefficients are being taken (DC coefficient will be left as it is). As per the watermark sequence, extremely small modifications are done on these 1000 coefficients. After that IDCT is performed to obtain the watermarked image D'.

Their novelty in proposing the low frequency is more robust than high frequencies is well accounted because in JPEG compression the high frequencies are being discarded. So if we embed the watermark data into the high frequencies those will be lost if a JPEG compression is performed even with a high-quality factor (i.e., less compression). But their approach to performing Global DCT is surely reducing the watermarking capacity of the proposed technique because performing NxN DCT of NxN image results only NxN coefficients. Out of those, a few will be of low frequencies. So Global DCT is undoubtedly decreasing the capacity of embedding watermark.

In the year 2006, Yuan et.al. proposed a multipurpose color image watermarking algorithm for copyright protection and image authentication [4]. The main idea is to embed the robust and fragile watermarks into different color components of the color host image simultaneously. The fragile watermark is embedded in the spatial domain of Blue component using conventional LSB algorithm to achieve the excellence in image authentication whereas the robust watermark is embedded in the frequency domain of Green component to obtain the goal of copyright protection by modifying the Discrete Cosine Transform (DCT) coefficients. The idea of embedding watermark in spatial and frequency domain altogether really sounds well. Watermarking in 'Blue' channel is also well counted because 'Blue' is least sensitive to HVS if the spatial domain is concerned. If spatial domain watermark is extracted intact then it would be understood that there is no attack is performed because spatial watermarks are very fragile in nature. But embedding another watermark at frequencies of 'Green' using DCT would not be efficient because, RGB color space is highly correlated and that's why it is not considered in frequency domain watermarking. Instead, YCbCr space is more suitable for such coding.

In 2009 Lin et.al. have proposed another idea of watermarking that was claimed robust against JPEG compression [5]. They have also accepted the idea proposed by Cox et.al. [3]— Low-frequency coefficients can offer more robustness than high frequencies against JPEG compression. According to their framework, the host image is transformed from RGB to YCbCr color space before frequency domain coding and Y part is considered for watermarking. They've performed 8x8 block DCT on host image and then quantized by standard JPEG quantization matrix. They claimed quantizing blocks prior to watermarking gives additional robustness against JPEG compression. But quantizing an image at the watermarking end is unacceptable because, quantization process discards many high frequencies (i.e., loss of image information) of an image so deteriorating the quality of host image at the time of watermarking is not at all accepted. They've identified the low frequency DCT coefficients at positions C(2, 0), C(1, 1), C(0, 2), C(0, 3), C(1, 2), C(2, 1), and C(3, 0). Out of these only two coefficients C(0, 2), C(2, 0) are considered for embedding watermark bits. Choosing only two coefficients may lead damage to the watermark by any counterfeiter because, even if these two frequencies are scaled (up or down) by a minimum amount, the watermark will be severely damaged. The re-watermarking attack is not also taken into consideration. In this attack, the counterfeiter usually embeds his own watermark into the watermarked image using the own secret key and claims the ownership.

In 2012 Deb *et al.* have proposed a combined DWT and DCT based watermarking technique with low frequency watermarking with weighted correction [12]. DWT has excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the human visual system (HVS). DCT based watermarking techniques offer compression while DWT based watermarking techniques offer scalability. The proposed method embeds of watermark bits are in the low-frequency band of each DCT block of selected DWT sub-band. The weighted correction is also used to improve the imperceptibility. The extracting procedure reverses the embedding operations without the reference of the original image. Choosing low-frequency band for watermark embedding like [3] [5] surely enhances the robustness of the scheme under various attacks such as JPEG compression but the quality of watermarked image is not that well obtained with respect to the PSNR reported. The security issues are not being taken into consideration.

In the year of 2013 Raval et.al. have proposed another approach of frequency domain watermarking through combined DWT-DCT [11]. They perform DWT on the host image then again DCT is applied on the decomposed sub bands. To make their framework robust against JPEG compression they passed the FDCT data into EBCOT (embedded block coding optimal truncatation) algorithm. After receiving, the algorithm outputs the binary watermark bits which are embedded into the frequencies of the host image. They did not mention the desired frequency region for watermarking. Considering high frequencies for watermarking surely decreases the robustness. Using EBCOT algorithm to resist the JPEG compression is also not very effective for common image processing applications those are using standard JPEG algorithm.

In 2016 Zong *et al.* [13] have proposed DCT based method for image watermarking. In the watermark embedding process, the host image is divided into blocks, followed by the 2-D DCT. A secret key is applied to each image block to randomly select a set of DCT coefficients of middle frequency for watermark embedding. Watermark bits are inserted into an image block by modifying the set of DCT coefficients with the help of an error buffer to deal with errors caused by attacks. In the watermark detection process, the corresponding detection matrices are formed from the received image using the same secret key. Afterward, the watermark bits are extracted from the detection matrices. Since the proposed watermarking method only uses two DCT coefficients (of middle frequencies) to hide one watermark bit, it has a limitation in hiding the watermark of bigger size. That means the size of watermark and host image ratio should be moderate enough. Though they have claimed that their method is robust against JPEG compression but using middle frequencies for watermark embedding may not sound good to higher degrees of JPEG compression. As they've used only two coefficients per block to embed watermark, the low-frequency components are suggested to good in the tradeoff between imperceptibility and robustness.

Keeping all the aforementioned limitations in the account, a DCT based invisible image watermarking framework is proposed hereinafter which is robust against JPEG compression, other leading image processing attacks as well as re-watermarking. In this work, we have performed 8x8 block DCT on the color host image to embed a binary watermark into it. The binary watermark is scrambled with a secret key to employing additional security. The watermarking information is embedded into one of the seven low-frequency coefficients of each 8x8 block depending on another secret key. Instead of embedding watermark bits, we have proposed a new phenomenon called scaled average. The watermark extraction is blind and the same set of secret keys is needed to extract the watermark.

The watermark embedding algorithm is reported in Section 3, the extraction algorithm is reported in Section 4. Result set analysis is depicted in Section 5 and conclusions are being made i Section 6.

III. Embedding Algorithm

The steps of proposed watermark embedding algorithm are described below—

Input: Host Image, Watermark, Secret key-1,Secret key-2

Output: Watermarked image

3.1 Color space transformation— Step 1

The host image (H) will be transformed from RGB color space to YCbCr color space because RGB color space is highly correlated and not suitable for frequency domain watermarking such as DCT [6]. Y part is called the luminance component whereas the Cb and Cr parts are called blue chrominance and red chrominance respectively. Although the luminance is much sensitive to HVS than the chrominance still the luminance (Y) channel of host image is considered for embedding watermark because JPEG compression discards a lot of chrominance information during chroma subsampling. So the watermark will not sustain against JPEG compression if the watermark is embedded at chrominance part. The transformation from RGB color space to YCbCr color space is done with following matrix [5]. Fig. 1 (a) shows the host image in RGB color space and Fig. 1 (b) shows the luminance (Y) of the host image.

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.148 & -0.289 & 0.437 \\ 0.615 & -0.515 & -0.100 \end{pmatrix} \times \begin{pmatrix} R \\ G \\ B \end{pmatrix} \quad (1)$$

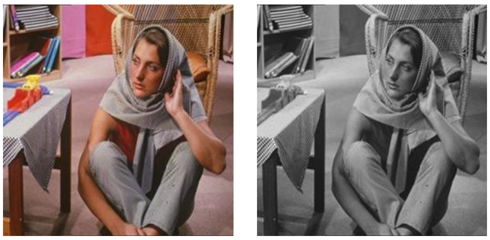

(a) (b)

Fig.1. (a) RGB Color space of host image (b) Y part of host image

3.2 Watermark scrambling— Step 2

The binary watermark (w) is taken and scrambled by applying Secret key-1. The watermark is scrambled to employ enhanced security to the proposed watermarking system. Even if a counterfeiter able to extract the watermark from a watermarked image, the scrambled watermark will be retrieved, not the original one. The binary watermark of size 256x256 is divided into sixty-four 32x32 nonoverlapping blocks. Depending on the 24-byte long Secret key-1 these sixty-four blocks get shuffled their positions as per our scrambling algorithm. With two different value of Secret key-1 such as β_1 and β_2 the watermark gets scrambled in an absolutely different manner as shown in Fig. 2.

24-byte key will be divided into 64 groups where each group contains consecutive 3 bits as follows—

101 | 010 | 001 |111 |110 |101 |001 |111 |……….
5 |2 |1 |7 |6 |5 |1 |7 |.………

Each consecutive 3 bits can represent a range of 0 — 7 as above. Therefore, consecutive 2 numbers able to represent a particular block position as follows—

(5, 2) (1, 7) (6, 5) (1, 7)…[Ranging from (0. 0) to (7, 7)]

Now every pair of 2 consecutive blocks will be swapped provided either of the blocks is not swapped earlier. In the above example, the block of position (5, 2) is swapped with (1, 7) but next pair (6, 5) will not be swapped with (1, 7) as because (1, 7) is already swapped with (5, 2). Continuing in this manner the logo will be scrambled.

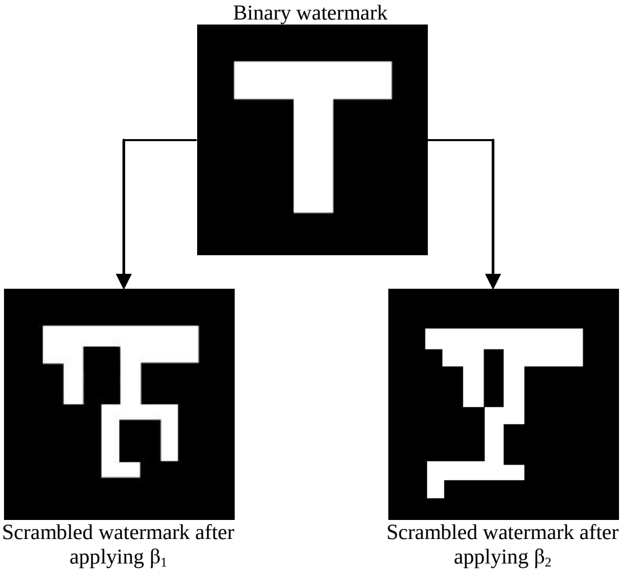

Binary watermark
Scrambled watermark after applying β1
Scrambled watermark after applying β2

Fig.2. Watermark scrambling with two different values of Secret key-1

3.2.1 Scrambling Algorithm

Input: Watermark (256x256), Secret Key-1(β of 24-byte)
Output: Scrambled Watermark (256x256)

```
STEP1:
LOOP (i=0; i<64; i++)
{
 xpos = i * 3;
 LOOP (a=0; a<3; a++)
  {
    Array1[a]= β[xpos+a];
    Array2[i] = decimal equivalent of
              Array[a] Array1[a+1] Array[a+2];
  }
}
STEP2:
LOOP (j=0; j<32; j++)
{
 ypos = j * 4;
 LOOP (b=0; b<4; b++)
  {
   p = Array2[ypos+b];
   q = Array2[ypos+b+1];
   r = Array2[ypos+b+2];
   s = Array2[ypos+b+3];
 If (flag[p][q]!=TRUE||flag[r][s]!=TRUE)
  {
   temp[0][0]  =  Block [p][q];
   Block[p][q] =  Block[r][s];
   Block[r][s] =  temp[0][0];
   flag[p][q] == TRUE;
   flag[r][s] == TRUE;
  }
 }
}
```

3.3 Texture localization— Step 3

The scrambled binary watermark can have two possible pixel values— 255 and 0. The pixels of scrambled watermark having value 255 are substituted with 0. On the other hand, the pixels having value 0 are substituted by the Y values of the host image. Fig. 3 (a) (b) (c) are provided in this regard.

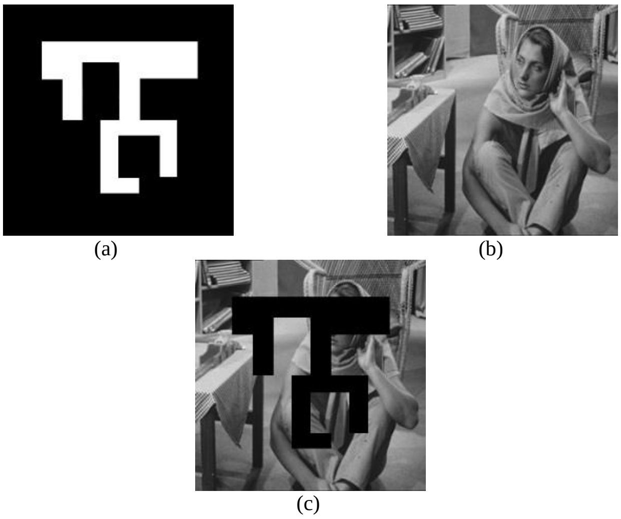


Fig.3. (a) Scrambled watermark (b) Y part of host image (c) Texture localized watermark

3.4 DCT of luminance of host image— Step 4

Discrete Cosine Transform is a well-known method for signal decomposition that transforms an image from spatial to the frequency domain. The DCT works by separating an image into parts of differing frequencies. The forward DCT of an image will be achieved from Equation2 [7].

$$DCT\ (i,j) = C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel\ (x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right] \qquad (2)$$

Where,

$$C(i), C(j) = \begin{cases} \sqrt{\frac{1}{N}} & for\ i,j = 0 \\ \sqrt{\frac{2}{N}} & for\ i,j = 1,2,3 \dots N-1 \end{cases}$$

p(x,y) is the x, y^{th} element of the image represented by matrix p. N is the size of the block on that the DCT is done. Equation2 determines one entry (i, j^{th}) of the transformed image from the pixel values of the original image matrix. In proposed framework, the luminance part Y of the host image is divided into 8X8 (N=8) nonoverlapping blocks and forward DCT is performed on each individual block.

3.5 Encoding— Step 5

Each 8x8 block is having 64 coefficients, out of these the (0,0) element is known as DC coefficient that has most significant information of that block. Other 63 coefficients are called AC coefficients where typically 7 coefficients from top-left corner of the block are considered as low frequency coefficients [5][6] such as—(0,1) (0,2) (1,0) (1,1) (1,2) (2,0) (2,1). The higher frequency coefficients are obtained traversing towards the right-bottom corner of the block. In JPEG compression the high frequencies are being discarded because our psycho visual system is less sensitive towards high frequencies [3][6]. So choosing high-frequency band for watermarking will surely lack robustness against JPEG compression. That's why low-frequency band is considered for hiding the watermark in current context.

Scaled average of two low-frequency coefficients is calculated and another low-frequency coefficient is substituted with the averaged value for such blocks where the value of DC coefficient is different in texture localized watermark and host image, i.e., the host image blocks where the watermark blocks are superimposed. On the other hand for the blocks where the value of DC coefficient doesn't differ will remain same. Fig. 4 shows the low-frequency coefficients of the 8x8 block. A 384 byte long Secret key-2 is taken (may be formed by repeating Secret key-1 for 16 times) and applied to determine which coefficients are to be averaged and which one will be substituted by averaged value. Proposed operations are as follows depending on different values of Secret key-2. Now consider the following key—

101001100000111101110 011000110110………

This key will be divided into 1024 groups where each group is having 3 bits.

101| 001| 100| 000| 111| 101| 110| 011| ….
5 | 1 | 4 | 0 | 7 | 5 | 6 | 3 | .....

Each of the 1024 values will be assigned to 1024 nos. of 8x8 blocks of the host image.

5→(0,0) 1→(0,1) 4→(0,2) 0→(0,3) 7→(0,4) 5→(0,5) 6→ (0,6) 3→(0,7) and so on.

Now consider, the DC coefficient of (0,0) block is different from DC coefficient of the same block of texture localized watermark. The (0,0) block will be encoded with the 5th rule as the key value 5 is assigned to (0,0) block. The set of rules are as follows—

For assigned value = 0/1 $(0,1) \leftarrow \frac{(1,0)+(1,1)}{1}$

For assigned value = 2 $(1,0) \leftarrow \frac{(0,1)+(2,0)}{2}$

For assigned value = 3 $(1,1) \leftarrow \frac{(0,2)+(1,0)}{3}$

For assigned value = 4 $(0,2) \leftarrow \frac{(0,1)+(1,1)}{4}$

For assigned value = 5 $(2,0) \leftarrow \frac{(0,1)+(1,0)}{5}$

For assigned value = 6 $(1,2) \leftarrow \frac{(0,1)+(2,1)}{6}$

For assigned value = 7 $(2,1) \leftarrow \frac{(1,2)+(1,0)}{7}$

DC	0,1	0,2
1,0	1,1	1,2
2,0	2,1	

Fig.4. Low-frequency coefficients of 8x8 block

The following image block analysis illustrates the encoding technique—

Let us assume that, block (6, 6) is such a block where DC value of the block is different in texture localized watermark and host image i.e., the block contains watermark information.

The luminance of aforesaid block be as follows—

166	192	160	119	94	73	43	27
194	190	139	100	67	44	33	26
189	157	115	81	47	30	30	26
162	122	93	55	35	33	31	25
127	101	70	38	34	34	27	24
113	79	44	30	32	32	27	25
93	49	28	30	30	28	28	29
62	28	32	37	32	26	27	31

After performing FDCT the coefficients are as follows—

-483	295	87	30	4	2	1	0
206	154	-7	-24	-30	-16	-10	-5
26	-21	-46	-14	0	-5	-5	-4
11	-9	-14	8	-13	-15	-2	-2
-1	-20	-22	-8	-10	-2	7	3
1	-6	-1	5	2	5	3	0
1	-3	-6	-2	0	0	0	0
-1	-2	-3	-2	1	-1	-1	0

Say the key value 2 is assigned for (6,6), so according to our framework the values of the coefficient (0, 1) and (2, 0) will be summed up and divided by the value 2. The resultant value will substitute the value of coefficient (1,0). The following equation is used to perform the operation—

For assigned value =2 $(1,0) \leftarrow \frac{(0,1)+(2,0)}{2}$

$(1,0) \leftarrow \frac{295+26}{2} \quad = \quad 160.5$

After the encoding, the watermarked block the coefficients are as follows —

-483	295	87	30	4	2	1	0
160.5	154	-7	-24	-30	-16	-10	-5
26	-21	-46	-14	0	-5	-5	-4
11	-9	-14	8	-13	-15	-2	-2
-1	-20	-22	-8	-10	-2	7	3
1	-6	-1	5	2	5	3	0
1	-3	-6	-2	0	0	0	0
-1	-2	-3	-2	1	-1	-1	0

Modified : (1, 0) = 160.5

3.6 IDCT— Step 6

Inverse DCT needed to be performed on individual blocks after encoding, IDCT will be done according to Equation3[7].

$$\text{pixel}\,(x,y) = C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} DCT(i,j)\ \cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \qquad (3)$$

Where

$$C(i), C(j) = \begin{cases} \sqrt{\dfrac{1}{N}} & for\ i,j = 0 \\ \sqrt{\dfrac{2}{N}} & for\ i,j = 1,2,3 \ldots N-1 \end{cases}$$

The Luminance of watermarked block (6,6) will be as follows—

158	184	152	112	86	65	35	19
187	183	133	93	60	38	27	19
184	153	111	77	43	26	26	21
160	120	92	53	33	32	29	23
128	103	72	39	36	35	29	26
118	84	49	35	36	37	32	30
100	56	35	37	36	35	35	36
69	36	39	45	40	34	35	39

3.7 Color space re-transformation— Step 7

Finally, the watermarked image will be obtained by transforming from YCbCr color space to RGB color space using Equation4. Fig. 5 Shows the final watermarked image.

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1.13983 \\ 1 & -0.39465 & -0.58060 \\ 1 & 2.03211 & 0 \end{pmatrix} \times \begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} \qquad (4)$$

Fig.5. Watermarked image

IV. Extraction Algorithm

At the extraction end, we need to execute the extraction algorithm keeping the watermarked image and both secret keys as the input parameters and the algorithm outputs the watermark. The steps of proposed watermark extraction algorithm are described below—

Input: Watermarked image, Secret key-1, Secret key-2
Output: Watermark

4.1 Color space transformation— Step 1

The watermarked image will be transformed from RGB color space to YCbCr color space using Equation1 and only Y part is taken for consideration. Fig. 6 (a) and (b) show the watermarked image in RGB space and luminance part (Y) of watermarked image respectively.

(a) (b)

Fig.6. (a) RGB of watermarked image (b) Y part of watermarked image

4.2 DCT of luminance of watermarked image— Step 2

Watermarked image is divided into 8x8 non-overlapping blocks and forward DCT is performed on the Y part of watermarked image for all such blocks using Equation2.

4.3 Decoding— Step 3

Each block is examined thoroughly after applying Secret key-2 (may be obtained by repeating Secret key-1 for 16 times) that is used at the time of encoding. A particular block is considered to be watermarked if a particular low-frequency coefficient (derived from Secret key-2) holds the frequency of scaled average of other two low-frequency coefficients (derived from Secret key-2).

The following example is provided to illustrate the decoding technique. The block (6, 6) is taken to examine it is watermarked or not. After performing FDCT the coefficients are as follows—

-483	295	87	30	3	2	1	0
161	154	-8	-24	-30	-16	-10	-5
26	-21	-46	-14	0	-5	-5	-5
11	-9	-13	8	-13	-15	-2	-2
-2	-20	-22	-8	-10	-2	7	3
1	-6	-1	5	2	5	3	0
1	-3	-6	-2	0	0	0	0
0	-2	-3	-2	1	-1	-2	0

Same assigned secret key value 2 that is used at the time of encoding is applied. According to our framework following calculation is performed—

For assigned value=2,

$$(1, 0) = \frac{(0,1)+(2,0)}{2} = \frac{295+26}{2} = 160.5 \pm \delta$$

Where 'δ' is a marginal threshold.

Here the block (6, 6) is considered as watermarked block because the scaled average of coefficients (0, 1) and (2, 0) (i.e., 160.5+0.5=161 where δ=+0.5) is found at coefficient (1, 0).

4.4 Frequency substitution— Step 4

The frequency of DC coefficient of a watermarked block is substituted by very high frequency (e.g. 2000) and the frequency of DC coefficient of an unwatermarked block is substituted with very low frequency (e.g. -2000). DC coefficients are holding the most significant information of every DCT block and as the binary watermark is considered in current context, substituted DC frequencies will be good enough to reconstruct the binary watermark. After high-frequency substitution at DC coefficient, the block (6, 6) is as follows—

2000	295	87	30	3	2	1	0
161	154	-8	-24	-30	-16	-10	-5
26	-21	-46	-14	0	-5	-5	-5
11	-9	-13	8	-13	-15	-2	-2
-2	-20	-22	-8	-10	-2	7	3
1	-6	-1	5	2	5	3	0
1	-3	-6	-2	0	0	0	0
0	-2	-3	-2	1	-1	-2	0

After low-frequency substitution at DC coefficient, an unwatermarked block say (1, 1) is as follows—

-2000	-51	16	3	0	0	1	-1
-151	-30	-17	-15	-1	-2	-4	2
-160	-58	46	-1	1	-5	3	0
-77	101	-35	-18	-7	-6	-1	3
20	-99	-50	25	1	6	2	3
-36	-14	46	18	10	4	2	0
12	9	16	17	0	1	0	0
3	14	24	-10	-4	0	1	1

4.5 IDCT— Step 5

Inverse DCT is performed using Equation3 to obtain the scrambled watermark in spatial form. Fig. 7 shows the extracted watermark in scrambled form.

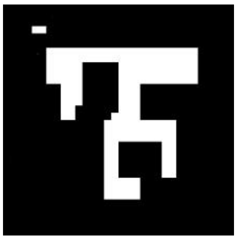


Fig.7. Extracted scrambled watermark

4.6 Descrambling— Step 6

Same Secret key-1 that is used at the time of scrambling the watermark is applied to descramble the extracted watermark to obtain it in its original form. Fig. 8 shows the final extracted watermark after descrambling.

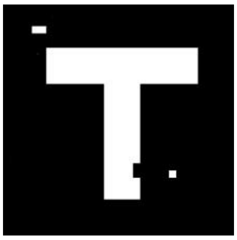


Fig.8. Descrambled watermark

V. Experimental Classification Results and Analysis

The experiments with the proposed watermarking framework are being performed on a variety of images with different watermarks and satisfactory results are being obtained. The leading features of proposed watermarking framework are stated below—

- Frequency domain watermarking framework offers more robustness than spatial domain.
- Using luminance component (Y) for embedding watermark makes the framework more robust because the human visual system is more sensitive to luminance and that's why most filter based image processing attack does not touch the luminance part of an image as such. In JPEG compression, also luminance part is not down-sampled [6]. Therefore, even after performing the filter based attacks and JPEG compression, the watermark can be still extracted in recognizable form.
- Considering low-frequency coefficients of individual DCT blocks of the luminance part (Y) of image for embedding watermark information resist the effect of JPEG compression. According to JPEG algorithm, the high frequencies are discarded at the time of quantization and low-frequencies are not modified as such because they carry significant

information of the image. So, watermark information can be retrieved from low-frequency coefficients even after high JPEG compression.

- There is no fixed block (8x8 DCT block) for embedding watermark information. The watermark embedding blocks are identified depending on the watermark itself. That employs additional robustness to the framework against re-watermarking. It empowers the owner to extract the watermark if the watermarked image is re-watermarked with a different logo by any counterfeiter.
- Security is well considered in the proposed framework. Two secret keys are used— the first one is used to scramble the watermark before embedding. And the second one is used to identify one of seven low-frequency coefficients within an 8x8 DCT block for watermark encoding. Without knowing these two secret keys a counterfeiter will not be able to extract the watermark.
- The extraction algorithm is blind that means, neither the host nor the watermark is required at the decoding end.
- If an attacker who knows the algorithm arbitrarily changes all of the seven low-frequency components, the image quality will be degraded severely. The counterfeiter won't be able to damage the watermark without degrading the watermarked image because embedding coefficients are chosen dynamically by Secret key-2.

The perceptual invisibility of watermark to HVS is established with PSNR. It is most commonly used as a measure of the quality of watermarked image and could be defined via root mean square error (RMSE) as described in Equation5. [8][14]. The detailed experiment has been carried out and we have achieved a set of nice PSNR values which are more than 50dB. Hence no difference between host and watermarked image can be noticed in bare eyes. Table 1 is provided in this regard.

$$PSNR = 20\, log_{10}\left(\frac{MAX}{RMSE}\right) \tag{5}$$

If a pixel in the host image is defined as Y (i,j) and that in the watermarked image is defined as y (i,j), then the root mean square error (RMSE) of the watermarked image is computed with Equation6 [9].

$$RMSE = \sqrt{\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[Y_{(i,j)} - y_{(i,j)}]^2}{M \times N}} \tag{6}$$

Table 1. PSNR analysis

Watermarked Image	Image Dimension	PSNR (dB)
Barbara	256 x 256	52.14
Lena	256 x 256	53.09
Baboon	256 x 256	51.37
Vegetable	256 x 256	56.71

The quantitive similarity measurement between the referenced watermark and extracted watermark is computed by normalized correlation (nc). The nc calculation is done with Equation7 [10].

$$nc = \frac{\sum\ \sum(I_w[i][j]*I_o[i][j])}{\sqrt{\sum\ \sum(I_w\,[i][j]*\,I_o[i][j])^2}} \tag{7}$$

The proposed watermarking framework is being tested regarding JPEG compression on a number of color images with different quality factors. But it is observed that the watermark is sustained and extracted well even at a low-quality factor. Some of the tested results on the image—'Barbara' is reported at Table 2 and some other results are depicted at Table 3

Table 2. JPEG compression result set

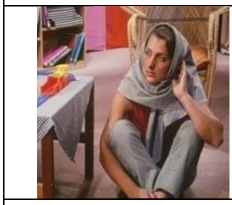
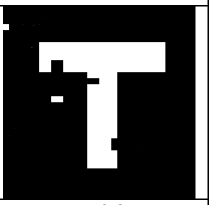
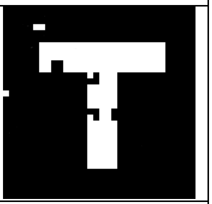
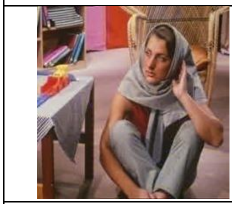
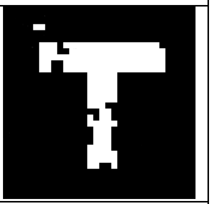
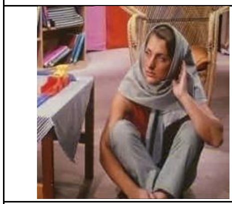
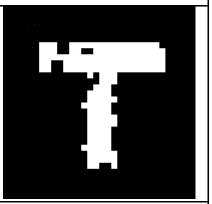
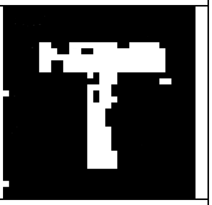
JPEG Compressed Watermarked Image	JPEG Quality Factor	Extracted Watermark
	80	
		nc = 0.94
	70	
		nc = 0.92
	60	
		nc = 0.87
	50	
		nc = 0.83
	40	
		nc = 0.79

Table 3. nc analysis after JPEG compression

Image	JPEG Quality Factor	nc
Lena	80	0.93
	70	0.90
	60	0.86
	50	0.81
	40	0.76
Baboon	80	0.94
	70	0.92
	60	0.88
	50	0.84
	40	0.80

The leading image processing filter based attacks like— auto tone, auto color, despeckle etc. are also considered in our experiments. The extracted watermark shows the robustness of the proposed framework against the different filter based attacks. Some of the tested results on the image—'Lena' is reported in Table 4 and some other results are depicted in Table 5.

Table 4. Filter based attack result set

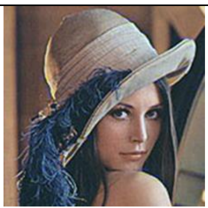
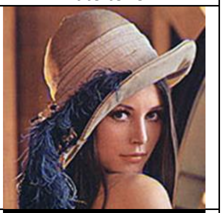
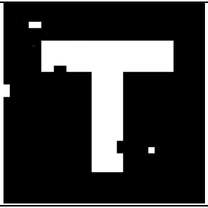
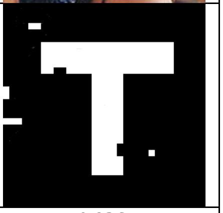
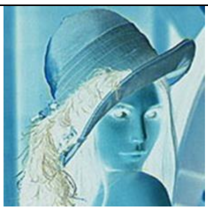
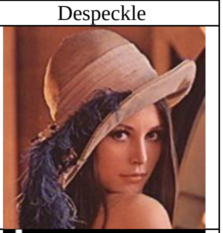
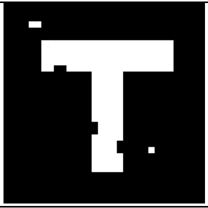
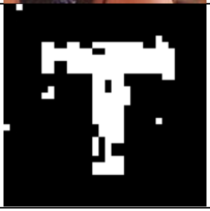
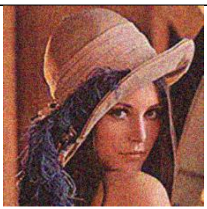
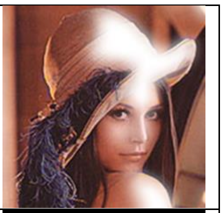
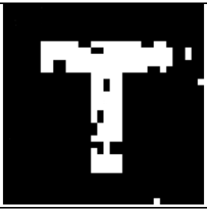
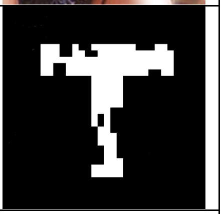
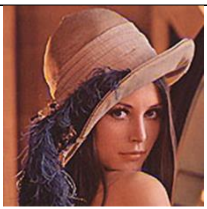
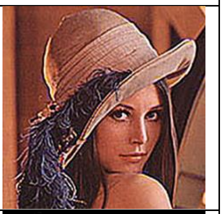
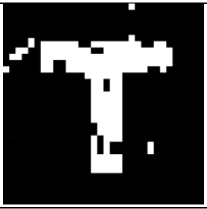
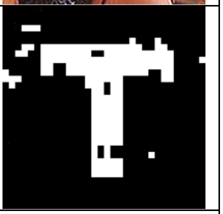
Attack Type	Auto color	Auto tone
Attacked Image		
Extracted Watermark		
Nc	0.957	0.936
Attack Type	Invert	Despeckle
Attacked Image		
Extracted Watermark		
nc	0.957	0.870
Attack Type	Noise	Diffuse glow
Attacked Image		
Extracted Watermark		
nc	0.819	0.679
Attack Type	Sharpen edge	Unsharp mask
Attacked Image		
Extracted Watermark		
nc	0.815	0.803

Table 5. nc analysis after filter attacks

Image	Attack Type	nc
Barbara	Auto color	0.948
	Auto tone	0.939
	Invert	0.850
	Despeckle	0.835
	Noise	0.875
	Diffuse glow	0.650
	Sharpen edge	0.782
	Unsharp mask	0.810
Baboon	Auto color	0.955
	Auto tone	0.952
	Invert	0.962
	Despeckle	0.856
	Noise	0.890
	Diffuse glow	0.660
	Sharpen edge	0.773
	Unsharp mask	0.865

The detailed experiment has also been carried out to determine the robustness of the proposed watermarking framework against re-watermarking and changing low-frequency coefficients (i.e., embedding positions). The footprint of the original watermark can be found even after re-watermarking because— 8x8 embedding blocks are watermark dependent. Two different watermarks can't be completely overlapped with each other. So at the extraction end, the second watermark (which is used by the counterfeiter) will be extracted as it is whereas the original first one may be extracted in partially damaged condition. And that is significant in claiming of ownership and copyright of the actual owner.

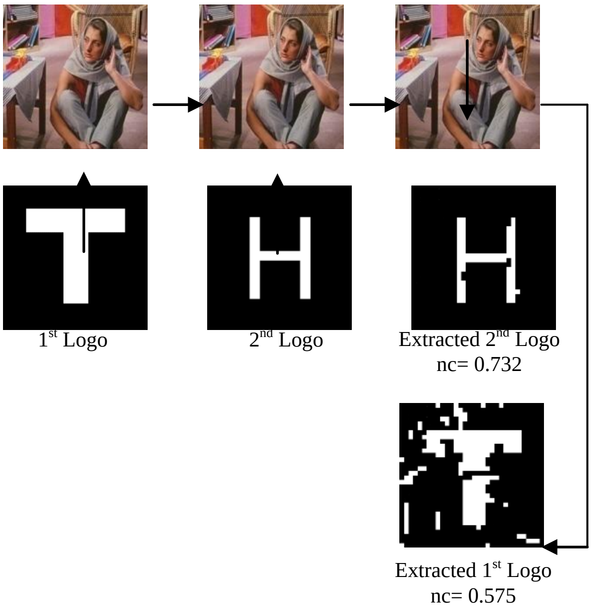
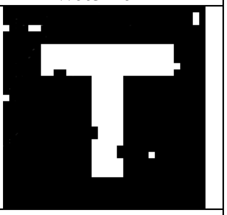
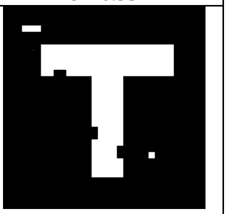
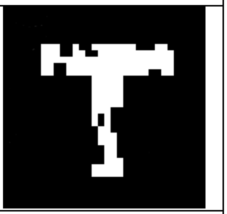
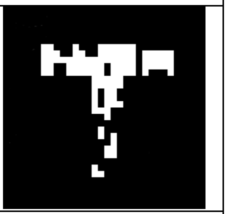


Fig.9. Re-watermarking attack

Table 6. Coefficient scaling result set

Scaled Watermarked Image	Operation	Extracted Watermark
	All low-frequency coefficients are scaled up by 50	
		nc = 0.934
	All low-frequency coefficients are scaled down by 50	
		nc = 0.946
	Alternative frequency coefficients are scaled up-down by 10	
		nc = 0.876
	Alternative frequency coefficients are scaled up-down by 20	
		nc = 0.805

VI. Conclusion

A DCT based invisible color image watermarking framework is proposed in this paper. The watermark is embedded in the low-frequency coefficients of the luminance of host image. Embedded watermark can be extracted even after high JPEG compression, filter based attacks like— auto color, auto tone, unsharp mask, noise, invert etc. Another leading aspect of the proposed framework is, the blocks selected in the host image for embedding watermark are the function of the watermark itself. The framework is proven robust against re-watermarking as well. The watermark extraction is blind i.e., neither the host nor the watermark is needed at the extraction end. Security aspects are well taken care of with two different secret keys where the first one is used to scramble the watermark and the second one is used to determine low-frequency coefficient for watermark coding. Experimental results show that the proposed framework outperforms the earlier works in DCT based image watermarking.

References

[1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker. 2008. Digital Watermarking and Steganography. *2nd Edition, Morgan Kaufmann Publishers.* (ISBN 978-0-12-372585-1).

[2] Monalisa Banerjee. 2007. Theory and application of cellular automata for authentication and watermarking. *Ph.D. thesis, Jadavpur University.*

[3] I.J Cox, J. Kilian, F.T. Leighton, and T. Shamoon. 1997. Secure spread spectrum watermarking for multimedia. in *IEEE Transactions on Image Processing, vol: 6 Issue: 12, Page(s):1673 -1687.*

[4] Yuan Jun, Cui Guo-hua, Zhang Yi-jia. 2006. A Practical Multipurpose Color Image Watermarking Algorithm for Copyright Protection and Image Authentication. *Proc. Digital Telecommunications, 2006. ICDT '06, Page(s):72–77.* Digital Object Identifier 10.1109/ICDT.2006.10.

[5] Shinfeng D. Lin, Shih-Chieh Shie, and Jim Yi Guo. 2009. Improving the Robustness of DCT-Based Image Watermarking Against JPEG Compression. *Elsevier, Journal of Computer Standard and Interfaces Volume 32, Issues 1-2, Page(s): 54-60.*

[6] Gregory K. Wallace. 1991. The JPEG Still Picture Compression Standard. *Communications of the ACM.*

[7] K. R. Rao, Ping Wip. 1990. Discrete Cosine Transform: algorithms, advantages, applications. *Academic Press.*

[8] Soumik Das, Pradosh Bandyopadhyay, Shauvik Paul, Atal Chaudhuri, Monalisa Banerjee. 2010. An Invisible Color Watermarking Framework for Uncompressed Video Authentication. *International Journal of Computer Applications (IJCA).* (ISBN: 978-93-80746-10-4).

[9] Soumik Das, Pradosh Bandyopadhyay, Atal Chaudhuri, Monalisa Banerjee. 2012. A Secured Key-based Digital Text Passing System through Color Image Pixel. *Proc. IEEE International Conference on Advances in Engineering, Science and Management (IEEE-ICAESM 2012).* (ISBN: 978-1-4673-0213-5).

[10] Soumik Das, Pradosh Bandyopadhyay, Monalisa Banerjee, Atal Chaudhuri. 2011. A Chip-Based Watermarking Framework for Color Image Authentication for Secured `Communication. *Communications in Computer and*

Information Science, 1, Volume 125, Springer. Advances in Computing, Communication and Control, Part 2, Springer.

[11] Keta Raval, Sameena Zafar. 2013. Digital Watermarking with Copyright Authentication for Image Communication. *Proc. IEEE International Conference on Intelligent Systems and Signal Processing (ISSP-13), Page(s): 111-116.* (ISBN: 978-1-4799-0316-0).

[12] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque, Md. Iqbal Hasan Sarkar. "Combined DWT-DCT based digital image watermarking technique for copyright protection". Proc. 7th International Conference on Electrical and Computer Engineering. 2012. IEEE.

[13] Tianrui Zong, Yong Xiang, Song Guo, Yue Rong. "Rank-Based Image Watermarking Method With High Embedding Capacity and Robustness". IEEE Access. 2016 IEEE. vol. 4. Page(s): 1689 – 1699.

[14] Anuja Dixit, Rahul Dixit. "A Review on Digital Image Watermarking Techniques". I.J. Image, Graphics and Signal Processing, 2017, 4, 56-66.

Authors' Profiles

Soumik Das experienced in research for last 7 years in cryptographic and watermarking frameworks for digital content's authentication and have published a number of research papers with ACM, Springer, IEEE, MacMillan, Academy Publisher and many more. For demonstrating the works and presenting papers Soumik has been invited to eminent Universities like— Jawaharlal Nehru University, NIT Rourkela, Thapar University, Calcutta University etc. Some of his papers are being archived by IEEE Xplore, IEEE CS Digital Library, ACM, DBLP, and Springer Link. He got registered in Computer Sc. & Engg. Dept, Jadavpur University as Ph.D. Scholar in early 2013 and completed his M.Tech. in IT from Bengal Engg. & Sc. University, Shibpur in the year 2009. He is also providing professional consultancy in web application development for several clients across the globe.

Dr. Monalisa Banerjee is an Associate Professor in Techno India, Salt Lake, West Bengal, India. She is Ph. D. in Computer Science and Engineering. Her Area of Specialization is Digital Watermarking, Network Security and Authentication. She is working with Techno India for last 14 years as an academician in the Department of Computer Application. She worked as a Research Scholar in Jadavpur University for 4 years; as a Project Staff in Bengal Engineering and Science University, Shibpur and also worked with Electronic Research and Development Center of India (under Govt. of India, Dept. of Electronics) as a Project Engineer.

Prof. Atal Chaudhuri is Senior Professor of Computer Sc. & Engg. Dept, Jadavpur University. As Project Engineer he received UNIDO fellowship in the year 1984 for visiting West German and USA for studying the state of art automation appropriate for Indian context. He received his PhD (Engg.) degree in the year 1989 for his thesis "An Approach Towards the Analysis and Design of Network Protocols using Petri Net Models". Prof. Chaudhuri has more than 100 research publications and guided 12 PhD research. He has travelled around the globe to deliver lecture on various research articles on contemporary modern science and engineering.

How to cite this paper: Soumik Das, Monalisa Banerjee, Atal Chaudhuri,"An Improved DCT based Image Watermarking Robust Against JPEG Compression and Other Attacks", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.9, pp.40-50, 2017.DOI: 10.5815/ijigsp.2017.09.05