A Novel Invisible Color Image Watermarking Scheme using Image Adaptive Watermark Creation and Robust Insertion-Extraction

Saraju P. Mohanty
Email: smohanty@cse.unt.edu
Dept. of Computer Science and Engineering
University of North Texas, Denton, TX 76203.

Parthasarathy Guturu
Email: guturu@unt.edu
Dept. of Electrical Engineering
University of North Texas, Denton, TX 76203.

Elias Kougianos
Email: eliask@unt.edu
Dept. of Engineering Technology
University of North Texas, Denton, TX 76203.

Nishikanta Pati
Email: nishi@unt.edu
Dept. of Computer Science and Engineering
University of North Texas, Denton, TX 76203.

Abstract

In this paper we present a robust and novel strategic invisible approach for insertion-extraction of a digital watermark, a color image, into color images. The novelty of our scheme lies in determining a perceptually important sub-image in the host image so that slight tampering of the sub-image will affect the aesthetic of the host image significantly. This eliminates the possibility of watermark removal, which in turn makes the watermark secure and robust. The other novel feature of our algorithm is the creation of a compound watermark image, called effective watermark, using the input user watermark (logo) and attributes of host image, which facilitates robust insertion-extraction processes. The effective watermark creation consists of two distinct phases: In the first phase, a statistical image is synthesized from a perceptually important sub-image of the host image and in the second phase, a compound image is created by fusing the input logo and synthetic statistical image. Results of exhaustive experimentation using standard benchmarks demonstrates the robustness and efficacy of our approach.

1 Introduction

Many research efforts over the past decade have enabled digital watermarking to establish itself as a potential solution for the protection of ownership rights and policing information piracy of multimedia elements like images, audio and video. Watermarking techniques developed for images are mainly classified into visible and invisible approaches. While the visible methods provide means for overt assertion of ownership with logos, the invisible methods provide covert protection of these rights.

Starting with IBM's Vatican Library project [10], visible watermarking technology quickly matured with a few but significant contributions (*e.g.* [1, 18, 13, 12]) from researchers. Invisible watermarking, on the other hand, is a well addressed topic that was initiated by the research teams of Cox [7], Craver [2] and others. Though invisible watermarking techniques helped in making the watermark imperceptible to human eye and less prone to attacks, serious challenges to protect the embedded watermark against different types of attacks still persist. Many of the current techniques use different transform domains to embed the watermark inspired by methods of information coding and image compression. The watermark is embedded into the cover image using the discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete fourier transform (DFT).

The paper is organized as follows: The contributions of this paper are presented in Section 2. The relevant related research works that served as motivation for this research work are discussed in Section 3. In Section 4 we present our innovative strategy for invisible watermark creation. Section 5 discusses the implantation of the compound watermark along with the rationale behind the approach. Section 6 presents our scheme for non-blind extraction of invisible watermarks implanted using our scheme. Finally, experimental results on the performance of our invisible watermarking scheme are presented in Section 7 followed by summary and conclusions in Section 8.

2 Our Contributions

In this paper, we propose a novel strategy for DCT domain robust invisible embedding and extraction through a unique approach for creation of a compound image to serve as the effective watermark.

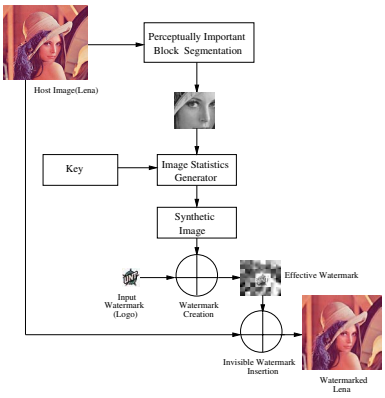


Figure 1. Overview of our Proposed Watermarking Scheme

Fig. 1 provides a schematic overview of the proposed watermarking method. Initially, the algorithm determines the *most eye sensitive sub-image that is a contiguous collection of significant blocks* in the image by considering several influencing characteristics of the Human Visual System (HVS). While a block is an $M \times N$ pixel matrix, the sub-image is a contiguous set of N_B blocks. The image statistics generator module computes the desired statistics from the segmented sub-image in the DCT domain and creates a synthetic image resembling the host sub-image. The input 'key' has two parts: position key and seed key. The 'position key' decides the selection of coefficients for the image statistics generation. The 'seed key' is used in the Gaussian and Laplacian variates as explained in Section 4. The statistical synthetic image created from the perceptually most important sub-image of the image supplements the robust extraction of the watermark for verification and authentication. We create an 'effective watermark' by embedding the user given distinct and recognizable logo to the synthetically generated image by fusing them together. This compound image, called the 'effective watermark', is implanted in the host image at the same location as the perceptually most important sub-image of the host invisibly. The motivation behind making a compound image for the watermark is that even though the logo might get distorted during any signal processing attack on the watermarked image, the synthetic image will follow the original image faithfully with respect to distortion and restoration helping us in robust extraction. Based on this consideration, we propose a strategic feedback based approach to extract the watermark from a possibly corrupted image.

3 Related Research and Motivation

In recent years, many watermarking algorithms have been suggested by researchers to maintain the originality and integrity of networked digital multimedia content. Invisible robust watermarking of digital images is one among the leading research efforts which are being performed in the DCT, DWT, or DFT domains. Cox *et al.* [7] use spread spectrum techniques to embed the watermark in the DCT domain. To improve Cox's method, Lu *et al.* [8] use cocktail watermark to improve the robustness and used HVS to maintain high fidelity of the watermarked image. Langelaar *et al.* [4] proposed an algorithm to embed a bit sequence in the digital image by selective removal of DCT coefficients but the modification of DCT coefficients in smooth regions may result in visual artifacts. Fei *et al.* [3] analyzed the performance of block based watermarking schemes in the presence of lossy compression and suggested a hybrid watermarking algorithm that has greater resilience to JPEG compression. Lu *et al.* [9] presented a novel multipurpose blind digital image watermarking technique based on the multistage vector quantizer structure, which can be applied to both image authentication and copyright protection. They embed both semi-fragile and robust watermarks using different embedding techniques. Jiang *et al.* [5] proposed a blind watermarking scheme in the DCT domain which exploits HVS characteristics to generate high visual quality watermarked images. With respect to strategies to break watermarking schemes, Holliman *et al.* [6] described a class of attacks on certain block-based oblivious watermarking schemes.

The other frequency transformation technique, DWT has been used recently by many researchers for digital image watermarking [19]. Yang *et al.* [20] proposed a DCT-DWT domain dual watermarking scheme exploiting the orthogonality of image sub spaces to provide robust authentication. As watermarking becomes more popular for copyright protection, researchers are focusing on the design of high performance, low-power hardware based watermarking systems for realtime applications. Though DWT yields better PSNR values compared to DCT, researchers are designing DCT based watermarking systems for hardware implementation because of the easiness of implementation [15].

Most of the above research works attempt to embed a pseudo-random sequence as a watermark. But, a source-based watermark like a unique identifiable color logo is more appealing for easy identification of the ownership and authentication. Thus, the robust watermarking scheme presented here proposes to invisibly hide a color or gray scale logo in the color or gray scale image. We address in this pa-

per the issue of strategically creating and implanting a watermark with the dual purpose of attack prevention and detection. The invisible robust watermarking scheme works in the DCT domain. To ensure robustness of the watermark, we create a synthetic compound watermark based on a well recognized logo, the user defined watermark. For the authentication purpose the compound watermark is created and verified with the extracted watermark.

4 Our Approach for Watermark Creation

In this section we discuss our approach for creating a synthetic compound watermark. It may be noted that the user is allowed to use a color or gray scale image as watermark and we create the compound image (*i. e.* effective watermark) and to use it as the medium for robust invisible watermark insertion and extraction. The creation of the watermark is a two step process: first step is the selection of a region of interest (sub-image) and gathering of host/original image statistical information and the second step is the fusion of user input watermark image (a recognizable logo) and generated synthetic image which create the effective watermark for our scheme.

For color images, the image is initially converted to gray scale for the segmentation of perceptually important sub-image in the image. Once the region is segmented, each band (red, green, blue) of the color image is considered for the synthetic image creation followed by creation of the watermark compound image. During the invisible insertion of the effective watermark into the color host image, each band of the host is processed with the respective band of the effective watermark image separately.

4.1 Automatic Detection of a Significant Sub-Image considering the Human Visual System (HVS) Sensitivity

In order to automatically find out the sensitive and perceptually important sub-image of an image with respect to human perception, we need to understand the factors which influence the Human Visual System (HVS), as suggested by Osberger *et al.* [14]. Earlier research works [11], [14] have identified many factors that influence the visual attention of humans. They have considered several factors as discussed below for determining perceptually the most sensitive blocks of the image. It may be noted that a block is a matrix of $M \times N$ pixels, same size as that used for DCT computation. What we are interested in is to *automatically* determine a contiguous set of perceptually significant such N_B blocks constituting a "sub-image".

Intensity: According to [11] the blocks of the image which are more close to the mid intensity of the image are most sensitive to the human eye.

Contrast: A block which has high level of contrast with respect to the surrounding blocks attract the human eye's attention and hence are perceptually more important.

Location: According to [14] the center-quarter of an image is perceptually more important than other areas of the image. So, we concentrate our focus at the central-quarter of the image.

Edginess: A block which contains prominent edges captures the attention of the human eye.

Texture: A highly textured block is less sensitive to noise. Modification inside a highly textured block is unnoticeable to human eye.

In order to determine the sub-image of interest, the host image is divided into $M \times N$ blocks and a sliding square window containing N_B number of such blocks in both the horizontal and vertical directions (a tentative sub-image) is considered. The sliding window slides across the image and computes a quantitative measure (M) for each one of the influencing factors at every location. The mathematical equations used to find the quantitative measure for these factors are described below.

Intensity Metric: The mid intensity importance $M_{intensity}$ of a sub-image (or window) W_i is computed as:

$$M_{intensity}(W_i) = Abs(AvgInt(W_i) - MedInt(I)), \quad (1)$$

where $AvgInt(W_i)$ is the average luminance of sub-image W_i, and $MedInt(I)$ is the average luminance of the whole image.

Contrast Metric: A sub-image which has high level of contrast with respect to the surrounding sub-images attracts the human eye's attention and supposedly is perceptually more important. If $AvgInt(W_i)$ is the average luminance of sub-image W_i and $AvgInt(W_{i-surrounding})$ is the average luminance of all its surrounding sub-images, then the contrast measure can be defined as:

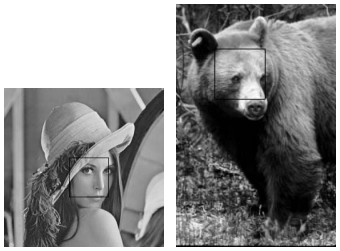
$$M_{contrast}(W_i) = AvgInt(W_i) - AvgInt(W_{i-surrounding}). \quad (2)$$

Location Metric: The location importance $M_{location}$ of each sub-image is measured by computing the ratio of the number of pixels of the sub-image who are lying in the center-quarter of the image to the total number of pixels in the sub-image. This can be expressed as:

$$M_{location}(W_i) = \frac{centre(W_i)}{Total(W_i)}, \quad (3)$$

where $centre(W_i)$ is number of pixels of the sub-image lying in the central quarter of the image and $Total(W_i)$ is the total number of pixels of the sub-image, *i. e.* the area of the sub-image.

Edginess Metric: The edginess of the window $M_{edginess}$ is computed by adding the blocks which are determined as



(a) Lena (b) bear

Figure 2. Automatic Determination of Perceptually Important Sub-images in Images

edge blocks. A block is declared as an edge block if the summation of absolute values of all the AC coefficients in a block exceeds a predetermined threshold as suggested by Shen *et al.* [17]. It may be noted that a spatial domain operator like Sobel or Canny could be used for edge detection, but we used the DCT domain techniques as we intended to perform all processing in DCT domain.

Texture Metric: The texture factor $M_{texture}$ is computed by adding the variance of all the AC coefficients of each block inside the window. It has been shown that a highly textured block has evenly distributed AC coefficients. So, a high variance value indicates that the sub-image is less textured. This can be calculated as:

$$M_{texture}(W_i) = \frac{\sum (F_{j,k} - \mu_{AC})^2}{(M \times N) - 1}, \tag{4}$$

where $F_{j,k}$ is the $(j,k)th$ AC coefficient of the sub-image W_i and μ_{AC} is the mean of all the AC coefficients.

After performing the above computation for the windows, we assign an important measure for each of the five factors. The measure for each factor is normalized to be in the range $[0, 1]$. After the normalization, we combine these five factors for each window to produce an overall Importance Measure (M) for each of the sub-images. We chose to square and sum all the factor measures to produce the final M for for each window W_i as described by the following equation [14]:

$$\begin{aligned} M(W_i) \quad &= (M_{intensity}(W_i))^2 + (M_{contrast}(W_i))^2 \\ &+ (M_{location}(W_i))^2 + (M_{edginess}(W_i))^2 \\ &+ (M_{texture}(W_i))^2. \end{aligned} \tag{5}$$

The calculated M for all the windows are sorted and the window having the highest value of M is selected as the perceptually most important region. The perceptually important sub-image found by our approach in the Lena and bear images are shown in Fig. 2 for block size of 8×8 pixels and sub-image (window) size of 5×5 blocks.

To deal with the color images, we convert the image to gray scale to find the location of perceptually the most important sub-image. The same location is used in all the bands during the synthetic image generation as well as the invisible insertion of the watermark.

4.2 Creation of the Watermark

The following steps are followed to initially generate a synthetic image from perceptually the most important region and finally create a compound image watermark where a logo or emblem is visibly embedded [12] in the generated synthetic image. The compound image serves as the invisible watermark in the algorithm proposed next.

1. Divide the host image into an integral number of $M \times N$ blocks (after necessary image extensions.)
2. Choose the blocks in perceptually the most important region of the host (*as found in the previous section*) for the generation of the synthetic image.
3. Obtain DCT coefficients for the individual blocks of the host and compute the standard deviations of the significant DCT coefficients over the sample space of the host image blocks.
4. Synthesize a statistical image (in DCT space) of the same size as the aforementioned sensitive area of the image using the formula:

$$ws^k_{i,j} = \begin{cases} G(c^k_{i,j}, \sigma_{i,j}) & \text{if } i = j = 0 \\ L(c^k_{i,j}, \sigma_{i,j}) & \text{otherwise} \end{cases} \tag{6}$$

   The super or subscripts k and (i, j) of the various terms denote the block and the block pixel indices, respectively and c and ws indicate the DCT coefficients of the host and synthetic images, respectively. $G(.,.)$ and $L(.,.)$ are Gaussian and Laplacian random variates, respectively, with the first parameter referring to the mean value of the distribution and the second parameter $\sigma_{i,j}$ referring to the standard deviation. For $\sigma_{i,j}$, we use the standard deviation of the (i, j)th DCT coefficient obtained in step 3. Our choice of these two distributions for modeling the DC and AC DCT coefficients of the host image is motivated by empirical results of Reininger and Gibson [16], *i. e.* Gaussian for DC and Laplacian for AC. This dual random distribution makes the watermark more homogenously adaptable to the distribution of DCT coefficients, which is a unique shift from existing schemes in which only one distribution is used.
5. Choose an input logo of smaller size (after necessary scaling down) for superposition on the synthetic image ws so generated. Divide it into $M \times N$ pixel size blocks and obtain its block-wise DCT coefficients (wc's).

(a) Synthetic Image Created from the host (b) Input Logo (c) Compound Image Created - Watermark

Figure 3. Watermark Creation for Lena

6. Fuse this in a less sensitive area of the synthetic image using any DCT based visible watermarking algorithm (*e.g.* [11]). This actually involves determination of two block-specific parameters α^k and β^k indicating the proportions of the synthetic image and the input watermark required for effective fusion. The block fusion formula for effective invisible watermark creation is given below:

$$wm_{ij}^k = \alpha^k \times ws_{ij}^k + \beta^k \times wc_{ij}^k, \qquad (7)$$

where wm represents the final compound watermark, ws symbolizes the synthetic image and wc stands for the chosen logo. Fig. 3 depicts the creation of a sample watermark compound image for block size of 8×8 pixels and sub-image (window) size of 5×5 blocks.

The position key determining the selection of DCT coefficients for the synthetic image generation and the seed used by the random variates during the statistics generation are saved for the use during authentication. To create a compound watermark from a user given color logo, each band of the color logo is treated as of the gray scale logo and finally stitched together to generate a color compound watermark.

5 Watermark Insertion

The compound watermark generated in the previous section is now embedded in the host image invisibly by fusion of the compound watermark (wm) blocks into the corresponding blocks of the earlier chosen perceptually most important region of the host image. To make the watermark invisible, we need to properly scale down the DCT coefficients of the watermark. In the formula given in the invisible insertion module of Fig. 4, we denoted the scaling factor corresponding to an individual DCT term by $\alpha_{i,j}^k$. However, by experimentation with various images, we found that only two scaling factors, one for the DC and the other for AC coefficients, need to be specified, and the values 0.02 and 0.1 for these two types of coefficients, respectively, give good results. This simplifies our computations. However, in order to make the presence of the watermark undetectable by simple statistical analysis, we depart from the simplified approach of Cox *et al.* [7] wherein the watermark is added to

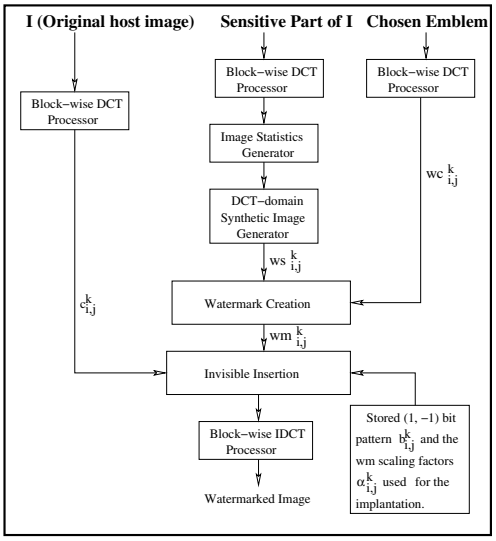


Figure 4. Algorithm for Watermark Insertion

the host at every term. We, on the other hand, add the watermark to the host DCT coefficients at some positions and subtract from them at the other, as suggested by Craver *et al.* [2]. This (1, -1) bit pattern/sequence (denoted by $b_{i,j}^k$) determining the addition or subtraction involved at each pixel position could be any arbitrarily chosen random sequence, but we chose to use an alternating sequence in the current implementation for the sake of simplicity. The mathematical formula used for the invisible insertion of the effective watermark into the host image is given below:

$$c_{ij}^{*k} = c_{ij}^k + b_{ij}^k \times \alpha_{ij}^k \times wm_{ij}^k. \qquad (8)$$

Here c represents the DCT coefficients of the original host image and c^* represents the DCT coefficients of the watermarked image.

In the case of colored hosts each band of the watermark is independently embedded into the corresponding band of the host and all the bands are stitched together to generate the color watermarked image. However, we convert the logo into gray scale to embed into gray-scaled hosts. Inverse Discrete Cosine Transformation (IDCT) block by block can be applied to the encoded image (c^*) resulting from DCT block fusion in the above step to produce the watermarked image in the spatial domain.

6 Watermark Extraction and Authentication

Fig. 5 depicts the modular scheme for watermark extraction in our proposed invisible watermarking scheme. In a naive situation where a watermarked image is not tampered, we need only to compute the block-wise DCT coefficients of the host and the watermarked image. The ex-

traction process being non-blind, availability of the originally used data- the host, the watermark, the bit sequence, and scaling parameters, is presumed. We *extract* the watermark from the watermarked image in DCT domain by using the mathematical formula which actually reverses the watermark embedding operation defined by the following equation:

$$w_{i,j}^k = \frac{b_{i,j}^k (c_{i,j}^{*k} - c_{i,j}^k)}{\alpha_{i,j}^k}. \quad (9)$$

Block-wise IDCT processing of the DCT domain watermark obtained as above gives the extracted watermark in the space domain. To determine how far the extracted watermark matches the stored original, we use the template matching (or correlation detection) algorithm which computes the correlation coefficient γ between the two images using the formula:

$$\gamma = \frac{\sum_{i,j}(we_{i,j} - \mu e)(ws_{i,j} - \mu s)}{\sqrt{\sum_{i,j}(we_{i,j} - \mu e)^2 \sum_{i,j}(ws_{i,j} - \mu s)^2}}, \quad (10)$$

where we and ws are the extracted and stored watermarks, and μe and μs, their pixel mean values, respectively. The subscript i, j of an image variable (we or ws) denotes the index of an individual pixel of the corresponding image. The summations are over all the image pixels. During extraction and authentication in color images, the watermark is extracted from each of the color bands. The mathematical formula used to compute a matching score for the extracted watermark is given below:

$$\gamma_{color} = \frac{\sum_{b,i,j}(we_{b,i,j} - \mu e_b)(ws_{b,i,j} - \mu s_b)}{\sqrt{\sum_{b,i,j}(we_{b,i,j} - \mu e_b)^2 \sum_{b,i,j}(ws_{b,i,j} - \mu s_b)^2}}, \quad (11)$$

where b denotes a color band, red (R), green (G) and blue (B) of the test color image.

The *authentication* process used in our approach uses the correlation (corr or γ) value provided by the correlation detector for decision making. It has two states. In the 'Initial' state, if it receives a $\gamma \geq 0.7$, it can authenticate (by setting its output z1 to 1) the presence of a copy of the stored watermark in the test image. Similarly, for a $\gamma \leq 0.4$, it can authenticate the absence of the watermark and hence sets it z3 output to 1. However, for values of γ between these two values, it sets its output z2 to 1 and goes to 'Uncertain' state. This necessitates further testing. As we show in the next section on our experimental results, the watermarked images, when restored after being subjected to some forms of distortion (*e.g.* noise addition), will yield very distorted watermarks possibly because of the over-smoothing of the watermarked images compared to the original hosts. The watermarks extracted after subjecting the host also to the same kind of smoothing were found to be of improved quality. For this reason, we used two multiplexors which will

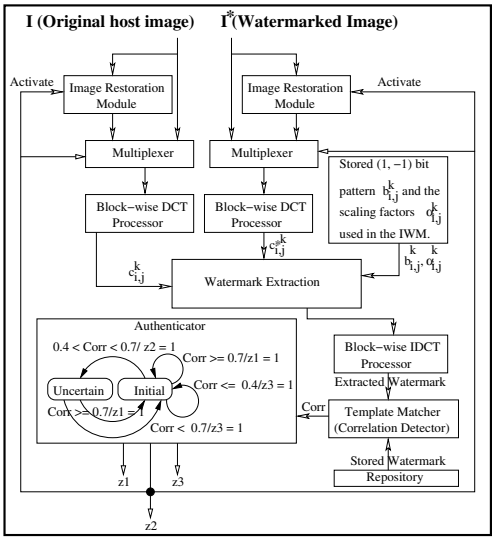


Figure 5. Algorithm for Watermark Extraction

forward symmetrically the two processed (smoothed) versions of the host and the watermarked images for the same processing as before. This is triggered by the z2 input of the authenticator which is currently in 'Uncertain' state. If the new $\gamma \geq 0.7$, it will authenticate the presence of the watermark, otherwise, its absence.

7 Experimental Results

Our experimentation with several images reveals the efficacy of our proposed algorithm in producing visually pleasing watermarked images similar to the sample results for gray scale images presented in Fig. 6 and color images in Fig. 7. We have chosen a standard block size of 8×8 pixels and sub-image of size 5×5 blocks in the experiments. We implemented our proposed algorithm in MATLAB. It was observed that typical execution time for watermarking in a Pentium 4, $3.2GHz$ computer with $1GB$ memory was $2sec$ for an image of size 256×256. The quality of the watermarked images using our method has been compared with existing watermarking techniques in terms of Peak Signal to Noise ratio (PSNR) values in decibels (dB) given by the following expression:

$$PSNR = 20\ log_{10}\left(\frac{255}{RMSE}\right), \quad (12)$$

where $RMSE$ is the root mean square error of the extracted watermark compared to the stored original. We have found the PSNR value of the watermarked image is having superior value compared to other existing watermarking schemes. The average PSNR value for the gray scale watermarked images was found to be approximately $48dB$.

(a) Original Lena (b) Watermarked Lena

(c) Original bear (d) Watermarked bear

Figure 6. Watermarking of Gray scale Images

(a) Original Color kid (b) Watermarked Color kid

(c) Original Color Lena (d) Watermarked Color Lena

Figure 7. Watermarking of Color Images

Table 1. Quality of the watermarked image after attacks and the quality and recognizability of the extracted watermark for gray scale Lena

Attack Type	Restored Image PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	38.02	0.9964
JPEG Compression (QF=60)	39.98	24.44	0.7575
Size Quadrupling and Resizing back	38.99	24.36	0.6942
Gaussian Blurred	43.42	29.50	0.9880
White Noise	42.95	27.01	0.9180
Sharpened	31.63	19.09	0.7232

Table 2. Quality of the watermarked image after attacks and the quality and recognizability of the extracted color watermark for Color Lena

Attack Type	Restored Image PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	35.17	0.9947
JPEG Compression (QF = 60)	38.30	24.69	0.7930
Size Quadrupling and Resizing back	40.09	26.82	0.9081
Gaussian Blurred	46.54	30.43	0.9856
White Noise	42.95	27.63	0.9286
Sharpened	34.58	21.96	0.7707

We used two metrics for assessing the attack resilience of the watermarks created by our approach: (1) Quality metric: PSNR of the extracted watermark in decibels and (2) Recognizability metric: the correlation coefficient γ (defined in 10) between the extracted and original watermarks. For visual inspection of the quality and recognizability of the extracted watermarks, we present in Fig. 8 and 9 the results obtained with watermarked images restored from various types of degradations. Results of our quantitative analysis using the two metrics is summarized in Table 1, 2. These results indicate that the restorations (*e. g.* noise pruning) involving smoothing of the watermarked image are the most pernicious for the watermarks. However, a symmetric smoothing of the stored host seems to remedy this problem. The results for color watermarked images are obtained after converting the images into gray scale images.

8 Conclusions

We presented a novel approach for the creation of invisible watermark and its embedding. The experimental results presented on the quality and recognizability of extracted watermarks demonstrate the performance of our method under various attacks. We converted the original colored logo to gray scale to implant into gray scale hosts. We have tested the algorithm for several standard test images. The quantitative measure of the extracted watermark for both gray scale and color images shows the resilience against different attacks. We are currently investigating a blind extraction method for the proposed scheme. This will be followed by a complete hardware based system implementation.

(a) No attack (b) Compressed (c) Resized

(d) Blurred (e) White Noise (f) Sharpened

Figure 8. Watermark Extracted from Grayscale Lena after Different Attacks

(a) No attack (b) Compressed (c) Resized

(d) Blurred (e) White Noise (f) Sharpened

Figure 9. Watermark Extracted from Color Lena after Different Attacks

References

[1] G. W. Braudaway, K. A. Magerlein, and F. Mintzer. Protecting Publicly Available Images with a Visible Image Watermark. In *Proceedings of the SPIE Conference on Optical Security and Counterfiet Deterrence Technique (Vol. SPIE-2659)*, pages 126–132, 1996.

[2] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. *IEEE Journal on Selected Areas in Communications*, 16(4):573–586, May 1998.

[3] C. Fei, D. Kundur, and R. H. Kwong. Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression. *IEEE Transactions on Image Processing*, 13:126 – 144, Feb 2004.

[4] R. L. G. Langelaar and J. Biemond. Watermarking by dct coefficient removal: Statistical approach to optimal parameter settings. In *Proc. SPIE IS&T/SPIE's 11th Annu. Symp on Electronic Imaging: Security and Watermarking of Multimedia Contents*, volume 3657, January 1999.

[5] S. S. X. L. Y.-D. K. Gangyi Jiang, Mei Yu. New blind image watermarking in dct domain. In *Proceedings of the 6th International Conference on Signal Processing*.

[6] M. Holliman and N. Memon. Counterfeiting attack on oblivious blockwise independent invisible watermarking schemes. In *IEEE Transactions on Image Processing*, volume 9, pages 432–441, March 2000.

[7] I.J.Cox, J. Kilian, T. Shamoon, and T. Leighton. Secure Spread Spectrum Watermarking of Images, Audio and Video. In *Proceedings IEEE International Conf on Image Processing*, volume 3, pages 243–246, 1996.

[8] C.-S. Lu, H.-Y. M. Liao, S.-K. Huang, and C.-J. Sze. Cocktail watermarking on images. In *Information Hiding*, pages 333–347, 1999.

[9] Z.-M. Lu, D.-G. Xu, and S.-H. Sun. Multipurpose image watermarking algorithm based on multistage vector quantization. *IEEE Transactions on Image Processing*, 14(6):822–831, 2005.

[10] F. C. Mintzer, et al., Towards online Worldwide Access to Vatican Library Materials. *IBM Journal of Research and Development*, 40(2):139–162, Mar 1996.

[11] S. P. Mohanty. Digital Watamerking of Images. Master's thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999.

[12] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli. A Dual Watermarking Technique for Images. In *Proceedings of the 7th ACM International Multimedia Conference (Vol. 2)*, pages 49–51, 1999.

[13] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli. A DCT Domain Visible Watermarking Technique for Images. In *Proceedings of the IEEE International Conference on Multimedia and Expo*, pages 1029–1032, 2000.

[14] W. Osberger and A. J. Maeder. Automatic identification of perceptually important regions in an image. In *Proceedings of the 14th IEEE Int. conf. on Pattern Recognition*, pages 701–704, August 1998.

[15] Y.-T. Pai, S.-J. Ruan, and J. Götze. Energy-efficient watermark algorithm based on pairing mechanism. In *Lecture Notes in Computer Science (LNCS), KES (1)*, pages 1219–1225, 2005.

[16] R. C. Reininger and J. D. Gibson. Distributions of the Two-Dimensional DCT Coefficients for Images. *IEEE Trans. Communications*, 31(6):835–839, June 1983.

[17] B. Shen and I. K. Sethi. Direct feature extraction from compressed images. In *Storage and Retrieval for Image and Video Databases (SPIE)*, pages 404–414, 1996.

[18] M. Topkara, A. Kamara, M. Atallah, and C. Nita-Rotaru. ViWiD: Visible Watermark Based Defense Against Phishing. *Lecture Notes in Computer Science (LNCS), IWDW 2005*, 3710:470–484, 2005.

[19] L. Xie and G. Arce. Joint wavelet compression and authentication watermarking. In *IEEE International Conference on Image Processing*, pages 427–431, Oct 1998.

[20] Y. Zhao, P. Campisi, and D. Kundur. Dual domain watermarking for authentication and compression of cultural heritage image. *IEEE Transactions on Image Processing*, 13(3):430–448, 2004.