Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas, Denton, TX 76207.
Email: smohanty@cse.unt.edu
and
Bharat K. Bhargava
Dept. of Computer Science
Purdue University, West Lafayette, Indiana, 47907.
Email: bbshail@purdue.edu

This paper presents a novel invisible robust watermarking scheme for embedding and extracting a digital watermark in an image. The novelty lies in determining a perceptually important sub-image in the host image. Invisible insertion of the watermark is performed in the most significant region of the host image such that tampering of that portion with an intention to remove or destroy will degrade the esthetic quality and value of the image. One feature of the algorithm is that this sub-image is used as a region of interest for the watermarking process and eliminates the chance of watermark removal. Another feature of the algorithm is the creation of a compound watermark using the input user watermark (logo) and attributes of the host image. This facilitates the homogeneous fusion of a watermark with the cover image, preserves the quality of the host image, and allows robust insertion-extraction. Watermark creation consists of two distinct phases. During the first phase, a statistical image is synthesized from a perceptually important sub-image of the image. A compound watermark is created by embedding a watermark (logo) into the statistical synthetic image by using a visible watermarking technique. This compound watermark is invisibly embedded into the important block of the host image. The authentication process involves extraction of the perceptive logo as well statistical testing for two-layer evidence. Results of the experimentation using standard benchmarks demonstrates the robustness and efficacy of the proposed watermarking approach. Ownership proof could be established under various hostile attacks.

Categories and Subject Descriptors: H.4.3 [**Information systems applications**]: Communications Applications

General Terms: Image, Content Protection, Copyright Protection

Additional Key Words and Phrases: Watermarking, Invisible Watermarking

1. INTRODUCTION

Digital watermarking is a method to hide some information that is integrated with a multimedia object [Voloshynovskiy et al. 2001; Sequeira and Kundur 2001]. The object may be any form of multimedia, such as, image, audio, video, or text. Electronic watermarking was invented in 1954 by Emil Hembrooke of the Muzac Corporation [Cox and Miller 2002]. Experts from computer science, cryptography, signal processing, and communications have worked together to develop watermarks suitable for various applications. Digital watermarking provides value-added protection on top of data encryption and scrambling for content protection and effective digital rights management. Digital watermarking raises a number of questions [Cox and Miller 2002], and still need to be addressed. This will allow the development of foolproof commercial watermarking systems [DWA 2007].

Watermarking has many different applications [Barnett 1999; Bender et al. 2000; Cox and Miller 2002; DWA 2007], such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. Watermarking schemes do not work effectively for all types of media and universally for various diverse applications. Depending on the target application and type, each watermark must satisfy certain characteristics [Mintzer et al. 1997]. The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks [Petitcolas et al. 1999; Voloshynovskiy et al. 2001]. The requirements for fulfilling desired characteristics and for succeeding against attacks are mutually conflicting [Heileman et al. 1999; Servette et al. 1998]. Several benchmark suites for testing performance robustness that combine many possible attacks into a unified framework are available [Voloshynovskiy et al. 2001; Guitart et al. 2006; Khan and Mirza 2007; Kutter and Petitcolas 1999].

A watermarking scheme consists of three parts: the watermark, the encoder, and the decoder and comparator [Memon and Wong 1998]. The watermarking algorithm incorporates the watermark into the object, whereas the verification algorithm authenticates the object by determining the presence of the watermark and its actual data bits. Available techniques use different transform domains to embed the watermark inspired by information coding and image compression. The watermarking is performed in the cover (host) image through several domains such as discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT), and fractal transform [Mohanty et al. 2006]. The watermarking algorithm proposed in this paper uses DCT ideas. Based on human perception, digital watermarks can be either visible or invisible. A visible watermark is a secondary translucent mark overlaid on the primary image and is visible to a viewer on careful inspection. The invisible watermark (may be either robust or fragile) is embedded in such a way that modifications made to the pixel value are perceptually unnoticeable and can be recovered only with an appropriate decoding mechanism. In multiple watermarking, two or three watermarks are embedded for copyright protection, content authentication, or captioning [Hua et al. 2001]. Since starting with IBM's Vatican Library project [Mintzer et al. 1996], visible watermarking technology progressed significantly [Mohanty et al. 2000; Hu and Kwong 2001; Topkara et al. 2005]. Invisible-robust watermarking was initiated by the research teams of Cox [Cox et al. 1997], Craver [Craver et al. 1998], and others. This paper is for invisible-robust watermarking.

Many social, legal, and technical issues need to be resolved before the watermarking schemes can serve in practice in a society's legal framework. The visible watermarking scheme has been used by IBM in the Vatican library project [Mintzer et al. 1996]. Invis-

ible watermarking has the greatest need for standardization [Mintzer et al. 1998]. For an invisible watermarking technique, the robustness property alone is not sufficient to guarantee content protection [Craver et al. 1998]. Application-specific watermarking techniques need to be developed with standard encoder-decoder systems incorporated in multimedia devices. Their development requires the formation of a standards body [Eskicioglu and Delp 2001; Cox and Miller 2002; Maes et al. 2000]. A well-known technical group involved with content stored on digital video discs (DVDs) is the Copy Protection Technical Working Group. For audio, the Secure Digital Music Initiative is standardizing watermarking technology. The legal framework provided for the applicability of digital watermarking is through the Digital Millennium Copyright Act, which protects against deliberate removal of, or attacks on, the watermark [Eskicioglu and Delp 2001]. Recently, the use of watermarking is being explored for digital video broadcasting [DWA 2007].

The contributions of this paper are summarized in Section 2. The relevant related research works that served as motivation for this research are discussed in Section 3. Section 4 presents 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 by using our scheme. Experimental results on the performance of our invisible watermarking scheme are presented in Section 7. Section 8 discusses conclusions of the paper with pointers for future research.

2. NOVEL CONTRIBUTIONS OF THIS PAPER

A schematic overview of the proposed watermarking method is presented in Fig. 1. The proposed algorithm initially 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). Whereas 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 of same size of the host sub-image. The input "key" has three parts: one part is used as a seed for Gaussian random number generation, another is used for Laplacian random number generation, and the last part is used for pseudorandom number generation. The synthetic image created supplements the robust extraction of the watermark for verification and authentication. A "compound watermark (image)" is created by fusing the user-given distinct and recognizable logo to the synthetically generated image. This compound watermark is then invisibly implanted in the host image at the same location as the perceptually most (as discussed in Section 4) important sub-image of the host color (gray-scale) image.

The motivation behind making a compound image for use as a watermark is that the compound image, which is adaptively created using host image statistics, will follow the original image faithfully and enable high-quality, image-friendly watermarking. This in turn will optimal for watermarking robustness and quality. Based on this consideration, we propose a strategic feedback-based approach to create and insert watermarks in host images and extract and authenticate the watermarks from possibly corrupted test images. The extraction of a perceptible watermark logo provides strong evidence of ownership. The watermark is robust because it is image-adaptive and secure because it is embedded in the perceptible, important sub-image. In the case of aggressive and severe attacks, if the

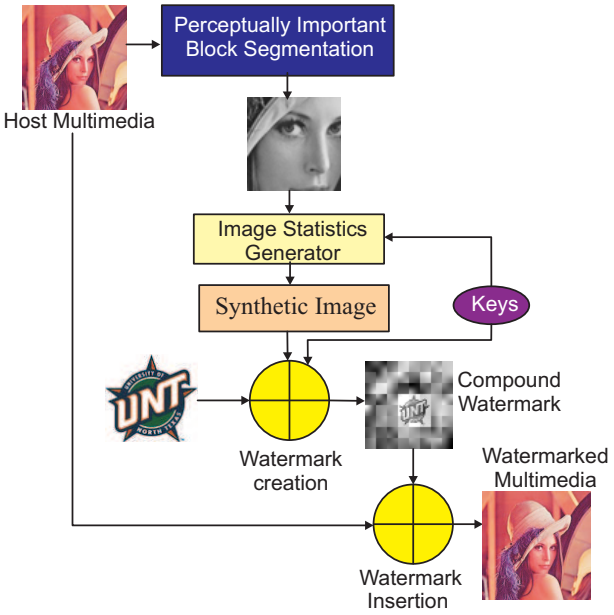


Fig. 1. Schematic Overview of our Proposed Novel Watermarking Scheme

watermark logo is not perceptually noticeable, then statistical techniques can be used for second-level authentication.

Our contributions to the advances in the state-of-the-art invisible-robust watermarking are summarized as follows:

(1) *Automatically determining a perceptually significant region for watermarking*: The proposed algorithm automatically determines the most perceptual significant region (sub-image) as the candidate for watermark insertion by considering various attributes, such as intensity, contrast, texture, center-quartile location, and edge of the cover (host) image.

(2) *Optimizing watermarking robustness and quality*: The algorithm uses the following approaches for robustness and quality trade-offs:
   (a) It creates a "compound image" by fusing a perceptual meaningful logo and a synthetic image and uses it as an effective watermark. The compound watermark ensures homogeneous fusion of the watermark with the cover image, preserving the quality of the host image, and robust insertion-extraction process.
   (b) The existing techniques use a Gaussian random number or pseudorandom number as a watermark and modify the alternating current (AC) DCT coefficients without considering the distribution of the DCT coefficients; thus, they may not result in an optimal approach for quality and robustness. In our approach, we modify both the direct current (DC) and the AC coefficients of DCT accounting for their distributions. We propose to use a Gaussian random number for DC coefficients and Laplacian for AC coefficients as optimal solutions for quality and robustness.
   (c) Use three types of scaling factors instead of one factor used in existing approaches to improve watermarked image quality.

(d) Use addition and subtraction operations based on pseudorandom sequence instead of one type of operation used in existing approaches to improve watermarked image quality and watermarking robustness.

(3) *Increasing watermarking security*: To increase watermarking security, we adopted the following methods:
   (a) Invisible insertion of the watermark in the most significant region of the host image such that tampering of that portion with intention to remove or destroy the watermark will degrade the esthetic quality and value of the image.
   (b) Use of three keys instead of one key to improve watermarking security.

(4) *Reliably extracting the logo to strengthen proof in a court of law*: To use watermarking as strong evidence in a court of law, the authentication process involves extraction of the perceptive logo to make ownership proof obvious. As a second-layer proof, statistical authentication testing is adopted, thus significantly reducing the chances of false detection of ownership.

3. RELATED PRIOR RESEARCH WORKS

Many watermarking algorithms have been proposed by researchers to maintain the originality and integrity of networked digital multimedia contents. Invisible-robust watermarking of digital images is one of the leading research areas. In this section, we discuss selected important contributions from the existing literature.

One of the earliest works by Cox et al. [Cox et al. 1997] uses the spread spectrum technique to embed a watermark in the DCT domain. To improve this method, Lu et al. [Lu et al. 1999] used a cocktail watermark to improve robustness and HVS to maintain high fidelity of the watermarked image. Langelaar and Biemond [Langelaar et al. 1999] propose an algorithm to embed a bit sequence in a digital image by selective removal instead of modification of DCT coefficients in smooth regions. This technique may result in visual artifacts. Fei et al. [Fei et al. 2004] analyze the performance of block-based watermarking schemes in the presence of lossy compression. A hybrid watermarking algorithm that has greater resilience to JPEG compression has been presented. Lu et al. [Lu et al. 2005] present 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. [Jiang et al. 2002] proposed a blind watermarking scheme in a DCT domain which exploits HVS characteristics to generate watermarked images with high visual quality. With respect to strategies which break watermarking schemes, the work of Holliman and Memon [Holliman and Memon 2000] describes a class of attacks on certain block-based oblivious watermarking schemes. Another frequency transform technique, DWT, has been used by researchers for digital image watermarking [Xie and Arce 1998]. Zhao et al. [Zhao et al. 2004] propose a DCT-DWT domain and dual watermarking scheme exploiting the orthogonality of image sub-spaces to provide robust authentication.

One spatial domain watermarking technique which is invisible, robust to geometric attacks and based on affine transformations is presented by Wu et al. [Wu et al. 2001]. Kang and Delp [Kang and Delp 2004] propose an invisible-robust watermarking technique in a three-dimensional DCT domain for volume data in which a two-dimensional black-and-white image is hidden as watermark. Kundur and Hatzinakos [Kundur and Hatzinakos

2004] present FuseMark which is based on the principles of image fusion. Saxena and Gupta [Saxena and Gupta 2007] present a collusion resistant watermarking scheme. These watermarking algorithms hide a simple two-level image compared to our algorithms that hides a color or gray scale watermark image.

Qi et al. have propose adaptive digital image watermarking method for both spatial and DCT domain processing [Qi et al. 2008]. Planitz and Maeder propose a region dependent watermarking scheme for medical images [Planitz and Maeder 2005]. Different techniques incorporating human visual system models in watermarking has been introduced by Wolfgang et al. [Wolfgang et al. 1999]. Podilchuk and Wenjun present image watermarking techniques considering visual models in image compression framework [Podilchuk and Wenjun 1998]. Yeung et al. [Yeung et al. 1997] discuss several techniques classified by their appearance and application domains for high-quality image watermarking. A list of watermarking method discussed and need of perceptual modeling is emphasized by Cox and Miller [Cox and Miller 1997].

Because watermarking is used for copyright protection, researchers investigate the design of high-performance, low-power hardware-based watermarking systems for real-time applications. Though DWT yields better peak signal-to-noise ratio (PSNR) values compared to DCT, researchers are designing DCT-based watermarking systems for hardware implementation because of the ease of implementation [Pai et al. 2005; Tsai and Lu 2001]. Mohanty et al. [Mohanty et al. 2006] propose a low-power watermarking chip that can insert both invisible and visible watermarks in images in the DCT domain.

Despite significant advances, research still needs to address many challenges related to attack resilience and robustness. Much of the current research attempts to embed a pseudorandom sequence as a watermark; however, a source-based watermark like a unique identifiable color logo is more appealing for easy identification of ownership, authentication, and acceptance as legal evidence. Thus, we address the issue of strategically creating and implanting a watermark with the dual purpose of attack prevention and detection.

4. PROPOSED APPROACH FOR IMAGE ADAPTIVE WATERMARK CREATION

We discuss the approach for creating a synthetic compound watermark. The user can use a gray-scale or color image as a watermark. The notations used to explain the algorithm throughout the paper are listed in Table I.

4.1 Automatic Detection of a Significant Sub-Image Considering HVS Sensitivity

To automatically find out the sensitive and perceptually important region (or sub-image) of an image with respect to human perception, we need to understand the metrics that influence the HVS. Earlier research works [Osberger and Maeder 1998; Mohanty et al. 1999; 2000] have identified many factors that influence the visual attention of humans. They have identified several metrics as discussed below for determining the perceptually most sensitive set of blocks (collectively called sub-image) of the image. It may be noted that a block is a matrix of 8×8 pixels, the same size as that used for standard DCT computation in JPEG compression. We are interested in *automatically* determining a contiguous and perceptually significant set of N_B blocks constituting a "sub-image." The size of the sub-image is lower because it is bound by the size of watermark logo (image).

To determine the sub-image B_i of interest, we divide the host image into 8×8 blocks and considered a sliding square window containing N_B of such blocks (a tentative sub-image of size $\sqrt{N_B} \times \sqrt{N_B}$ blocks). The sliding window moves across the image and

Table I. Algorithm notations

I	: Original (or host) image (a color or gray-scale image).
W	: Watermark logo (a color or gray-scale image).
I^*	: Watermarked image (a color or gray-scale image).
W_e	: Extracted watermark logo (a color or gray-scale image).
N_B	: Number of contiguous blocks in a sub-image.
b_i	: i-th block of size 8×8 pixels.
B_i	: Sub-image consisting of N_B number of b_i blocks.
N_I	: Number of 8×8 b_i blocks of the overall image I.
$\chi_{intensity}$	: Intensity metric to quantify comparative intensity significance of a sub-image.
$\chi_{contrast}$	: Contrast metric to quantify contrast significance of a sub-image.
$\chi_{location}$	: Location metric of a sub-image to quantify significance with respect to center quarter.
$\chi_{edginess}$	: Edginess metric to quantify significance of edge containing sub-image.
$\chi_{texture}$	: Texture metric to quantify texture significance of a sub-image.
χ	: Overall quantitative measure of perceptual significance of a sub-image.
$c_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of image block k.
$c^*_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of watermarked image block k .
$wo_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of watermark logo block k.
$ws_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of synthesized image block k.
$wf_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of compound watermark block k.
$we_{i,j,k}$	: DCT coefficient corresponding to position (i, j) of extracted watermark block k.
$G(\mu, \sigma)$	: Gaussian probability density function of mean μ and standard deviation σ.
$L(\mu, \sigma)$	: Laplacian probability density function of mean μ and standard deviation σ.
α_k and β_k	: Scaling factors corresponding to block k.
$b_{i,j,k}$	: Pseudorandom bit pattern $(1, -1)$ corresponding to block k.
$\alpha_{i,j,k}$	: Scaling factor corresponding to position (i, j) in block k.
γ	: Correlation coefficient for a gray-scale image.
γ_{color}	: Correlation coefficient for a color image.
$RMSE$	: Root mean square error.
$PSNR$	: Peak signal-to-noise ratio.

computes a quantitative measure (χ) for each of the influencing metrics at every location. We consider various attributes of the images, such as intensity, contrast, location, edginess, and texture to locate the appropriate sub-image as a candidate for watermark insertion. In the following sections, we discuss the significance of these attributes and propose metrics to quantify them. A metric χ is presented that captures the overall perceptual significance of a sub-image under consideration in a host or cover image.

4.1.1 *Intensity Metric.* The blocks of the image that are close to the mid-intensity of the image are more sensitive to the human eye [Mohanty et al. 1999; 2000]. The mid-intensity importance $\chi_{midintensity}$ of a sub-image B_i is computed as follows:

$$\chi_{intensity}\left(B_i\right) = \left|AvgInt\left(B_i\right) - MedInt(I)\right|, \tag{1}$$

where $AvgInt(B_i)$ is the average luminance of sub-image B_i, and $MedInt(I)$ is the average luminance of the overall image I. The metric $\chi_{midintensity}$ quantifies the perceptual significance of the sub-image with respect to the overall global intensity of the image. The intensity levels needs not be calculated from the spatial domain information; they can be calculated from the DC values of DCT coefficients for each block as follows:

$$AvgInt\left(B_i\right) \;=\; \frac{1}{N_B}\sum_{k=1}^{N_B} c_{0,0,k}, \tag{2}$$

$$MedInt(I) = \frac{1}{N_I}\sum_{k=1}^{N_I} c_{0,0,k}. \quad (3)$$

This calculation facilitates complete processing in DCT domain, which will eventually enable compressed domain processing.

4.1.2 *Contrast Metric.* A region of an image that has a high level of contrast with respect to the surrounding region attracts the human eye's attention and hence is perceptually more important than other regions [Osberger and Maeder 1998]. Thus, there is a need to quantify the contrast of an sub-image. We present metric $\chi_{contrast}$ to quantify the contrast aspects of a sub-image as

$$\chi_{contrast}(B_i) = |AvgInt(B_i) - AvgInt(B_{i-surrounding})|. \quad (4)$$

$AvgInt(B_i)$ is the average luminance of sub-image B_i and $AvgInt(B_{i-surrounding})$ is the average luminance of all the surrounding sub-images. $AvgInt(B_{i-surrounding})$ is computed same way as $AvgInt(B_i)$, but it is for the neighboring sub-images of sub-image i. The metric $\chi_{midintensity}$ quantifies the perceptual significance of the sub-image with respect to the surrounding (local) intensity. The metrics $\chi_{midintensity}$ and $\chi_{contrast}$ are different; the first one is with respect to global intensity and second with respect to local intensity. The metric $\chi_{contrast}$ can also be calculated in a DCT domain similar to that of $\chi_{intensity}$.

4.1.3 *Location Metric.* Eye focuses on the center quarter of the image [Osberger and Maeder 1998]. The center quarter of a screen is perceptually more important than other areas of the image. The location $\chi_{Location}$ of each sub-image is measured by computing the ratio of the number of pixels of the sub-image lying in the center quarter of the image to the total number pixels in the sub-image:

$$\chi_{location}(B_i) = \frac{center(B_i)}{Total(B_i)}. \quad (5)$$

The $center(B_i)$ is the number of pixels of the sub-image lying in the center quarter (25%) of the image, and $Total(B_i)$ is the total number of pixels of the sub-image; i.e., the area of the sub-image.

4.1.4 *Edginess Metric.* The HVS is sensitive to edge portion of the images because they capture attention easily compared to other portions. A sub-image that contains an edge is called an edge sub-image and must be handled carefully to ensure that the perceptual visibility of the image is not degraded. The edginess of the sub-image $\chi_{edginess}$ is also computed in the DCT domain [Shen and Sethi 1996; Mohanty et al. 2006]. A sub-image is declared an edge sub-image if the summation of absolute values of all the AC coefficients in the sub-image exceeds a predetermined threshold as suggested by [Shen and Sethi 1996] and [Mohanty et al. 2006]. Thus, the edginess of a sub-image is calculated as follows (when both i and j are indices for AC coefficients):

$$\chi_{edginess} = \left(\frac{\frac{1}{N_B}\sum_{k=1}^{N_B}\left(\frac{1}{63}\sum_i\sum_j |c_{i,j,k}|\right)}{\text{maximum}\left\{\frac{1}{N_B}\sum_{k=1}^{N_B}\left(\frac{1}{63}\sum_i\sum_j |c_{i,j,k}|\right)\right\}_{\forall \text{ sub-images in } I}} \right), \quad (6)$$

where maximum $\left\{ \frac{1}{N_B} \sum_{k=1}^{N_B} \left(\frac{1}{63} \sum_i \sum_j |c_{i,j,k}| \right) \right\}_{\forall}$ sub-images in $_I$ computes the maximum value of the mean of absolutes of AC coefficients across all sub-images in the image. A spatial domain operator like Sobel or Canny can be used for edge detection, but we used the DCT domain techniques because we intended to perform all processing in a DCT or compressed domain.

4.1.5 *Texture Metric.* A highly textured block is less sensitive to noise. Modification inside a highly textured block is unnoticeable to the human eye. The texture factor $\chi_{texture}$ is computed by adding the variance of all the AC coefficients of each block inside the window [Mohanty 1999]. It has been shown that a highly textured block has evenly distributed AC coefficients. A higher value variance indicates that the block is less textured. The texture metric of a sub-image is calculated as follows (when both i and j are indices for AC coefficients):

$$\chi_{texture}(B_i) = \frac{1}{N_B} \sum_{k=1}^{N_B} \left(\left(\frac{1}{63} \right) \sum_i \sum_j (c_{i,j,k} - \mu_{AC_k})^2 \right). \tag{7}$$

The $c_{i,j,k}$ is the $(i,j)th$ AC coefficient of the k-th block, and μ_{AC_k} is their mean and is calculated as follows:

$$\mu_{AC_k} = \left(\frac{1}{63} \right) \sum_i \sum_j c_{i,j,k}. \tag{8}$$

4.1.6 *Overall Perceptual Measure of a Sub-Image.* After performing the above computation for the windows, we assign an importance measure for each of the five metrics. The measure for each metric is normalized in the range $[0, 1]$, where 1 stands for maximum importance or significance. After the normalization, we combine the metrics for each window to produce an "overall importance (or significance) measure" (χ) for each sub-image. We chose to square and sum all the measures to produce the final metric (χ) for for each window/sub-image B_i as described by the following equation:

$$\begin{aligned} \chi(B_i) = [\chi_{intensity}(B_i)]^2 + [\chi_{contrast}(B_i)]^2 + [\chi_{location}(B_i)]^2 \\ + [\chi_{edginess}(B_i)]^2 + [\chi_{texture}(B_i)]^2. \end{aligned} \tag{9}$$

The calculated χ values for all the windows are sorted, and the window having the highest χ is selected as the perceptually most important region (sub-image). Our calculations of χ allows a higher significance to be given to sub-images that rank very strongly in some metrics [Osberger and Maeder 1998]. A simple average of the measures would not provide this. A square can increase the range of number and enable better decision making. Fig. 4 shows sample images in which significant region are identified using the above measure. It may be noted that there can be visually more than one perceptually important sub-images. However, the sub-image considered for watermarking is the one that has the maximum χ. We have observed in our experiments that this came out to be one and unique and value, thus selecting only one sub-image for watermarking.

4.2 Creation of the Watermark

The watermark creation process is shown in Fig. 2. The following steps generate a synthetic image from the perceptually important region. To create a compound watermark image we fuse it with a source-end logo.

(1) Divide the host image into an integral number of 8×8 blocks (after necessary image extensions). The subscripts (i, j, k) of various terms denote the block pixel indices (i, j) and the block k, respectively.

(2) Choose the blocks in the perceptually most important region of the host 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. Standard deviation of the k-th block can be calculated as follows (where i and j correspond to the AC coefficients):

$$\sigma_{AC_k} = \left(\frac{1}{63}\right) \sum_i \sum_j \left(c_{i,j,k} - \mu_{AC_k}\right)^2 . \tag{10}$$

(4) Synthesize a statistical image (in DCT space) of the same size as the aforementioned sensitive area of the image using the following equation:

$$ws_{i,j,k} = \begin{cases} G\left(c_{i,j,k}, \sigma_{AC_k}\right) & \text{if } i = j = 0 \text{ (i.e., DC coefficients);} \\ L\left(c_{i,j,k}, \sigma_{AC_k}\right) & \text{otherwise, AC coefficients.} \end{cases} \tag{11}$$

With the same denotation as above for k and (i, j), $c_{i,j,k}$ and $ws_{i,j,k}$ are the DCT coefficients of the host and synthetic images, respectively. $G(\mu, \sigma)$ and $L(\mu, \sigma)$ are Gaussian and Laplacian random variates, respectively, with the first parameter referring to the mean value of the distribution and the second parameter σ_{AC_k} referring to the standard deviation of block b_k. The choice of these two distributions for modeling the image DC and AC coefficients of DCT is motivated by empirical results presented in [Reininger and Gibson 1983] and [Mohanty 1999]. For most of the images, the DC DCT coefficients are Gaussian distributed, and the AC DCT-coefficients follow Laplace distribution. So, instead of using a Gaussian-type watermark (as used by many watermarking algorithms presented in the current literature), a watermark consisting of both Gaussian distribution (for DC coefficients) and Laplace distribution (for AC coefficients) is more robust; and at the same time, image quality is maintained.

(5) Divide the input watermark logo image into 8×8 blocks and obtain its block-wise DCT coefficients (wo's). It may be noted that the synthetic image size is lower bounded by the size of the input logo. In other words, the size of the synthetic image created above needs to be larger than the input watermark logo in order to accommodate it. Once the number of blocks N_B for the synthetic image is decided, the watermark logo image needs to be scaled down accordingly.

(6) Embed this logo in an insensitive area of the synthetic image using any DCT-based visible watermarking algorithm [Mohanty et al. 2000]. This step actually involves determination of two block-specific parameters α_k and β_k indicating the proportions of the the synthetic image and the watermark logo required for effective embedding. The block fusion equation for compound watermark creation is given below:

$$wf_{i,j,k} = \alpha_k \times ws_{i,j,k} + \beta_k \times wo_{i,j,k}. \tag{12}$$

Here, wf represents the final compound watermark, ws symbolizes the synthetic image and wo stands for the chosen input watermark logo.

The seed used by the random or pseudorandom number generator during the statistics generation is stored for use during authentication. For a color image, the image is initially

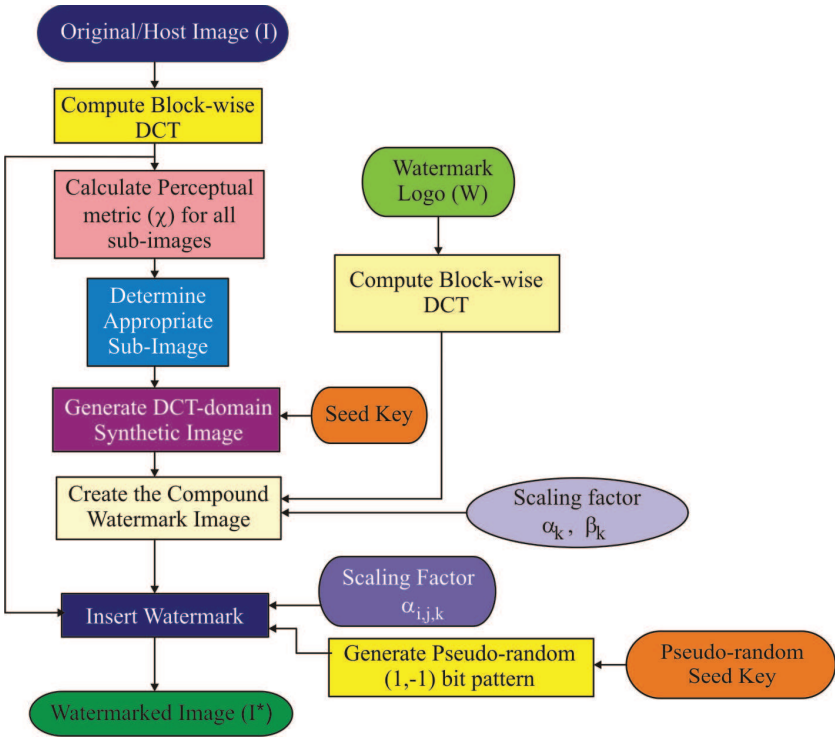


Fig. 2. Representation of the Proposed Watermark Creation and Insertion Process

converted to its (Y, C_r, C_b) color space, and the perceptually important region of the image is identified by analyzing its Y component. Once the region is identified, each band (red, green, blue) of the color image is considered for synthetic image creation followed by creation of the compound watermark image.

5. WATERMARK INSERTION PROCESS

As listed in Fig. 2, the following steps are used to insert the watermark. The compound watermark is now invisibly embedded into the host image by fusing the compound watermark (wf) blocks with the corresponding blocks of the earlier chosen perceptually important region of the host image. The DCT coefficients of the watermark are to be scaled appropriately to make the watermark invisible. The mathematical equation used for the invisible insertion of the final watermark into the host image is given below:

$$c^*_{i,j,k} = c_{i,j,k} + b_{i,j,k} \times \alpha_{i,j,k} \times wf_{i,j,k}, \tag{13}$$

where $c_{i,j,k}$ represents the DCT coefficients of the original host image and $c^*_{i,j,k}$ represents the DCT coefficients of the watermarked image.

We denote the scaling factor corresponding to an individual DCT term by $\alpha_{i,j,k}$. However, through experimentation with various images, we found that only two scaling factors need to be specified, one for the DC and the other for the AC coefficients. The values 0.02 and 0.1 for these two types of coefficients, satisfy quality and perceptibility, thus simplifying the computations. In order to make the presence of the watermark undetectable

by simple statistical analysis, we take a different approach than that in [Cox et al. 1997], wherein a watermark is added to the host at every term. We add the watermark to the host DCT coefficients at some positions and subtract from them at others, as suggested in [Craver et al. 1998]. The pseudorandom $(1, -1)$ bit pattern/sequence (denoted by $b_{i,j,k}$) determining the addition or subtraction involved at each pixel position could be any arbitrarily chosen pseudorandom sequence, but we choose to use an alternating sequence in the implementation.

For simplicity, we convert the logo into gray scale to embed it into gray-scale hosts. However, 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. An inverse DCT block by block can be applied to the encoded image resulting from the DCT block fusion in the above step to produce the image in the spatial domain.

6. WATERMARK EXTRACTION AND AUTHENTICATION

The watermark extraction process of the proposed invisible watermarking scheme is presented in Fig. 3. The extraction process is non-blind. So the availability of the originally used data (the host, the watermark, the bit sequence, and scaling parameters) is presumed. The blind decoding process does not need the original image for detection. Thus, watermarking based on blind detection is space (memory) efficient. However, such mechanisms do not extract watermarks, but rather they detect (decode) the watermark and prove ownership with the help of statistics. Thus, their usefulness in a court of law is weaker. A non-blind extraction approach is strongly useful in a court of law.

As the first step for extraction and authentication, the block-wise DCT coefficients of the original host image (I) and the possibly watermarked image (I^*) are computed. We extract the watermark from the watermarked image in the DCT domain by using a reverse process of insertion. The mathematical formula that actually reverses the watermark embedding operation is defined by the following equation:

$$we_{i,j,k} = \frac{b_{i,j,k} \times \left(c^*_{i,j,k} - c_{i,j,k}\right)}{\alpha_{i,j,k}}. \tag{14}$$

Block-wise inverse DCT processing of the DCT domain watermark obtained as above gives the extracted watermark in a spatial domain. If the input watermark logo is present in this extracted work W_e, then the ownership is established right away. But in some cases, when the logo is not visibly present on the extracted watermark, if the test image was really not watermarked, or it is needed for second layer proof, then further processing is necessary. This leads to the authentication steps presented below.

To establish authentication, we used the template matching (or correlation detection) algorithm that computes the correlation coefficient γ between the two images using the following equation:

$$\gamma = \frac{\sum_{i,j} \left(we_{i,j} - \mu e\right) \left(wf_{i,j} - \mu f\right)}{\sqrt{\sum_{i,j} \left(we_{i,j} - \mu e\right)^2 \sum_{i,j} \left(wf_{i,j} - \mu f\right)^2}}, \tag{15}$$

where we and wf are the extracted and stored watermarks, and μe and μf are their pixel mean values, respectively. The subscript i, j of an image variable (we or wf) denotes the

index of an individual pixel of the corresponding image. The summations are over all the image pixels.

During extraction and authentication of 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 in the following equation:

$$\gamma_{color} = \frac{\sum_{b,i,j} \left(we_{b,i,j} - \mu e_b\right)\left(wf_{b,i,j} - \mu f_b\right)}{\sqrt{\sum_{b,i,j} \left(we_{b,i,j} - \mu e_b\right)^2 \sum_{b,i,j} \left(wf_{b,i,j} - \mu f_b\right)^2}}, \tag{16}$$

where b denotes a color band (red, green, and blue) of the test color image, we_b are the extracted marks from the different bands of the test color image, and wf_b are the compound watermarks in the respective color bands. The μe_b and μf_b are the pixel mean values in red, green, and blue bands of the extracted watermark and stored watermark, respectively. The subscripts i, j of an image variable (we_b or wf_b) denote the index of an individual pixel of the corresponding image. The summations are over all the image pixels.

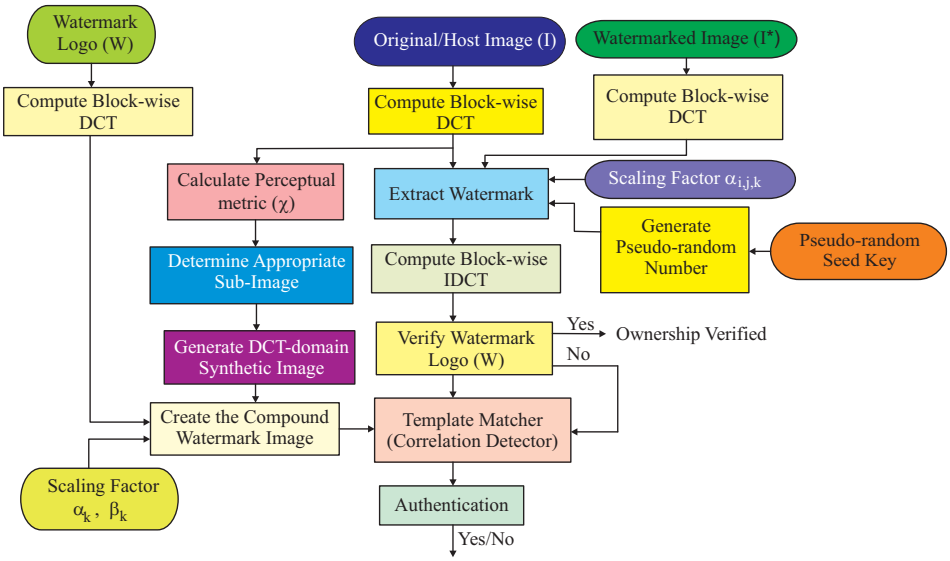


Fig. 3. Proposed watermark extraction and authentication process

The authenticator module used in our approach uses the correlation (corr or γ) value provided by the correlation detector for decision making. There are two possible cases. In the first case, if the module receives a $\gamma \geq 0.7$, it can authenticate the presence of a copy of the stored watermark in the test image and establish ownership. Similarly, for a $\gamma \leq 0.4$, it can authenticate the absence of the watermark and hence ownership is not established. However, for values of γ between these two values, the case is "uncertain"and necessitates further testing. As shown in the experimental results, when a watermarked image is restored, after some types of distortion, it will yield distorted watermarks. This is possibly because of the oversmoothing of the watermarked images compared to the original hosts. The watermarks extracted after subjecting the host image to the smoothing

filter were found to be of improved quality. Thus, we propose to forward symmetrically the two processed (smoothed) versions of the host and the watermarked images for the same processing as before. In this case, the authenticator has to give a decisive outcome based on the γ received from the revised processing. If the new $\gamma \geq 0.7$, it will authenticate the presence of the watermark; else its absence.

7. EXPERIMENTAL STUDIES

7.1 Experimental Setup

We implemented the proposed algorithm in MATLAB. The computation platform was a a Pentium 4 processor with a speed of $3.2GHz$ and $1GB$ of memory. A larger volume of benchmark images was used for experiments, but only results for selected benchmark images are presented for brevity. Similarly, a large set of logos was used in the experiment, but results are presented for one logo for brevity as well due to the fact that proposed watermarking scheme is independent of watermarking logo. We have chosen a standard block size of 8×8 pixels and a sub-image size of 5×5 blocks.

7.2 Testing Automatic Region Identification and Watermark Creation

The first phase of the experiments involved testing the automatic identification of the perceptually important region of the images. The perceptually most significant sub-image found by our approach in the Lena and bear images are shown in Fig. 4 for a block size of $8 \times 8 = 64$ pixels and a sub-image (window) size of N_B of $5 \times 5 = 25$ blocks. Similarly, it can be computed for any size N_B of a sub-image. It was observed that the algorithm could identify the important region for both gray-scale and color images.

(a) Lena (b) Bear

Fig. 4. Automatic determination of perceptually important sub-images in test images

The algorithm was tested for its effectiveness to create the compound watermark. The values of α_k and β_k were assumed to be 0.9 and 0.1. The algorithm could create a compound watermark for all test cases with the input logo visible. Fig. 5 depicts the creation of a sample compound watermark.

(a) Synthetic image created from the host (b) Watermark logo (c) Compound image created for use as a watermark

Fig. 5. A compound watermark created from the Lena image

7.3 Testing Watermark Insertion and Quality

To test the insertion of an invisible watermark, we performed experiments on a large number of gray-scale and color images. The experiments revealed the efficacy of the proposed algorithm in producing visually pleasing watermarked images. The value of the scaling factors was 0.02 for the DC coefficients and 0.01 for the AC coefficients. Selected results for gray-scale images are presented in Fig. 6 and for color images in Fig. 7. It was observed that the typical execution time for insertion was $2sec$ on a Pentium 4 processor with a speed of $3.2GHz$ and $1GB$ memory for an image with a size of 256×256. Thus, the time overhead of the algorithm was minimal. The storage requirement overhead was also very small because of only the keys needed to be stored by the owner to prove ownership. The memory requirement to store the keys is insignificant compared to the memory requirement of the host image.

The quality of the watermarked images using this method has been compared with existing watermarking techniques in terms of PSNR values in decibels (dB) given by the following expression [Kutter and Petitcolas 1999]:

$$PSNR = 20\, log_{10} \left(\frac{255}{RMSE} \right), \tag{17}$$

where $RMSE$ is the root mean square error of the watermarked image compared to the original image. The $PSNR$ for gray-scale Lena, gray-scale bear, color child image, and color Lena image are presented in 2nd column of Tables II, III, IV, and V, respectively. Similar values of $PSNR$ was observed for all the test images. The $PSNR$ for both color and gray images were alike. This demonstrates the efficacy of the proposed scheme, it works irrespective of content, type, and size of the images. We found the $PSNR$ value of the watermarked image had a superior value compared to other existing watermarking schemes. The average $PSNR$ value for the gray-scale watermarked images was found to

be approximately $48dB$. Thus, the watermarking insertion process produced high-quality watermarked images.

Our watermarking algorithm is unique in being image adaptive, considering distribution of DCT co-efficient, using multiple keys to improve security, hiding logo inside host, etc. together in an unified approach as stated in Section 2. To best our knowledge there is no other counterpart for direct comparison. Hence, we provide a broad perspective with watermarking selected algorithms that hide image inside image for fairness. The average $PSNR$ for [Wu et al. 2001] is $25dB$, which is approximately 50% lower in quality than our algorithm. The average $PSNR$ for [Saxena and Gupta 2007] is $30dB$, which is approximately 36% lower in quality than our algorithm. Similar observations were made compared to other related research works discussed in Section 3. It may be noted that these watermarking algorithms hide a simple two-level image compared to our algorithms that hides a color or gray scale watermark image.

7.4 Testing Watermark Extraction and Authentication, and Robustness

The last set of experiments involved testing the algorithm for extraction and authentication. We used two metrics for assessing the attack resilience of the watermarks created by our approach: (i) quality metric and (ii) recognizability metric. The quality mertic $PSNR$ of the extracted watermark is calculated with respect to the original in terms of decibels using equation of the previous of subsection. The recognizability metric is the the correlation co-efficient γ between the extracted and the original watermarks. For visual inspection of the quality and recognizability of the extracted watermarks, we present the results obtained with watermarked images restored from various types of degradations in Fig. 8. Fig. 9, Fig. 10, and Fig. 11. The experiments are performed for all the attacks provide in Stirmark [Petitcolas et al. 1998; Petitcolas 2000], such as cropping, compression, filtering, sharpening, transformation, etc. However, we have presented the results for a sub-set of attacks for brevity. The results are shown for gray-scale images of Lena and the bear and color images of the child and Lena, respectively. It is observed that the input logo was present in the extracted watermark for most of the test cases, thus proving ownership.

Results of our quantitative analysis using the two metrics are summarized in Tables II, III, IV, and V for gray-scale Lena, gray-scale bear, color child image, and color Lena image, respectively. The 3rd column of each of the above Tables represent $PSNR$ of the extracted watermark logo and 4th column of each Tables represent γ. These results establish a relationship between the quality of restoration of the distorted watermarked images and the quality and recognizability of the extracted watermarks. These results also indicate that the restorations (*e.g.,* noise pruning) involving smoothing of the watermarked image are the most pernicious for the watermarks. However, a uniform smoothing of the stored host seems to remedy this problem. The correlation values were approximately between 0.7 to 0.9 for all the test images and logo used in the experiments, an approximate range of 0.2. Our authentication algorithm is influenced by this observation. The correlation coefficient γ between the extracted and the original watermarks are observed to be in the range of values to establish ownership.

To provide a broad comparative perspective of the extraction process we discuss the $PSNR$ of the extracted logo watermark. For our algorithm the average $PSNR$ for all the test images, watermarks, and attacks is $24dB$. This $PSNR$ for [Saxena and Gupta 2007] that uses a two-level watermark logo and considers only JPEG compression of different quality factors as attack is $23dB$. This $PSNR$ for [Wu et al. 2001] and [Kundur and

Table II. Relationship between the quality of the invisible watermarking image restored from an attack and the quality and recognizability of the extracted watermark in the Lena image

Attack Type	Host Image's PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	38.02	0.9964
JPEG Compression	39.98	24.44	0.7575
Size Quadrupling and Resizing Back	38.99	24.36	0.6942
Median Filtered	38.22	24.33	0.8352
Gaussian Blurred (Blind Deconvolution)	43.42	29.50	0.9880
Sharpened	31.63	19.09	0.7232

Table III. Relationship between the quality of the invisible watermarking image restored from an attack and the quality and recognizability of the extracted watermark in the bear image

Attack Type	Host Image's PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	36.23	0.9967
JPEG Compression (Quality Factor = 50)	36.07	22.91	0.8693
Size Quadrupling and Resizing Back	36.59	23.43	0.8181
Median Filtered	34.23	21.61	0.8695
Gaussian Blurred (Blind Deconvolution)	45.83	31.03	0.9917
White Noise	43.21	26.94	0.9307

Table IV. Relationship between the quality of the invisible watermarking image restored from an attack and the quality and recognizability of the extracted color watermark in the color image of the child

Attack Type	Host Image's PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	33.80	0.9114
JPEG Compression	38.34	25.15	0.7217
Size Quadrupling and Resizing Back	42.88	29.31	0.7746
Median Filtered	41.43	27.39	0.8332
Gaussian Blurred (Blind Deconvolution)	48.52	30.77	0.8905
White Noise	42.98	27.85	0.8314

(a) Original Lena image (b) Lena image with an invisible watermark

(c) Original bear image (d) Bear image with an invisible watermark

Fig. 6. Results of invisible watermarking on gray-scale images

Hatzinakos 2004] that use a two-level watermark logo is $22dB$ and $25dB$, respectively. Our algorithm uses color or gray-scale logo and considers more severe and diverse attacks compared to this algorithm and hence has better performance. In addition our approach is highly robust to cropping as cropping of the image on the regions where watermark is not present does not affect the extraction or authentication. Cropping of the perceptual significant region of the image is not an attractive option as it would affect the value of the image and hence implicitly making the algorithm cropping resistant. Our authentication scheme further provides a statistical authentication as a second layer proof.

8. CONCLUSIONS AND FUTURE WORK

We present a novel approach for the creation of a watermark that homogeneously adapts to the host image. A watermark insertion, extraction, and authentication scheme is proposed.

(a) Original image of child

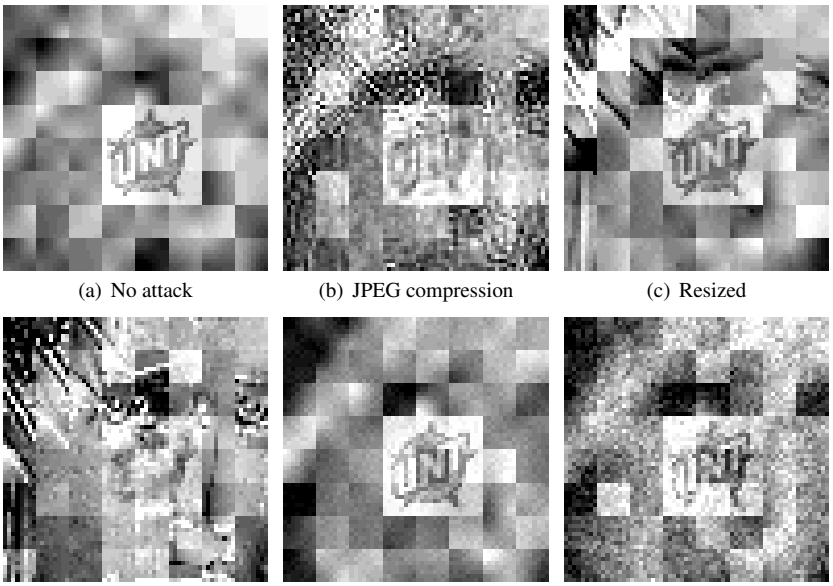
(b) Child's image with an invisible watermark

(c) Colored Lena image

(d) Colored Lena image with an invisible watermark

Fig. 7. Results of invisible watermarking on color images

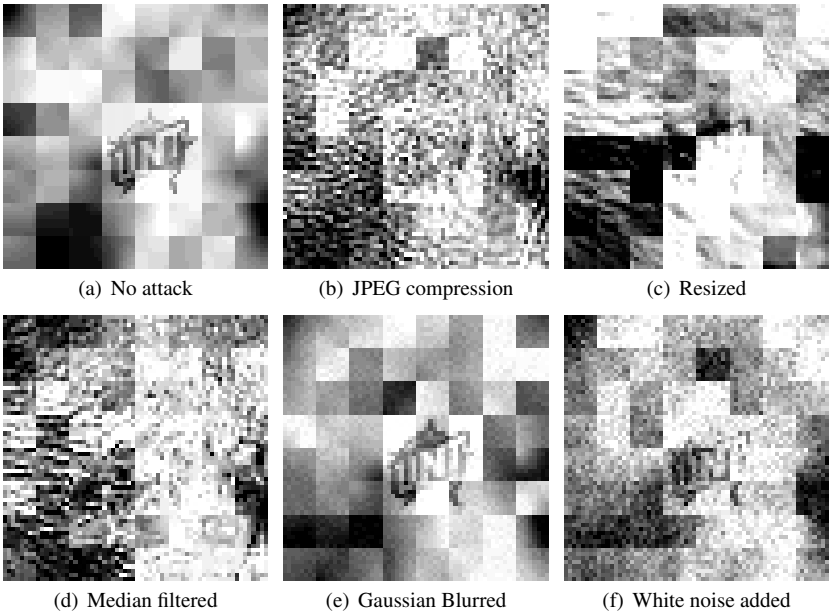
The watermark is inserted in the most perceptually significant sub-image, thus eliminating chances of its being subjected to severe digital attacks, which will reduce the value of the image. The experimental results presented on the quality and recognizability demonstrate the performance of our method under various attacks. We converted the original colored logo to gray scale to implant it 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 to different attacks. We are investigating a blind extraction method for the proposed scheme to compare its performance with that of the proposed non-blind scheme. This comparison will be followed by a complete hardware-based system implementation using field-programmable gate array technology and custom integrated circuit technology. The energy-efficient, low-power version of the



(a) No attack (b) JPEG compression (c) Resized

(d) Median filtered (e) Gaussian blurred (f) White noise added

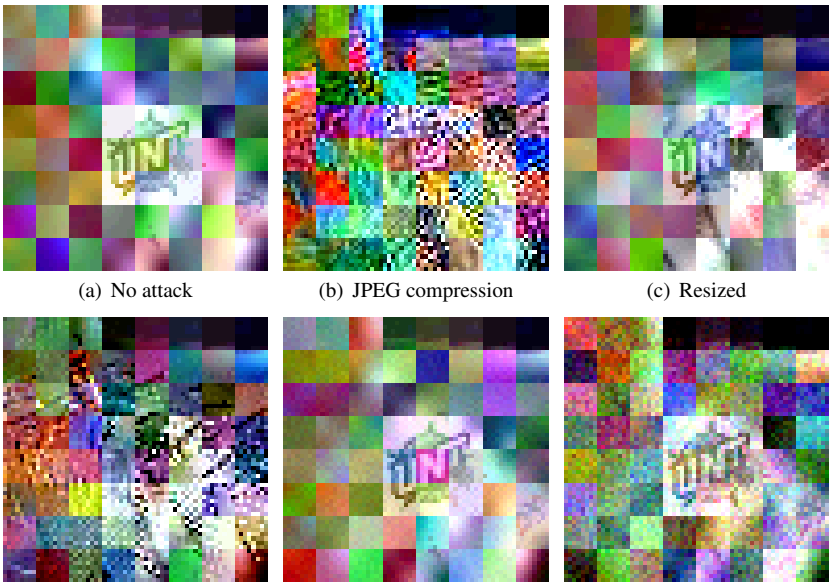
Fig. 8. Watermarks extracted from the Lena's image restored from different types of attacks



(a) No attack (b) JPEG compression (c) Resized

(d) Median filtered (e) Gaussian Blurred (f) White noise added

Fig. 9. Watermarks extracted from the bear's image restored from different types of attacks



(a) No attack (b) JPEG compression (c) Resized

(d) Median filtered (e) Gaussian blurred (f) White noise added

Fig. 10. Watermarks extracted from the color image of the child restored from different types of attacks

(a) No attack (b) JPEG compression (c) Resized

(d) Median filtered (e) Gaussian blurred (f) White noise added

Fig. 11. Watermarks extracted from the Lena color image restored from different types of attacks

Table V. Relationship between the quality of the invisible watermarking image restored from an attack and the quality and recognizability of the extracted color watermark in the Lena color image

Attack Type	Host Image's PSNR	Extracted Watermark's PSNR	Extracted Watermark's γ
No Attack	∞	35.17	0.9947
JPEG Compression (Quality Factor = 60)	38.30	24.69	0.7930
Size Quadrupling and Resizing back	40.09	26.82	0.9081
Median Filtered	38.80	25.58	0.8373
Gaussian Blurred (Blind Deconvolution)	46.54	30.43	0.9856
White Noise	42.95	27.63	0.9286

algorithm is also under investigation. Finally, we intend to investigate options to integrate the watermarking hardware in consumer electronic appliances, such as digital cameras.

ACKNOWLEDGMENTS

The authors would like to thank the associate editor, Prof. Ketan Mayer-Patel, and the anonymous reviewers of this paper for their helpful feedbacks. The authors acknowledge the help of Elias Kougianos, Parthasarathy Guturu, and Nishikant Pati at the University of North Texas. This research is partially supported by grants from NSF 0242840 and NSF 0219110 at Purdue University.

REFERENCES

2007. Digital Watermarking Alliance (DWA). `http://www.digitalwatermarkingalliance.org/`.

BARNETT, R. 1999. Digital Watermarking : Application, Techniques, and Challengs. *IEE Electronics and Communication Engineering Journal*, 173–183.

BENDER, W., BUTERA, W., GRUHL, D., HWANG, R., PAIZ, F. J., AND POGREB, S. 2000. Applications for Data Hiding. *IBM Systems Journal 39,* 3 and 4, 547–568.

COX, I. J., KILIAN, J., LEIGHTON, T., AND SHAMOON, T. 1997. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing 6,* 12 (Dec), 1673–1687.

COX, I. J. AND MILLER, M. 1997. A Review of Watermarking and Importance of Perceptual Modelling. In *Proceedings of SPIE Human Vision and Imaging*. Vol. 3016. 92–99.

COX, I. J. AND MILLER, M. L. 2002. Electronic Watermarking : The First 50 Years. *EURASIP Journal of Applied Signal Processing 2002,* 2 (February), 126–132.

CRAVER, S., MEMON, N., YEO, B. L., AND YEUNG, M. M. 1998. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. *IEEE Journal on Selected Areas in Communications 16,* 4 (May), 573–586.

ESKICIOGLU, A. M. AND DELP, E. J. 2001. An Overview of Multimedia Content Protection in Consumer Electronics Devices. *Elsevier Signal Processing : Image Communication 16*, 681–699.

FEI, C., KUNDUR, D., AND KWONG, R. H. 2004. Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression. *IEEE Transactions on Image Processing 13*, 126 – 144.

GUITART, O., KIM, H. C., AND DELP, E. J. 2006. Watermark evaluation testbed. *Journal of Electronic Imaging 15,* 4 (October - December).

HEILEMAN, G. L., PIZANO, C. E., AND ABDALLAH, C. T. 1999. Performance Measures for Image Watermarking Schemes. In *Proceedings of the Fifth Baiona Workshop on Emerging Technologies in Telecommunications*. 149–152.

HOLLIMAN, M. AND MEMON, N. 2000. Counterfeiting attack on oblivious blockwise independent invisible watermarking schemes. In *IEEE Transactions on Image Processing*. Vol. 9. 432–441.

HU, Y. AND KWONG, S. 2001. Wavelet Domain Visible Watermarking. *IEE Electronic Letters 37,* 20 (September), 1219–1220.

HUA, X. S., FENG, J. F., AND SHI, Q. Y. 2001. Public Multiple Watermarking Resistant to Cropping. In *Proceedings of the 6th international conference on pattern recognition and information processing*. 263–268.

JIANG, G., YU, M., SHI, S., LIU, X., AND KIM, Y. D. 2002. New blind image watermarking in DCT domain. In *Proceedings of the 6th International Conference on Signal Processing*. Vol. 2. 1580 – 1583.

KANG, H. I. AND DELP, E. J. 2004. An image normalization based watermarking scheme robust to general affine transformation. In *Proceedings of the IEEE International Conference on Image Processing (ICIP)*. 1553–1556.

KHAN, A. AND MIRZA, A. M. 2007. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. *Information Fusion 8,* 4, 354–365.

KUNDUR, D. AND HATZINAKOS, D. 2004. Toward Robust Logo Watermarking Using Multiresolution Image Fusion Principles. *IEEE Transactions on Multimedia 6,* 1 (February), 185–198.

KUTTER, M. AND PETITCOLAS, F. A. P. 1999. A fair benchmark for image watermarking systems. In *Proceedings of SPIE Security and Watermarking of Multimedia Contents*. Vol. 3657. 226–239.

LANGELAAR, G., LAGENDIJK, R., AND BIEMOND, J. 1999. Watermarking by DCT coefficient removal: Statistical approach to optimal parameter settings. In *Proceedings SPIE IS&T/SPIE's 11th Annual Symposium on Electronic Imaging: Security and Watermarking of Multimedia Contents*. Vol. 3657.

LU, C.-S., LIAO, H.-Y. M., HUANG, S.-K., AND SZE, C.-J. 1999. Cocktail Watermarking on Images. In *Proceedings of the 3rd International Workshop on Information Hiding*. 333–347.

LU, Z.-M., XU, D.-G., AND SUN, S.-H. 2005. Multipurpose image watermarking algorithm based on multistage vector quantization. *IEEE Transactions on Image Processing 14,* 6 (June), 822–831.

MAES, M., KALKER, T., LINNARTZ, J. P. M. G., TALSTRA, J., DEPOVERE, G. F. G., AND HAITSMA, J. 2000. Digital Watamarking for DVD Video Copyright Protection. *IEEE Signal Processing Magazine 17,* 5 (Sep), 47–57.

MEMON, N. AND WONG, P. W. 1998. Protecting Digital Media Content. *Communications of the ACM 41,* 7 (July), 35–43.

MINTZER, F., BRAUDAWAY, G., AND YEUNG, M. 1997. Effective and Ineffective Digital Watermarks. In *IEEE International Conference on Image Processing*. Vol. 3. 9–12.

MINTZER, F., BRAUDAWAY, G. W., AND BELL, A. E. 1998. Opportunities for Watermarking Standards. *Communications of the ACM 41,* 7 (July), 57–64.

MINTZER, F. C., BOYLE, L. E., CAZES, A. N., CHRISTIAN, B. S., COX, S. C., GIORDANO, F. P., GLADNEY, H. M., LEE, J. C., KELMANSON, M. L., LIRANI, A. C., MAGERLEIN, K. A., PAVANI, A. M. B., AND SCHIATTARELLA, F. 1996. Towards online Worldwide Access to Vatican Library Materials. *IBM Journal of Research and Development 40,* 2 (Mar), 139–162.

MOHANTY, S. P. 1999. Digital Watamerking of Images. M.S. thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India.

MOHANTY, S. P., GUTURU, P., KOUGIANOS, E., AND PATI, N. 2006. A Novel Invisible Color Image Watermarking Scheme Using Image Adaptive Watermark Creation and Robust Insertion-Extraction. In *Proceedings of the 8th IEEE International Symposium on Multimedia (ISM)*. 153–160.

MOHANTY, S. P., RAMAKRISHNAN, K. R., AND KANKANHALLI, M. S. 1999. A Dual Watermarking Technique for Images. In *Proceedings of the 7th ACM International Multimedia Conference (Vol. 2)*. 49–51.

MOHANTY, S. P., RAMAKRISHNAN, K. R., AND KANKANHALLI, M. S. 2000. A DCT Domain Visible Watermarking Technique for Images. In *Proceedings of the IEEE International Conference on Multimedia and Expo*. 1029–1032.

MOHANTY, S. P., RANGANATHAN, N., AND BALAKRISHNAN, K. 2006. A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain. *IEEE Transactions on Circuits and Systems II (TCAS-II) 53,* 5 (May), 394–398.

OSBERGER, W. AND MAEDER, A. J. 1998. Automatic identification of perceptually important regions in an image. In *Proceedings of the 14th IEEE International conference on Pattern Recognition*. 701–704.

PAI, Y.-T., RUAN, S.-J., AND GÖTZE, J. 2005. Energy-Efficient Watermark Algorithm Based on Pairing Mechanism. In *Lecture Notes in Computer Science (LNCS)*. 1219–1225.

PETITCOLAS, F. A. P. 2000. Watermarking Schemes Evaluation. *IEEE Signal Processing 17,* 5 (September), 58–64.

PETITCOLAS, F. A. P., ANDERSON, R. J., AND KUHN, M. G. 1998. Attacks on Copyright Marking Systems. In *Proceedings of the 2nd International Workshop on Information Hiding*. 218–238.

PETITCOLAS, F. A. P., ANDERSON, R. J., AND KUHN, M. G. 1999. Information Hiding - A Survey. *Proceedings of the IEEE 87,* 7 (July), 1062–1078.

PLANITZ, B. M. AND MAEDER, A. J. 2005. A Study of Block-Based Medical Image Watermarking Using a Perceptual Similarity Metric. In *Proceedings of the Digital Image Computing on Techniques and Applications*. 70.

PODILCHUK, C. I. AND WENJUN, Z. 1998. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications 16,* 4 (May), 525–539.

QI, H., ZHENG, D., AND ZHAO, J. 2008. Human visual system based adaptive digital image watermarking. *Signal Processing 88,* 1, 174–188.

REININGER, R. C. AND GIBSON, J. D. 1983. Distributions of the Two-Dimensional DCT Coefficients for Images. *IEEE Trans. Communications 31,* 6 (June), 835–839.

SAXENA, V. AND GUPTA, J. P. 2007. Collusion Attack Resistant Watermarking Scheme for Images using DCT. In *Proceedings of the 15th IEEE Conference on Signal Processing and Communications Applications*. 1–4.

SEQUEIRA, A. AND KUNDUR, D. 2001. Communications and information theory in watermarking : A survey. In *Proceedings of SPIE Multimedia Systems and Application IV*. Vol. 4518. 216–227.

SERVETTE, S. D., PODILCHUK, C., AND RAMCHANDRAN, K. 1998. Capacity Issues in Digital Watermarking. In *IEEE International Conference on Image Processing, ICIP-98*. Vol. 1. 445–449.

SHEN, B. AND SETHI, I. K. 1996. Direct Feature Extraction from Compressed Images. In *Storage and Retrieval for Image and Video Databases (SPIE)*. 404–414.

TOPKARA, M., KAMARA, A., ATALLAH, M., AND NITA-ROTARU, C. 2005. ViWiD: Visible Watermark Based Defense Against Phishing. *Lecture Notes in Computer Science (LNCS), IWDW 2005 3710*, 470–484.

TSAI, T. H. AND LU, C. Y. 2001. A Systems Level Design for Embedded Watermark Technique using DSC Systems. In *Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems*.

VOLOSHYNOVSKIY, S., PEREIRA, S., PUN, T., EGGERS, J., AND SU, J. 2001. Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks. *IEEE Communications Magazine 39,* 9 (August), 118–126.

WOLFGANG, R. B., PODILCHUK, C. I., AND DELP, E. J. 1999. Perceptual watermarks for digital images and video. *Proceedings of the IEEE 87,* 7 (July), 1108–1126.

WU, Y., GUAN, X., KANKANHALLI, M. S., AND HUANG, Z. 2001. Robust Invisible Watermarking of Volume Data Using the 3D DCT. In *Proceedings of Computer Graphics International (CGI)*. 359–362.

XIE, L. AND ARCE, G. 1998. Joint wavelet compression and authentication watermarking. In *IEEE International Conference on Image Processing*. 427–431.

YEUNG, M. M., MINTZER, F. C., BRAUDAWAY, G. W., AND RAO, A. R. 1997. Digital Watermarking for High-Quality Imaging. In *Proceedings of the IEEE First Workshop on Multimedia Signal Processing*. 357–362.

ZHAO, Y., CAMPISI, P., AND KUNDUR, D. 2004. Dual domain watermarking for authentication and compression of cultural heritage image. *IEEE Transactions on Image Processing 13,* 3 (Mar), 430–448.

Submitted on September 2007. Revised on December 2007. Accepted on February 2008.