A Perceptually-Adaptive High-Capacity Color Image Watermarking System

Lahouari Ghouti
Department of Information and Computer Science, King Fahd University of Petroleum and Minerals.
Dhahran 31261. Saudi Arabia
[E-mail: lahouari@kfupm.edu.sa]

Received May 26, 2016; revised October 3, 2016; accepted November 15, 2016; published January 31, 2017

Abstract

Robust and perceptually-adaptive image watermarking algorithms have mainly targeted gray-scale images either at the modeling or embedding levels despite the widespread availability of color images. Only few of the existing algorithms are specifically designed for color images where color correlation and perception are constructively exploited. In this paper, a new perceptual and high-capacity color image watermarking solution is proposed based on the extension of Tsui et al. algorithm. The CIEL*a*b* space and the spatio-chromatic Fourier transform (SCFT) are combined along with a perceptual model to hide watermarks in color images where the embedding process reconciles between the conflicting requirements of digital watermarking. The perceptual model, based on an emerging color image model, exploits the non-uniform just-noticeable color difference (NUJNCD) thresholds of the CIEL*a*b* space. Also, spread-spectrum techniques and semi-random low-density parity check codes (SR-LDPC) are used to boost the watermark robustness and capacity. Unlike, existing color-based models, the data hiding capacity of our scheme relies on a game-theoretic model where upper bounds for watermark embedding are derived. Finally, the proposed watermarking solution outperforms existing color-based watermarking schemes in terms of robustness to standard image/color attacks, hiding capacity and imperceptibility.

Keywords: Color image watermarking, spatio-chromatic Fourier transform, perceptual models, data hiding capacity

A preliminary version of this paper appeared in the International Conference on Computer and Communication Engineering (ICCCE' 12), pp. 349-353, July 2012. This research is supported by King Fahd University of Petroleum and Minerals.

https://doi.org/10.3837/tiis.2017.01.030 **ISSN : 1976-7277**

1. Introduction

Following the Internet surge, illegal usage of image content over the cyber world urged content owners and standardization bodies to ” redesign” digital image watermarking systems [1]. However, most of the existing image watermarking solutions did not primarily consider the color information in terms of processing, embedding and modeling despite the claim that these solutions can be straightforwardly extended to color images [1]. Then, interest in color image watermarking solutions revived thanks to the the pioneering work of Fleet and Heeger [2] who first suggested concealing watermark data into a color axis (the b* scale in of the CIEL*a*b* domain). Using the human visual system (HVS) properties, Fleet and Heeger paved the way for perceptually-adaptive color image watermarking. In this paper, a high-capacity scheme is proposed where the watermarking conflicting requirements are satisfied using the SCFT transform, a CIEL*a*b* perceptual model and game-theoretic data hiding bounds. In this scheme, additive spread-spectrum embedding and SR-LDPC codes are used to extend the watermark robustness and capacity of the block-based color image watermarking scheme proposed by Tsui et al. [3]. Embedding is controlled by a perceptual map derived from the non-uniform just-noticeable color difference (NUJNCD) thresholds of the CIEL*a*b* space [4].

Unlike Tsui et al. algorithm, the watermark sequence is blindly recovered where a Weibull model for the SCFT coefficients and a maximum likelihood (ML) decoder are used. In addition, the proposed color image watermarking scheme outperforms its non-blind counterpart proposed by Tsui et al. in terms of watermark imperceptibility and data hiding capacity while retaining enhanced robustness to typical image and color attacks and lower bit error rates at the watermark detector side.

The rest of the paper is organized as follows. The conflicting requirements of digital watermarking technologies are outlined in Section 2. Then, a review of latest developments in color image watermarking techniques is provided in Section 3. In Section 4, the mathematical description of the SCFT is introduced. The details of the CIEL*a*b* space, related to the underlying perceptual model, are discussed too along with concepts of uniform, non-uniform just-noticeable differences (UJNDs and NUJNDs) and color perceptual redundancy. A detailed discussion of the proposed scheme is given in Section 5. Details of watermark embedding and recovery are given along with the detector structures therein. Then, a game-theoretic formulation of the data hiding capacity estimates is laid out in Section 6. The robustness of this scheme to affine, geometric, color conversion and JPEG/JPEG2000 compression attacks is documented in Section 7. Performance results attained by an existing block-based SCFT algorithm are also provided for comparison purposes. Section 8 completes the paper where concluding remarks are given.

2. Design Requirements of Robust Digital Watermarking Systems

It is worth noting, before shedding the light on the requirements imposed on any digital watermarking “standard” requirements that all digital watermarking systems should satisfy and comply with. These requirements, application-dependent in general, drastically differ from one application to another. However, the basic core requirements that must be satisfied by any digital watermarking system may be summarized in what follows:

Robustness [1]**:** The watermark payload should, in general, be robust to incidental and intentional distortions depending on the application. It must remain with the composite signal regardless of the possible processing tasks that the composite signal may undergo.

Transparency: Aside from visible watermarking systems, the embedded watermark should be imperceptible. Hence, the watermark embedding should exploit the existing redundancy in the host signal and the target receptive imperfections.

Oblivious Decoding: Any practical digital watermarking system should not require the original host signal during watermark detection/recovery. Systems with the above-mentioned property are known as: ”oblivious decoding” systems.

Watermark Security and Secret Keys: Watermark security addresses the secrecy of the embedded information. Hence, the recovery of the watermark should be made impossible for unauthorized parties even though it is assumed that the embedding/decoding process is known. All digital watermarking systems designed with this requirement in mind are known to comply with ”*Kerckoffs's principle*” [1]. Secret keys may be used to strengthen the watermark security at both embedding and decoding levels.

Low Decoding Errors: For multi-bit watermark embedding, it is desirable to keep the BER during the decoding/recovery phase as the lowest level possible. This requirement is quite common for fingerprinting and high capacity watermarking systems [5]. However, it is difficult to satisfy this requirement when using oblivious decoding.

Capacity: Robustness, an attractive feature for any digital watermarking system, is related to the embedding capacity. The higher is the embedding capacity, the less robust is the watermark. This is due to the fact that less energy is allocated to each embedded bit. Hence, caution must be exercised to determine the best trade-off between imperceptibility, robustness and capacity. It is worth mentioning that the incorporation of good perceptual models in the embedding stage, would allow maximizing the energy in each embedded bit while maintaining higher watermark imperceptibility. According to capacity, there are two classes of watermarking systems, namely, single-bit and multi-bit systems. Most of the existing watermarking systems in the literature belong to the first class whose decoding relies on hypothesis testing to determine the watermark presence.

Fig. 1 illustrates the conflicting relations between the main characteristics of any digital watermarking system. The watermark embedding/attack processes are modeled as a game between the watermark embedded and attacker. Distortions on the host signal/image resulting from watermark embedding and removal are quantified by D_1 and D_2, respectively. In additon, to reconcile between the requirements, the embedding process should be confined in the shaded regions where:

$$\begin{aligned} wat\_cap &\in [c, c^{'}] \\ wat\_imp &\in [i, i^{'}] \\ wat\_rob &\in [r, r^{'}] \end{aligned} \tag{1}$$

where wat_cap, wat_imp and wat_rob quantify the watermark capacity, imperceptiblity and robustness, respectively. Upper and lower bounds for the data hiding capacity, robustness and imperceptibility are given by c/c’, r/r’and i/i’, respectively.

[1] For tamper-detection applications, watermark fragility and semi-fragility are considered instead of robustness.

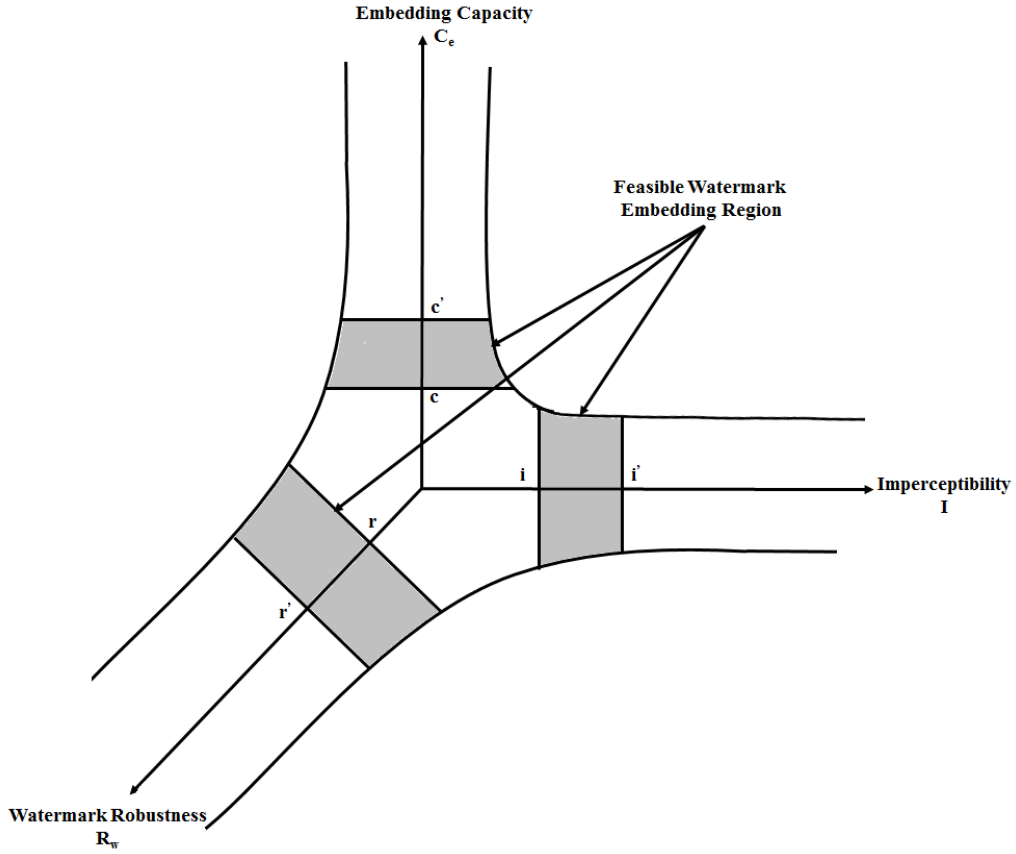


Fig. 1. Conflicting relations between design requirements of digital watermarking systems.

3. Review of Full-Color Image Watermarking Algorithms

To limit the scope of this section, only full-color image watermarking algorithms are reviewed chronologically. Building on their expertise in psychovision research, Fleet and Heeger [2] exploited the yellow-blue channel in the CIEL*a*b* space to hide a high frequency amplitude-modulated sine wave in the host image.

The embedding approach took advantage of the low frequency content of the host image and the low sensitivity of the HVS system to high frequencies. Chou and Liu [6] associated a new visual model with the discrete wavelet transform (DWT). This model provides an estimate of the profile of error visibility thresholds for each DWT coefficient. In [7], Chou and Wu extended their scheme, proposed in [6], to quantize the host coefficients using quantization index modulation (QIM) technique to ensure watermark imperceptibility. One of the earliest full-color image watermarking algorithms, attributed to Bas et al. [8], embeds watermark bits in the hypercomplex domain using the quaternion Fourier transform (QFT) coefficients. Tsui et al. [3] proposed a block-based SCFT watermarking scheme in the CIEL*a*b* space where watermark embedding takes place in a single coefficient of 8x8 SCFT blocks. However, the original image is required for watermark decoding and recovery, which is not suitable for practical applications.

Chou and Liu concealed watermark sequences in the most distortion-tolerable locations in the image color channels without causing any perceivable distortion in the watermarked images [9]. For watermark recovery, the decoder applies a majority-vote decision to select the most robust bit. In [10], Ghouti and Landolsi proposed a high capacity embedding scheme where the watermark payload is hosted by wide bandpass SCFT regions. In this scheme, the watermark bits are perceptually embedded using a CIEL*a*b* space color model and recovered based on a Weibull-based detector.

Using quaternion principal component analysis (QPCA) and feature point extraction, Lang et al. [11] embedded watermark bits in the most robust regions of the host image. Shao et al. [12] proposed a different approach to embed encrypted red-green-blue (RGB) watermark images using the double random phase encoding technique (DRPE) in the quaternion gyrator transform (QGT) domain [13]. A novel approach for spatial-domain watermark embedding is suggested by Lusson et al. [14] where two color systems are exploited. Since the embedding is carried out in two different color systems, Lusson et al. suggested two different approaches for watermark embedding using the RGB and YCbCr domains.

To mitigate color attacks, Wang et al. [15] combined the use of the QFT transform and the least-squares SVMs algorithm (LS-SVM) to blindly recover embedded watermarks. Ouyang et al. [16] proposed another QFT-based color image watermarking algorithm where the correlation between the color channels is fully exploited for watermark imperceptibility and robustness purposes. A quaternion moment-based scheme is suggested in [17] where Tsougenis et al. introduced the quaternion radial Tchebichef moments.

Given the limitations of the QFT-based color watermark solution proposed by Bas et al. [8], Chen et al. [18] suggested the use of a full 4-dimensional QFT to avoid the loss of some watermark payload due to color conversion. Chen et al. imposed specific symmetry constraints on the 4D-QFT coefficients. To eliminate the effects of desynchronization attacks on the watermark recovery, Wang et al. embedded watermark data using local quaternion exponent moments [19].

The first adaptive moment-based scheme is proposed by Tsougenis et al. [20]. Using accurate estimates of quaternion radial moments (QRM), Tsougenis et al. astutely exploited high reconstruction capability and rotation invariance to achieve watermark robustness and imperceptibility. Yang et al. [21] proposed a different approach for moment-based watermark embedding. In this approach, the polar harmonic transform (PHT) is extended to the quaternion domain (QPHT) for embedding watermark payload where color invariance is achieved.

Su et al. [22] adopted a rather unconventional approach to design a novel blind-dual color image watermarking scheme. In their scheme, Su et al. modified host color images in the YCbCr domain to host color image watermarks encoded using the RGB domain. The scheme duality is attributed to the use of both RGB and YCbCr color domains.

Al-Otum and Samara [23] exploited the multiresolution inter-coefficient relation between the color pixels using a wavelet tree structure. Watermark embedding takes place in the multiresolution domain using the inter-pixel relation to encode the sign bits of the watermark sequence. To embed the watermark payload, each color channel in the RGB representation of the host color image is processed separately to identify the significant host locations in the multiresolution domain using the wavelet-tree structure.

Vahedi et al. used the wavelet domain of the host color image to embed the watermark payload [24]. The embedded sequence consisted of a logo watermark for copyright protection purposes. The host color image is first transformed to the HSI color space prior to wavelet transformation to take advantage of the HSI space properties. To simultaneously satisfy the

three conflicting requirements of watermarking systems (imperceptibility, robustness and high capacity), a genetic algorithm solution is propose to optimize the parameters of these three requirements.

In [25], Prathap et al. presented a blind and highly robust color image watermarking method where spatial and frequency domains are optimally exploited. In this scheme, each RGB channel in the host image is processed separately to identify features using the gray level co-occurrence matrix (GLCOM) in the spatial domain.

To keep its content unchanged, Su et al. [26] computed the direct current (DC) coefficient in each 8x8 block of the Y channel of the YCbCr representation of the host color image. Then, given a specific quantization step Δ, the effect of quantizing each DC coefficient is propagated to all associated alternating current (AC) coefficients in each block.

Findik et al. [27] suggested a color image watermarking algorithm that embeds the watermark payload in the blue channel of an RGB image. For watermark recovery purposes, the binary watermark payload, of length m, is used to train the artificial immune recognition system. Therefore, the watermark recovery is carried out using the trained model where the watermarked color image is considered as a testing sequence.

Liu et al. [28] modified an existing color perceptual model [29] to conceal the embedded watermark bits in a color host image. Prior to watermark concealment, the YCbCr components of the host image are transformed into the wavelet domain using a JPEG2000 compliant wavelet filters. Then, noise detection threshold of each wavelet coefficient in the transformed Y (luminance) and Cb/Cr (chrominance) components is estimated which provides an embedding threshold that the watermark strength should not exceed to guarantee watermark imperceptibility and robustness at the same.

Another blind color image watermarking scheme is attributed to Su et al. [30] which embeds watermark information data into a factorized representation of color images. This scheme is based on the fact that the factorization of any matrix using the singular value decomposition (SVD) yields highly correlated elements in the resulting orthogonal matrix. This correlation is more pronounced between the second row first column element and the third row first column element of the orthogonal matrix.

Another robust DWT-based color image watermarking scheme is suggested by Al-Otum and Al-Sowayan [31] which embeds the watermark payload into the subband coefficients of the U and V transformed channels using watermark embedding thresholds. These thresholds are estimated based on the color permissibility of the U and V channels.

Moghaddam and Nemati [32] modified the imperialistic competition algorithm (ICA) to embed watermark information bits in the RGB pixels of the host color image in the spatial domain. The modified ICA algorithm selects the least significant color band as a host for the watermark image pixels. This selection process is based on the dynamic range of the color information in each 5x5 image block.

Ou et al. [33] proposed a new scheme for reversible data hiding in the color domain. To boost the embedding performance and exploit the inter-channel correlation, Ou et al. perceptually embed the watermark payload using a channel-dependent approach. The watermark payload is partitioned and embedded in each channel using the channel prediction-error histogram (PEH).

4. Color Models, Representations and Spectral Transformations

The SCFT representation of color images, introduced by McCabe et al. [34], exploits the properties of the HVS system in the perception of colors as opponent combinations [34]. A

brief review of the relevant color spaces and scales is provided first in this section followed by a detailed description of the SCFT transform [34].

4.1 CIEL*a*b* Color Space

The CIEL*a*b* space defines color scales based on the opponent-color theory where color is perceived by the human eye receptors as a pair of opponent color directions [35]. This color representation is depicted in **Fig. 2-a**. This representation allows the separation of luminance and chrominance elements such that the L* component represents the luminance and the color information is represented by a* and b* scales. The a* and b* scales define the green-red and the blue-yellow axes. The hue and chroma in the CIEL*a*b* space, shown in **Fig. 2-b**, are defined as follows [35]:

$$H_{a^*b^*} = \arctan\left(\frac{b^*}{a^*}\right) \tag{1}$$

$$C_{a^*b^*} = \sqrt{(a^*)^2 + (b^*)^2} \tag{2}$$

4.2 Perceptual Redundancy

Thanks to the perceptual redundancy concept, colors with different tristimulus cannot be perceptually discriminated which works favorably for color image watermarking solutions [35]. However, unlike other color spaces, colors are uniformly distributed in the CIEL*a*b* space where the same perceptual color difference corresponds to the same distance quantified in the tristimulus representation of this space [7]. The perceptual redundancy of the CIEL*a*b* space is illustrated in **Fig. 2-c**. A set of perceptually indistinguishable is represented by a sphere with one central color. These color spheres have the same radius commonly known as the just noticeable color difference (JNCD) [7]. An example of JNCD sphere is portrayed in **Fig. 2-d**. In this paper, the watermark embedding process defines the embedding weights such that the JNCD thresholds are not exceeded. The Euclidean distance between two perceptually-distinguishable colors is given by [7]:

$$\sqrt{(\Delta L^*)^2 + (\Delta a^*)^2 + (\Delta b^*)^2} \geq JNCD_{L^*a^*b^*} \tag{3}$$

where ΔL*, Δa* and Δb* represent the intensity differentials in the L*, a* and b* color components, respectively. The JNCD thresholds, $JNCD_{L^*a^*b^*}$, are illustrated in **Fig. 2-d**.

The JND profiles for color images, defined in [7], form the basis of color-adaptive image watermarking solutions developed by Chou and his team [7]. Our color image watermarking scheme derives the watermark embedding weights using the non-uniform JNCD (NUJNCD) thresholds of the CIEL*a*b* space.

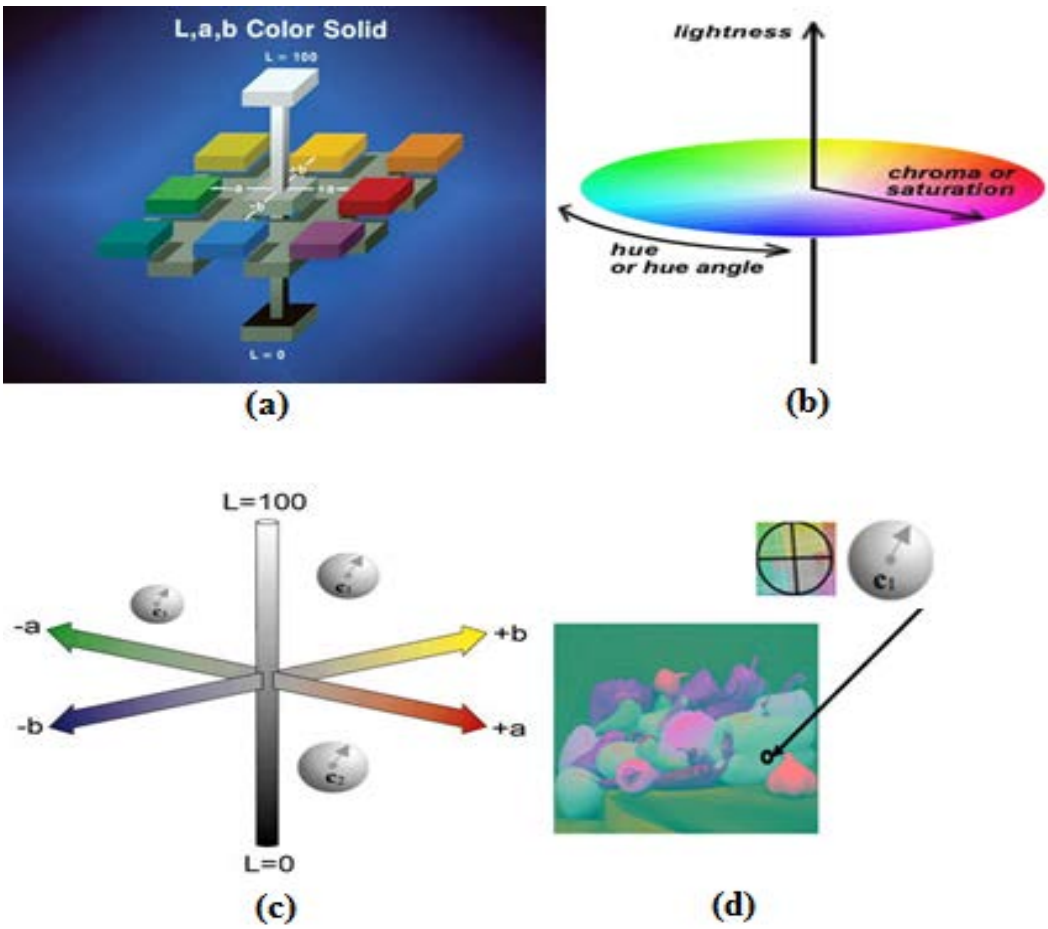


Fig. 2. (a) CIEL*a*b* color opponent system. (b) CIEL*a*b* chroma and hue. (c) Uniform JNCD spheres. (d) JNCD sphere in *Peppers* image.

4.3 Forward and Inverse SCFT Transforms

Several image transforms such as the conventional discrete Fourier transform (DFT), discrete cosine transform (DCT) and DWT are often used as embedding domains [1]. In this paper, we propose the use of a frequency-bandpass SCFT domain to conceal the watermark payload in this band. The SCFT transform offers the attractiveness of efficient "complex-domain" representations with implementation complexity similar to that of the DFT transform. The forward SCFT transform handles the a* and b* components as a complex entity prior to DFT transformation as defined below [34]:

$$[A^*(u,v) + jB^*(u,v)] = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[a^*(x,y) + jb^*(x,y)] \cdot \exp^{\frac{-2\pi j(ux+vy)}{N}} \quad (4)$$

where NxN is the size of the image. [a*(x, y) + j b*(x, y)] and [B*(u, v) + j B*(u, v)] are the complex chromacity coordinates at the spatial and frequency points (x, y) and (u, v), respectively. Once color-based processing is carried out on [A*(u, v) + j B*(u, v)], a* and b* can be recovered using the inverse SCFT transform [34]:

$$[a^*(x,y) + jb^*(x,y)] = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[A^*(u,v) + jB^*(u,v)] \cdot \exp^{\frac{2\pi j(ux+vy)}{N}} \quad (5)$$

5. Proposed Color Image Watermarking Scheme

The proposed color image watermarking scheme uses a bandpass representation of the SCFT transform in conjunction with direct-sequence spread-spectrum watermark embedding to mitigate the effects of low signal-to-noise ratio (SNR) on the watermark bits. In this way, the watermark payload is encoded with a pseudo-random sequence to spread the power spectrum of the information data. To achieve watermark imperceptibility, a simple, yet efficient, NUJNCD-based image-adaptive embedding mechanism is adopted as well.

5.1 Perceptually-Adaptive Color Image Watermarking Model

A model of the proposed scheme is shown in **Fig. 3**. The process of watermark encoding is independent of the host image $\boldsymbol{I}$ where the watermark weights are controlled by the NUJNCD thresholds. The watermarked image, $\boldsymbol{I}'$, is transmitted through a noisy channel where possible image attacks may take place. Finally, the received corrupted image $\boldsymbol{I}'_{noisy}$ is then processed by the detector/decoder stage for watermark recovery.

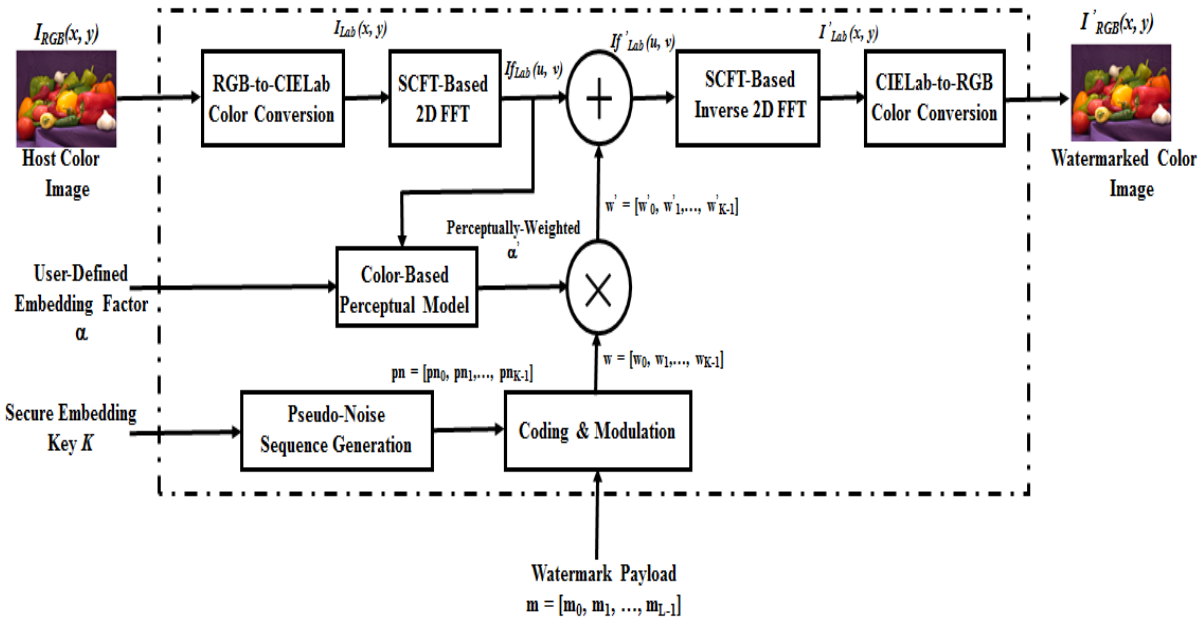


Fig. 3. Diagram of the proposed color image watermarking system.

5.2 Watermark Embedding Algorithm

5.2.1 Embedding Steps

The main steps of the proposed scheme are detailed below:

1. Generate a binary pseudo-random sequence, $\boldsymbol{m}$, consisting of ±1 using a private embedding key $\boldsymbol{K}$.
2. Perform code repetition and SR-LDPC coding on m to generate the sequence $\boldsymbol{m_{enc}}$.
3. Transform the N_rxN_c host image, $\boldsymbol{I_{RGB}(x, y)}$, to the CIEL*a*b* space to get $\boldsymbol{I_{Lab}(x, y)}$.

4. Apply forward SCFT transform on the complex-valued quantity, ***[a*(x, y) + j b*(x, y)]***, using Equation (4) to get the SCFT quantities ***[A*(u, v) + jB*(u, v)]***.
5. Estimate the perceptual weights, α_i, using the NUJNCD thresholds.
6. Modulate a pseudo-random sequence by m_{enc} to produce the sequence w.
7. Scale proportionally w using the weights α_i.
8. Perform watermark embedding using additive-multiplicative rule:

$$s_i^w = s_i\left(1+\alpha_i w_i\right) \tag{6}$$

where s_i^w and s_i are the ith samples of the host and watermarked SCFT quantities ***[A*(u, v) + jB*(u, v)]*** and ***[(A*(u, v))^w + j(B*(u, v))^w]***, respectively.

9. Apply inverse SCFT transform on ***[(A*(u, v))^w + j(B*(u, v))^w]*** using Equation (5) to get the spatial domain chromatic coefficients ***[(a*(x, y))^w + j(b*(x, y))^w]***.
10. Form $I_{Lab}^w(x, y)$ by combining L*, (a*)^w and (b*)^w components.
11. Finally, convert $I_{Lab}^w(x, y)$ to the RGB space to get the watermarked image $I_{RGB}^w(x, y)$.

5.2.2 Selection of Embedding Parameters

To ensure watermark imperceptibility, only a band of the SCFT coefficients, defined in Equation (4), are used for watermark embedding. Low and high frequency bands are exempted from the embedding process as illustrated in **Fig. 4**. The selected mid-frequency bands are used in the data hiding capactity estimation given in Section 6.

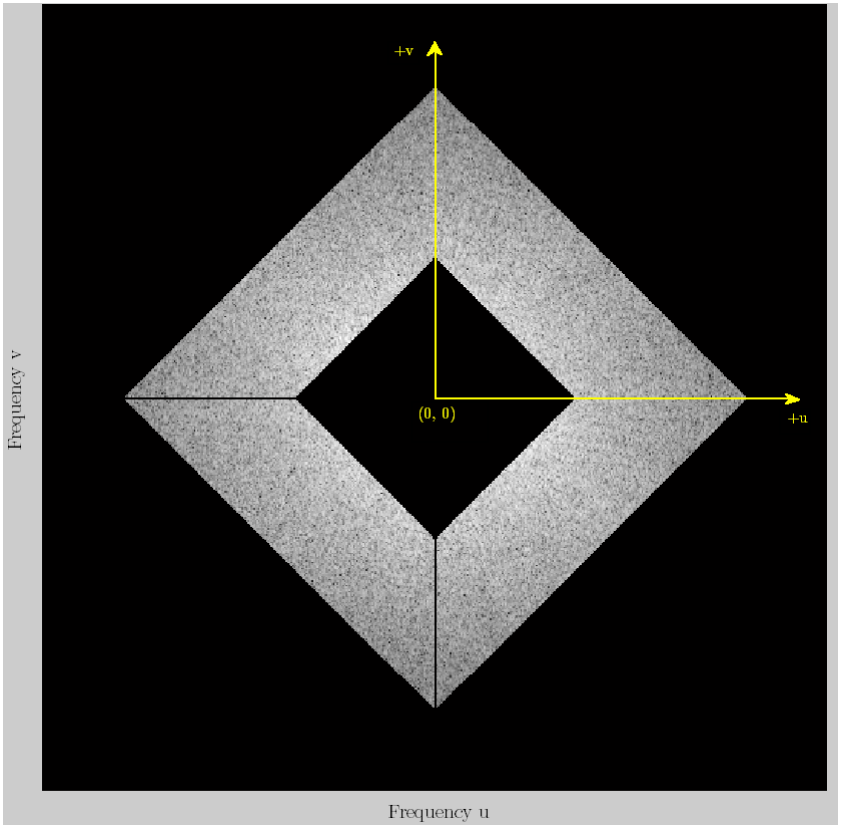


Fig. 4. Selected mid-frequency bands in the SCFT domain for watermark embedding.

In addition, the percptual weights, α_i, are maintained below the NUJNCD levels as follows:

$$\alpha_i = \frac{1}{2} NUJNCD_i \tag{7}$$

where NUJNCDi is the perceptual thresholds defined in Equation (3). The spatial NUJNCD thresholds are illustrated in **Fig. 2-d**.

5.3 Watermark Decoding

Watermark decoding is reminiscent of detecting a signal in background noise where the maximum likelihood (ML) detector extracts each embedded bit. In this paper, we model the watermarked SCFT coefficients using the Weibull distribution to blindly recover the embedded bits. It should be noted that the Weibull model parameters are estimated assuming that the embedding distortion is relatively small [36]. For any $r > 0$, the Weibull model of the SCFT coefficients is given by [37]:

$$f_r(r) = \left(\frac{\beta}{\gamma}\right)\left(\frac{r}{\gamma}\right)^{\beta-1} \exp\left(-\left(\frac{r}{\gamma}\right)^{\beta}\right) \tag{8}$$

where γ and β are the scale and shape parameters which are estimated using moment matching techniques [36]. At the decoder stage, the following hypothesis test is performed:

Hypothesis H_0 : a bit 0 is embedded (b = -1),
Hypothesis H_1 : a bit 1 is embedded (b = 1),

The corresponding maximum log-likelihood decision rule decides for the bit to be a 1 if the threshold, Δ_{SCFT}, exceeds one as shown below:

$$\begin{aligned}\Delta_{SCFT} &= \sum_{j=1}^{\chi} \beta_j \ln\left(1-\gamma m_j\right) + \sum_{j=1}^{\chi}\left(\frac{r_j}{\alpha_j\left(1-\gamma m_j\right)}\right)^{\beta_j} \\ &\quad - \sum_{j=1}^{\chi} \beta_j \ln\left(1+\gamma m_j\right) + \sum_{j=1}^{\chi}\left(\frac{r_j}{\alpha_j\left(1+\gamma m_j\right)}\right)^{\beta_j} \\ &\geq 0\end{aligned} \tag{8}$$

where χ is the chip rate, and mj is the jth spreading sequence element for the received bit. In Equation (8), the dependence of the ML decoder on α_j and β_j is made explicit.

5.4 Application of Semi-Random LDPC Codes

The embedding capacity can be greatly improved by ECC codes. In this work, we mainly focus on the powerful class of SR-LDPC codes which are linear block codes typically characterized by a sparse, pseudorandom parity-check matrix ***H*** with very low row and column weights compared to the code block size. SRLDPC codes are characterized by a low-complexity iterative belief propagation decoding algorithm. This algorithm approaches ML-optimal decoding when the associated bipartite code graph has no cycles [38]. However,

SR-LDPC encoding operation, for arbitrary random-like code constructions, is more complex than other ECC codes. In particular, the parity check matrix ***H*** has to be first transformed into systematic form to obtain the generator matrix G. In many existing image watermarking solutions, 1/2-rate regular LDPC codes of sizes ranging from 128 to 1024 bits are usually used [37]. In this paper, we will extend the watermark sequences to 2048 bits given the high capacity of the proposed watermarking scheme and the efficiency of SR-LDPC codes.

6. Data Hiding Capacity Estimates

The proposed scheme assumes two basic configurations for watermark embedding [36]:

1. **Scalar Watermarking Game:** All SCFT host coefficients belong to a single Gaussian channel where all coefficients have equal local variance set to σ^2 and carry the same watermark energy.
2. **Parallel Watermarking Game:** In this configuration, the SCFT host coefficients are assigned to different (parallel) Gaussian channels based on the level of their local variances.

In the scalar watermarking game, the watermark embedder and attacker (zero-sum game players) are allowed to introduce distortions bounded by D_1 and D_2, respectively. In this case, the data hiding capacity is defined as [36]:

$$C = \Gamma\left(\sigma^2, D_1, D_2\right) \overset{\Delta}{=} \begin{cases} \frac{1}{2}\log\left(1+\frac{D_1}{D}\right), & \text{if } D_1 < D_2 < \sigma^2 \\ 0, & \text{if } D_2 \geq \sigma^2 \end{cases} \tag{9}$$

where $D \overset{\Delta}{=} \sigma^2 \frac{D_2 - D_1}{\sigma^2 - D_2}$. In most cases, the host coefficient energy is larger than the distortion levels by order of magnitudes. Therefore, given that $\sigma^2 >> D_1$, D_2 and $D = D_2 - D_1$, we can write:

$$C \approx \frac{1}{2}\log\left(1+\frac{D_1}{D_2 - D_1}\right) \tag{10}$$

Equation (10) hints that the capacity, ***C***, is independent of host image energy. To allow energy-aware watermark embedding, the SCFT coefficients are classified into L parallel Gaussian channels based on their local variances σ^2_l. Then, the overall data hiding capacity of the parallel channels is given by [36]:

$$C = \max_{d_1} \min_{d_2} \sum_{l=1}^{L} r_l \cdot \Gamma\left(\sigma_l^2, d_1^l, d_2^l\right) \tag{11}$$

where r_l and $\Gamma(\sigma_l^2, d^l_1, d^l_2)$ define the lth channel rate and data hiding capacity, respectively. In each channel l, the watermark embedder and attacker can apply distortions lower than d^l_1 and d^l_2, respectively.

Using a subjective evaluation tool, D_1 values for the color versions of standard *Lenna*, *Barbara*, *Peppers* and *Baboon* are found to be 50, 70, 80 and 120, respectively. Solving Equations (10) and (11) using these images results in data hiding capacity estimates summarized in **Table 1**. To assess the data hiding capacity of Tsui et al. [3], a spike model is used where the SCFT coefficients are classified into two separate channels using a coarse quantization with threshold equal to $2D_2$ [36]. At mild attacks ($D_2 = 2D_1$), Baboon image provided the highest embedding capacity of 8179 bits for regular and spike models due to the rich color texture available in this image. When this image is strongly attacked ($D_2 = 5D_1$), its capacity drops to 2921 bits to ensure watermark survival. The same image achieves the maximum data hiding capacity with 2045 bits under the spike model using Tsui et al. scheme [3]. Finally, the estimates shown in **Table 1** clearly indicate the superiority of the proposed scheme in terms of data hiding capacity thanks to the proper selection of the SCFT passband frequencies with the highest local energies.

Table 1. Total data-hiding capacities (in bits) for images of size NxN = 512x512 using proposed and Tsui et al. [3] watermark embedding schemes.

Image	D_1	$D_2 = 2\ D_1$		$D_2 = 5\ D_1$	
		Capacity	Capacity (Spike)	Capacity	Capacity (Spike)
Lenna (proposed)	**50**	5677	5678	1827	1828
Lenna (Tsui et al.)		1419	1419	457	456
Barbara (proposed)	**70**	5677	5678	1827	1828
Barbara (Tsui et al.)		1419	1419	457	456
Peppers (proposed)	**80**	6242	6243	2057	2058
Peppers (Tsui et al.)		1560	1560	514	514
Baboon (proposed)	**120**	**8179**	**8179**	**2921**	**2921**
Baboon (Tsui et al.)		2044	2045	730	730

7. Simulation Results

We run experiments to evaluate the performance of the proposed color image watermarking scheme using standard color images such as *Lenna*, *Woman*, *Peppers* and *Baboon*. In addition, a database consisting of 6000 color images is used to report averaged performance results. Sample images of this database are illustrated in **Fig. 5**. To highlight the performance improvement of the proposed scheme, performance evaluation results pertaining to the schemes proposed by Tsui et al. [3] and Wang et al. [15] are also presented. We will thoroughly investigate:

- Effect of watermark embedding on image perceptual quality.
- Effects of detector structure on watermark recovery.
- Data hiding capacity improvement using ECC codes.
- Robustness to affine, geometric and color attacks.
- Robustness to JPEG and JPEG 2000 coding and compression attacks.
- Detection performance using perceptual embedding weights

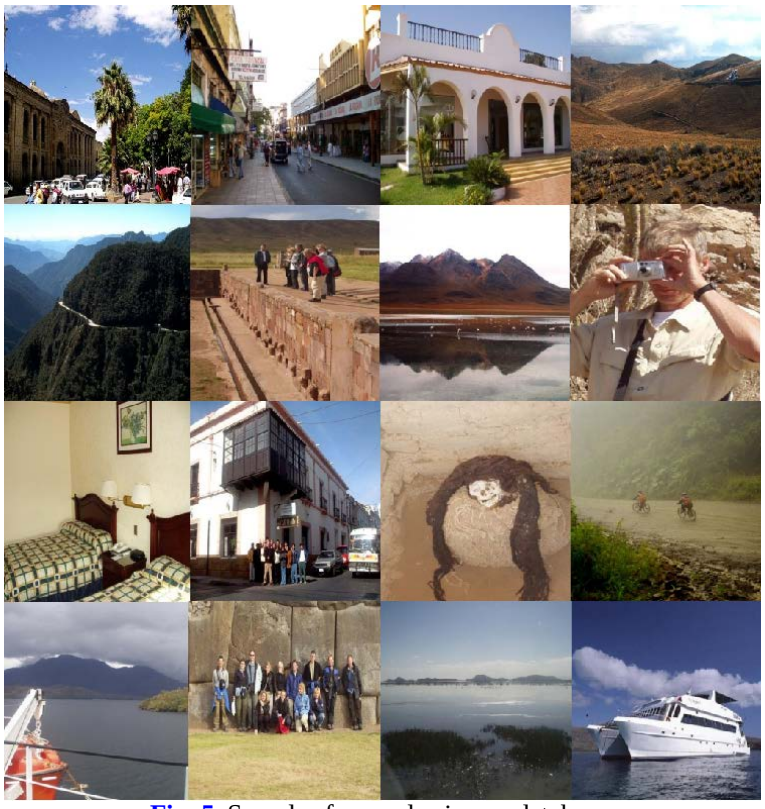


Fig. 5. Samples from color image database.

Throughout the evaluation experiments, each watermark bit is repeated a specific number of times which will further enhance the robustness of the watermark sequences. The repetition or chip rate is defined based on the watermark length sequence, which varies from 128 to 2048 bits.

7.1 Performance Measure

The performance of the proposed scheme is evaluated using the normalized bit error rate (BER). Given two L-length binary sequences, $\boldsymbol{w_{orig}}$ and $\boldsymbol{w_{rec}}$, the normalized BER is defined by:

$$BER = \frac{\sum_{i=1}^{L} w_{orig}^{i} \oplus w_{rec}^{i}}{L} \tag{12}$$

where $\oplus$ represents the bit-wise logical XOR operator. To ensure the unbiasedness of the performance evaluation experiments, we will report 100 runs-averaged normalized BER using all color images in the database.

7.2 Effect of watermark embedding on image perceptual quality

To assess the effect of watermark embedding on the image perceptual quality, we will quantify the watermark imperceptibility using the peak signal-to-noise ratio (PSNR) measure. The PSNR measure is based on the mean square error (MSE) measure. Given two M-by-N images $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$, the MSE measure is given by:

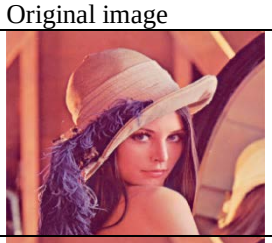
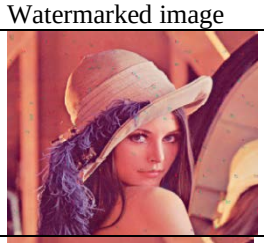
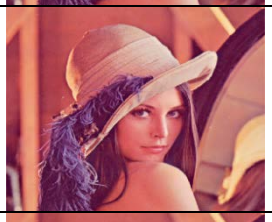
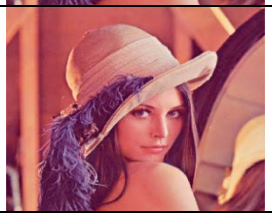
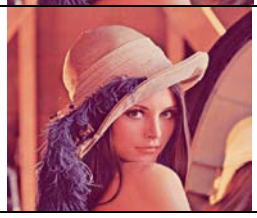
$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_1(x,y) - I_2(x,y)\right)^2 \tag{13}$$

Then, the PSNR measure (in decibels) is defined as:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{14}$$

where 255 is used to represent the maximum value of an image pixel. Watermark payloads with 1024 bits are concealed in *Lenna* image using the proposed, Tsui et al. [3] and Wang et al. [15] embedding schemes. **Table 2** summarizes the resulting perceptual quality in the watermarked images. **Table 2** reveals an interesting aspect of Tsui et al. scheme where the embedding has not only impaired the host image quality but also its color as "greenish" spots start appearing on the watermarked image.

Table 2. Effect of watermark embedding on image perceptual quality using PSNR measure.

	Original image	Watermarked image	PSNR (dB)
Tsui et al. scheme [3]			**28.90**
Wang et al. scheme [15]			**40.30**
Proposed scheme			**108.88**

7.3 Effects of Detector Structure on Watermark Recovery

This experiment contrasts the performance of model-based detection, used in our watermarking algorithm, to that using standard correlation and covariance measures where the watermark sequences are recovered from attack-free watermarked images. A correlation detector, the simplest among available watermark detectors, is optimal only when the watermark payload in embedded into the host image in an additive fashion using host features that are normally-distributed [37]. The simplest form of a correlation detector is given by:

$$det\_bit = \begin{cases} 1 & \text{if } corr(c_w, wat_{seq}) > \tau_{det} \\ \text{no watermark} & \text{if } -\tau_{det} \leqslant corr(c_w, wat_{seq}) \leqslant \tau_{det} \\ 0 & \text{if } corr(c_w, wat_{seq}) < -\tau_{det} \end{cases} \tag{15}$$

where $\boldsymbol{corr(c_w, wat_{seq})}$ and τ_{det} are the inner product between the watermark coefficient and payload vectors and the detection threshold, respectively.

However, the embedding is neither additive as shown in Equation (6) nor the watermarked coefficients are normally-distributed [5]. In fact, optimum detection is ensured only using a Bayes detector where the statistical characteristics of the SCFT coefficients are taken into consideration. It is worth noting that the correlation detector, defined in Equation (15), would perform better if the elements of the inner product, $\boldsymbol{corr(c_w, wat_{seq})}$, were orthogonal. When the orthogonality assumption does not hold, it is preferred to use a covariance detector instead. A covariance detector is a mean-normalized version of the correlation detector [37].

Fig. 6 summarizes the performance of the proposed ML-based detector and correlation- and covariance-based detectors as well. It is interesting to note that the covariance-based detector does not only outperform the correlation-based one but it attains low BERs similar to the ML-based detector. The ML-based detector achieved the best decoding performance with zero decoding errors when recovering sequences of 128 and 256 bits. In addition, more than 85% of 2048 bits are decoded correctly by this detector. This clearly indicates that the ML-based achieves double embedding capacity compared to the correlation-based counterpart thanks to the Weibull distribution modeling [37].

Therefore, the ML-based detector will be used throughout the remaining performance evaluation experiments.

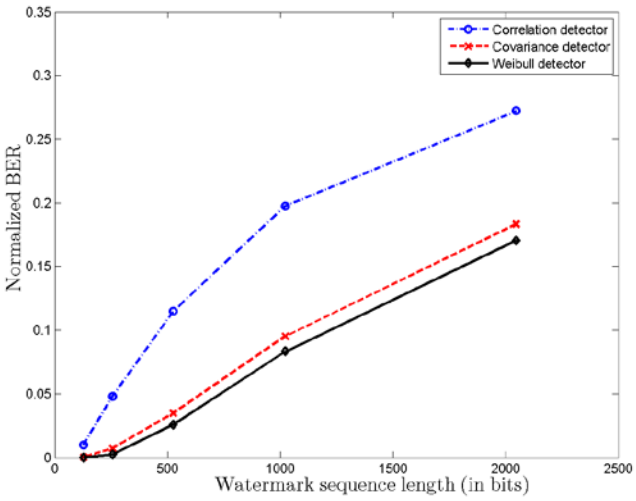


Fig. 6. BER performance of proposed scheme using different watermark detector structures.

7.4 Data Hiding Capacity Improvement Using ECC codes

Using the ML-based watermark detector, we will investigate the effect of BCH and SR-LDPC codes on the data hiding capacity.

7.4.1 BCH Codes

Bose-Chaudhuri-Hocquenghem (BCH) codes, a special class of cyclic linear block codes, are binary codes characterized by the tuple ***(n, t, k)*** where n, t and k represent the code block length, the message length and the error correction capability, respectively. Given a block length of few hundred bits and a specific code rate, BCH codes usually outperform all other block codes [39]. Given a channel with error probability p_{ch}, the BER of an (n, t, k) BCH code is approximated as [39]:

$$BER \approx \frac{1}{n}\sum_{m=t+1}^{n} m\binom{n}{m} p_{ch}^{m}(1-p)^{n-m} \tag{14}$$

Table 3 gives the approximated BER rates for various 1/2 BCH codes codes considered in this paper.

Table 3. BER rates of various 1/2 BCH codes.

n	k	t	BER(pch= 0.001)	BER(pch= 0.01)	BER(pch= 0.1)
15	7	2	$9.02 \cdot 10^{-8}$	$8.40 \cdot 10^{-5}$	$4.15 \cdot 10^{-2}$
31	16	3	$3.97 \cdot 10^{-9}$	$3.31 \cdot 10^{-5}$	$5.85 \cdot 10^{-2}$
63	30	6	$5.85 \cdot 10^{-14}$	$3.80 \cdot 10^{-7}$	$5.96 \cdot 10^{-2}$
127	64	10	$1.73 \cdot 10^{-19}$	$6.71 \cdot 10^{-9}$	$8.20 \cdot 10^{-2}$
255	123	19	$1.62 \cdot 10^{-32}$	$2.16 \cdot 10^{-13}$	$9.30 \cdot 10^{-2}$
511	250	31	$2.59 \cdot 10^{-47}$	$3.94 \cdot 10^{-17}$	$9.99 \cdot 10^{-2}$

Given a channel with probability of error, $p_{ch} = 0.01$, an (127, 64, 10) BCH code will achieve a decoding accuracy improvement of two magnitude orders compared to an (31, 16, 3) BCH code. At watermark lengths of 128 and 256 bits, all BCH codes achieve error-free watermark recovery. At longer watermark sequences, the (15, 7, 2) BCH code yielded the lowest decoding errors of 0.2% , 2.48% and 13.67% for watermark sequences with 512, 1024 and 2048 bits, respectively. The worst performance with decoding errors up to 17.41% is attributed to the (127, 64, 10) BCH code at the recovery of watermark sequences with 2048 bits.

7.4.2 1/2 SR-LDPC Codes

Using the same settings as above, watermark sequences of lengths 128 bits to 2048 bits were recovered using the ML-based detector and 1/2 SR-LDPC codes. **Fig. 7** summarizes the decoding performance of the proposed scheme. For comparison purposes, the performance of the best BCH code with size (15, 7, 2) is also reported. At short lengths (128 and 256 bits), both codes yielded error-free watermark sequences. However, at medium and long sequences, SR-LDPC codes do not only outperform the best BCH code but attained BER rates smaller by orders of magnitudes. For instance, while the SR-LDPC code successfully recovered 98% of the 2048 watermark bits of the watermark sequences, the best BCH code failed to correctly decode 14% of the same sequences. **Fig. 7** clearly confirms the superiority of SR-LDPC codes reported in the literature [38].

Therefore, the 1/2 SR-LDPC codes will be used in the remaining performance evaluation experiments.

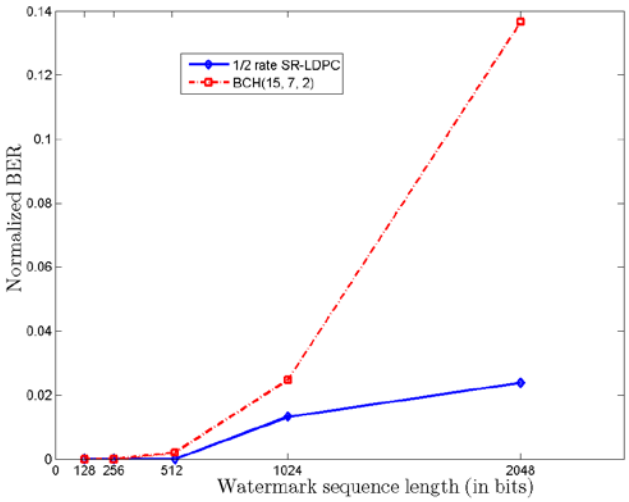


Fig. 7. BER performance of ½ SR-LDPC and (15, 7, 2) BCH codes.

7.5 Robustness to Affine, Geometric and Color Attacks

7.5.1 Affine and Geometric Attacks

The robustness to intentional attacks ranging from mild to severe is evaluated below.

Table 4 provides a summary of the performance of the proposed and Tsui et al. schemes under median and Wiener filtering attacks where all watermarked images were processed through local median and Wiener filters. The size of these filters was varied from 3x3 to 11x11 prior to watermark decoding. Under median filtering attack, the lowest performance of the proposed scheme did not exceed 6% of decoding errors, which is not the case of Tsui et al. scheme, which recovered the watermark sequences with approximately half of the bits in errors.

The effect of Wiener filtering attack on Tsui et al. scheme is quite intriguing since we always obtain a fixed decoding error rate regardless of the filter size. The normalized BER rates fluctuated around 50%. However, the performance of the proposed scheme degraded linearly with the increase in the filter size and watermark sequence. This scheme recovered 128 bits watermark sequences without errors under 3x3 filter attack. Against 11x11 Wiener filters, the proposed scheme yielded its worst performance with 10.2% errors in the recovery of 2048 bits watermark sequences. At this level, the proposed scheme still outperforms the best configuration of Tsui et al. scheme which scored 49.43% of decoding errors.

Table 4. Watermark recovery BER rates of proposed and Tsui et al. [3] schemes under median and Wiener filtering attacks.

	Proposed Scheme					**Tsui et al. [3] Scheme**				
Filter / Watermark Length	128	256	512	1024	2048	128	256	512	1024	2048
Median 3x3	**0.11**	2.01	2.94	3.63	4.19	50.05	49.67	49.99	50.14	50.11
Median 5x5	4.89	4.99	5.24	5.27	5.39	50.58	50.51	49.87	49.88	49.96
Median 7x7	5.41	5.38	5.49	5.46	5.51	49.80	50.16	49.95	49.92	49.99
Median 9x9	5.46	5.38	5.52	5.51	5.52	49.89	49.85	50.56	50.17	50.13
Median 11x11	5.44	5.45	5.51	5.52	5.54	49.88	49.70	50.80	49.99	49.93

Wiener 3x3	**0**	0.42	4.53	6.43	8.0	50.31	49.53	49.72	49.95	50.41
Wiener 5x5	**4.54**	**6.61**	**8.20**	**9.31**	**10.2**	50.31	49.53	49.71	49.95	50.41
Wiener 7x7	4.54	6.61	8.20	9.31	10.2	50.31	49.53	49.71	49.95	50.41
Wiener 9x9	4.54	6.61	8.20	9.31	10.2	50.31	49.53	49.71	49.95	50.41
Wiener 11x11	4.54	6.61	8.20	9.31	**10.2**	50.31	49.53	49.71	49.95	50.41

Then, to model the effects of many image alterations, we conducted another experiment where the watermarked images were locally contaminated with a zero-mean and variable local variance additive white Gaussian noise (AWGN). The noise local variance was varied from 0.005 to 0.01 in 0.001 steps. The performance of the proposed and Tsui et al. schemes under AWGN noise attack is outlined in **Table 5**. The proposed scheme has exhibited a steady robustness to noise contamination as evidenced by watermark decoding errors not exceeding 2% for watermark sequences up to 1024 bits. However, Tsui et al. scheme yielded a fluctuating performance where approximately 50% of watermark bits were erroneously recovered. The increase in the BER, exhibited by our proposed scheme, at higher watermark payloads is mainly attributed to the reduction of the available embedding bandwidth at such payloads which impacts the overall signal-to-noise ratio (SNR) which, in turn, affects the watermark decoder performance.

Table 5. Watermark recovery BER rates of proposed and Tsui et al. [3] schemes under AWGN noise attack with variable variance σ^2_n.

	Proposed Scheme					**Tsui et al. [3] Scheme**				
Noise Variance / Watermark Length	128	256	512	1024	2048	128	256	512	1024	2048
σ^2_n = 0.005	**1.35**	1.53	1.66	1.75	2.38	50.10	49.90	49.53	49.99	50.12
σ^2_n = 0.006	1.71	1.76	1.86	1.90	2.61	50.30	50.08	49.71	49.98	49.71
σ^2_n = 0.007	1.73	1.81	1.88	1.91	2.71	49.77	50.17	49.80	50.26	50.12
σ^2_n = 0.008	1.77	1.83	1.89	1.93	2.72	50.09	49.82	50.10	49.93	50.01
σ^2_n = 0.009	1.77	1.85	1.90	1.93	2.82	49.53	49.89	49.89	50.07	50.01
σ^2_n = 0.01	1.80	1.87	1.90	1.95	**2.83**	49.54	49.77	49.73	49.87	50.04

Finally, the class of geometric attacks represents the hardest type of watermark attacks that can severely damage the embedded watermarks [36]. To assess the robustness of the proposed scheme to this class of attacks, the watermarked images were rotated clockwise using angles varying from 1 to 26 degrees. The performance of the proposed and Tsui et al. schemes under this attack is summarized in **Table 6**. Given the effect of image rotation on the watermark recovery, the proposed scheme attained one of its lowest performances where more than 10% of the bits were not successfully recovered. This performance degradation confirms the need for a rotation-invariant embedding to ensure acceptable robustness against this type of attacks. The effect of this attack on the robustness of Tsui et al. scheme is more severe as indicated by the high BER rates reaching up to 50%.

Table 6. Watermark recovery BER rates of proposed and Tsui et al. [3] schemes under image rotation attack with variable angle θ_{rot}.

	Proposed Scheme					**Tsui et al. [3] Scheme**				
Rotation Angle / Watermark Length	128	256	512	1024	2048	128	256	512	1024	2048
$\theta_{rot} = 1^o$	**9.93**	9.98	10.08	9.99	10.03	50.02	49.95	50.28	50.16	50.07
$\theta_{rot} = 6^o$	9.94	10.02	9.99	10.07	9.97	50.73	50.13	49.87	50.25	49.96
$\theta_{rot} = 11^o$	10.0	10.02	10.04	9.96	10.01	50.15	50.47	50.21	50.16	49.99
$\theta_{rot} = 16^o$	10.13	9.97	10.0	10.02	10.02	50.51	49.9	49.96	50.14	50.02
$\theta_{rot} = 21^o$	9.94	10.05	10.01	10.03	10.03	49.99	50.15	50.05	50.24	49.98
$\theta_{rot} = 26^o$	9.99	10.02	10.06	10.02	**10.03**	51.59	49.82	50.02	50.0	49.96

7.5.2 Color Attacks

Both proposed and Tsui et al. schemes exploit the color information in host images to conceal the watermark payloads which makes color manipulation an appropriate attack. In this experiment, we will consider two color manipulation attacks: 1) color component swapping in the CIEL*a*b* space and 2) color-to-gray conversion. The former attack is illustrated in **Fig. 8** where the a* and b* components are swapped in the watermarked versions of *Lenna*, *Woman*, *Peppers* and *Baboon*.

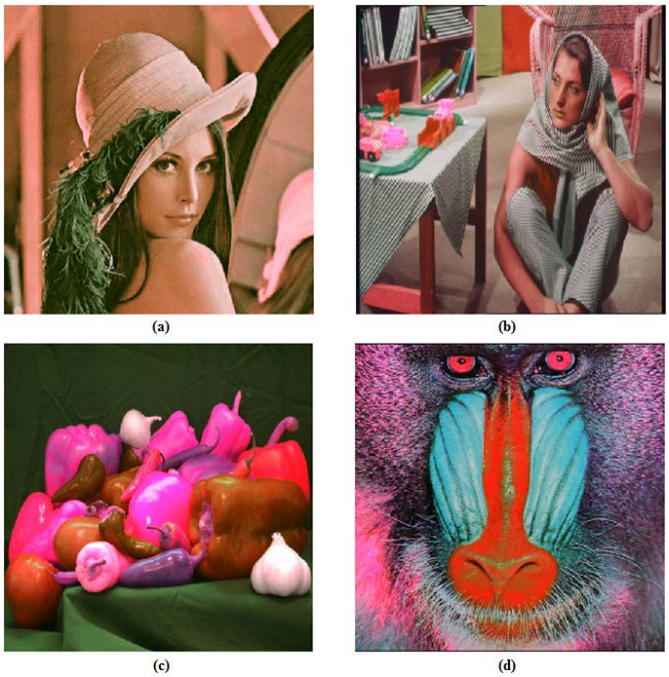


Fig. 8. Effect of a* and b* swapping attack on color images. (a) *Lenna*. (b) *Woman*. (c) *Peppers*. (d) *Baboon*.

Table 7 gives a summary of performance of the proposed and Tsui et al. schemes under these attacks. Under color swapping attack, the proposed scheme recovered watermark sequences up to 512 bits without errors. The decoding performance degraded with longer watermark sequences where more than 23% of the recovered bits were in error. On the other hand, Tsui et al. scheme performed very poorly with all watermark lengths to score a low BER of 50% which means basically a ”*guess*”-based decoding. The effect of gray-to-scale conversion

attack on the proposed scheme is less in terms of decoding accuracy where this scheme attained its best and worst performance with BER rates of 10.66% and 12.44%, respectively. However, this attack has an effect similar to that of color swapping on Tsui el al. scheme and the lowest decoding error was approximately 49.31%.

Table 7. Watermark recovery BER rates of proposed and Tsui et al. [3] schemes under color manipulation attacks.

	Proposed Scheme					**Tsui et al. [3] Scheme**				
Color Attack	128	256	512	1024	2048	128	256	512	1024	2048
Swapping of a* and b*	**0**	**0**	**0**	12.16	**23.48**	50.30	50.38	49.77	50.20	50.15
Color-To-Gray	10.66	10.97	11.24	11.80	12.44	49.31	49.64	50.16	49.75	50.11

7.6 Robustness to JPEG and JPEG 2000 Image Coding and Compression Attacks

Fig. 9 depicts the effects of JPEG and JPEG 2000 compressions on Woman and Peppers images. At very low quality factor (QF) and bits per pixel (bpp) values, the severe compression effect is easily noticeable as indicated by **Fig. 9-c** and **Fig. 9-d** in the case of QF = 5 and 0.01 bpp for JPEG and JPEG 2000 image coders, respectively. **Fig. 9** hints that JPEG/JPEG 2000 compression attacks should be carried out using image quality-preserving levels only. In this attack scenario, all watermarked images were compressed using MATLAB© JPEG and a standard JPEG 2000[2] coders. While the QF in the JPEG coder was varied from 100 to 5, the compression rates in the JPEG 2000 coder ranged from 8 bpp to 0.05 bpp.

Fig. 9. (a) Original *Woman*. (b) JPEG-compressed *Woman* using QF = 5. (c) Original *Peppers*. (b) JPEG 2000-compressed *Peppers* using 0.01 bpp.

[2] Kakadu software available at http://www.kakadusoftware.com.

The robustness of the proposed and Tsui et al. schemes to these attacks is outlined in **Table 8**. At high QF values (e.g., QF=100), the proposed scheme recovered the watermarked sequences with decoding errors of 7.83% and 14.09% for shortest and longest watermark sequences, respectively. However, at QF values lower than 70, the decoding accuracy deteriorated rapidly to reach 16.99% errors at its lowest performance. This indicates that some watermark locations are impaired with JPEG compression at low QF values (below 20 mainly). The scheme, proposed by Tsui et al., exhibited a performance trend similar to that under affine, geometric and color attacks with best performance attained at BER rates of 49.23%.

Table 8. Watermark recovery BER rates of proposed and Tsui et al. [3] schemes under JPEG and JPEG 2000 (J2K) attacks.

	Proposed Scheme					**Tsui et al. [3] Scheme**				
Compression Attack	128	256	512	1024	2048	128	256	512	1024	2048
JPEG QF = 100	**7.83**	10.20	11.67	13.02	14.09	49.99	50.04	49.50	49.97	49.97
JPEG QF = 70	7.50	17.27	16.97	16.89	16.89	49.23	50.50	50.37	50.02	49.97
JPEG QF = 40	17.41	17.22	16.83	16.88	16.74	50.35	50.38	49.95	50.19	49.90
JPEG QF = 20	16.99	17.08	16.64	16.71	16.72	50.04	49.93	50.18	49.95	50.05
JPEG QF = 10	16.82	16.89	16.60	16.77	16.71	50.23	49.77	50.10	50.13	50.10
JPEG QF = 5	16.91	16.65	16.65	16.64	16.66	49.88	50.14	50.24	49.72	49.69
J2K rate = 8 bpp	**0**	**0**	0.02	5.96	8.96	49.65	49.19	49.93	49.84	50.21
J2K rate = 4 bpp	7.75	10.35	11.87	13.21	14.21	49.98	49.65	49.98	50.0	50.09
J2K rate = 1 bpp	16.39	16.56	16.66	16.47	16.64	50.63	50.33	49.40	50.05	50.15
J2K rate = 0.5 bpp	16.67	16.93	16.88	16.63	16.76	50.35	50.30	50.02	50.08	50.02
J2K rate = 0.1 bpp	**50.61**	**50.07**	**50.09**	**49.92**	**49.95**	50.23	49.89	49.50	49.94	50.12
J2K rate = 0.05 bpp	**49.57**	**50.37**	**50.28**	**49.78**	**50.10**	51.15	50.56	50.14	50.35	50.03

Under JPEG 2000 compression attack, the proposed scheme successfully recovered the 128 and 256 bits watermark sequences without errors. Then, the decoding performance dropped linearly with the increase in the compression rate up to 0.5 bpp where decoding errors did not exceed 17%. However, the robustness of the proposed scheme drops drastically at high compression rates (i.e., low bpp values). This performance deterioration is mainly due to the severe damage impacted on the watermarked images by such compression attacks as clearly indicated in **Fig. 9-d**. In fact, at these rates, the "*value*" of attacked images becomes worthless and the watermark decoder is merely "guessing" the watermark bits.

7.7 Detection Performance Using Perceptual Embedding Weights

Sections 7.5 and 7.6 assessed the performance of the embedding algorithm proposed by Tsui et al. [3] and its extension suggested in this paper. To complete the performance analysis, this section extends our analysis to investigate the performance of another full-color image watermarking scheme proposed by Wang et al. [15]. Setting the embedding rate (α_i) of our proposed scheme to half the optimal NUJNCD-thresholds and the watermark payload to 128 bits, we investigated the performance of the watermark detector using true and false positive rates (tpr and fpr). Results in **Fig. 10** summarize the experimental approach in reference [40][3]. The embedding strength, Δ, of Wang et al. scheme is set to 270 as suggested in their paper. **Fig. 10** depicts the resulting receiver operating characteristic (ROC) curves using the tpr and fpr measures. In agreement with the previous simulation results, Tsui et al. scheme is mainly

[3] This approach is suggested by one of the anonymous reviewers and reference [40] as well.

behaving through "guessing" the watermark sequence as evidenced by the almost-straight line behavior in **Fig. 10**. On the other hand, Wang et al. and our proposed schemes exhibited an excellent performance where no loss in robustness is noted. In addition, the introduction of the NUJNCD-based perceptual model has significantly enhanced the robustness of our proposed scheme without targeting a given perceptual quality of the watermarked images [40].

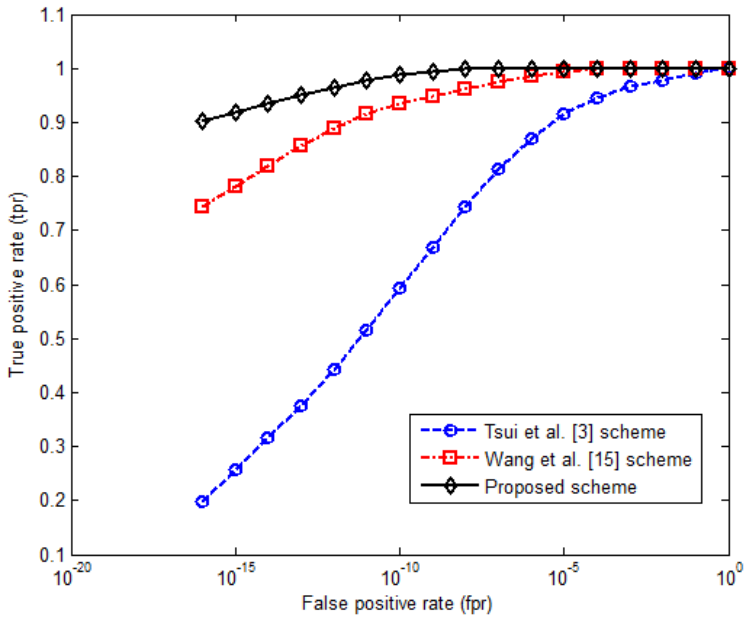


Fig. 10. ROC curves of proposed, Tsui et al. [3] and Wang et al. [15] schemes.

7.8 General Comments

The robustness of the proposed scheme to typical image and color attacks has been thoroughly assessed using a large database of 6000 color images. Also, this scheme has outperformed existing full-color schemes in terms of robustness to standard image/color attacks and hiding capacity in all attack scenarios considered. This performance superiority is mainly attributed to the use of: 1) a larger support for watermark embedding (SCFT subbands); 2) ML-based watermark detector using Weibull distribution; and 3) SR-LDPC codes that extend further the embedding capacity. However, it should be noted that Tsui et al. scheme concealed watermark payloads in a very limited number of SCFT coefficients, which drastically reduces the available hiding capacity. In addition, it does neither incorporate code repetition nor ECC coding strategy which results in poor performance compared to the proposed scheme.

8. Conclusion

In this paper, we have proposed a new approach for embedding watermark payloads into the chrominance components of host color images in the CIEL*a*b* space. The SCFT transform is astutely exploited thanks to its capability to produce colors by simple color arithmetic (addition and subtraction). A well-established perceptual model is adopted to ensure watermark imperceptibility through perceptual redundancy. The perceptual model, based on an emerging color image model, exploits the non-uniform just-noticeable color difference (NUJNCD) thresholds of the CIEL*a*b* space. To maximize the data hiding capacity of the proposed scheme, SR-LDPC codes are used in conjunction with spread-spectrum modulation

and code repetition, which simultaneously maximizes the watermark size and robustness by orders of magnitude, compared to existing color-based embedding schemes. In addition, the data hiding capacity of our scheme relies on a game-theoretic model where upper bounds for watermark embedding are derived. Extensive performance evaluation experiments demonstrate the robustness of the proposed scheme to various intentional and accidental attacks including affine, geometric, compression/encoding and color alteration attacks.

Acknowledgments

The author would like to thank King Fahd University of Petroleum and Minerals (KFUPM) University for supporting this work and the anonymous reviewers whose comments have drastically improve the overall paper quality.

References

[1] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking," *EURASIP Journal on Applied Signal Processing*, vol. 2002, January. Article (CrossRef Link)

[2] D. J. Fleet and D. J. Heeger, "Embedding invisible information in color images," in *Proc. of the IEEE International Conference on Image Processing (ICIP' 97)*, vol. 1, pp. 532–535, 1997. Article (CrossRef Link)

[3] T. K. Tsui, X.-P. Zhang, and D. Androutsos, "Color image watermarking using multidimensional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 16–28, March 2008. Article (CrossRef Link)

[4] G. Sharma, W. Wu, and E. N. Dalal, "The CIEDE 2000 color-difference formula: Implementation notes, supplementary test data, and mathematical observations," *Color Research & Application*, vol. 30, pp. 21–30, February 2005. Article (CrossRef Link)

[5] P. Moulin and M. K. Mihçak, "A framework for evaluating the data-hiding capacity of image sources," *IEEE Transactions on Image Processing*, vol. 11, no. 9, pp. 1029–1042, September 2002. Article (CrossRef Link)

[6] C.-H. Chou, and K.-C. Liu, "Color image watermarking based on a color visual model," in *Proc. of the Second IEEE Workshop on Multimedia Signal Processing*, pp. 367–370, 2002. Article (CrossRef Link)

[7] C.-H. Chou, and T.-L. Wu, "Embedding color watermarks in color images," *EURASIP Journal on Applied Signal Processing*, vol. 2003, pp. 32–40, 2003. Article (CrossRef Link)

[8] P. Bas, N. Le Bihan, and J.-M. Chassery, "Color image watermarking using quaternion Fourier transform," in *Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP' 03)*, vol. 3, pp. 521–524, 2003. Article (CrossRef Link)

[9] C.-H. Chou and K.-C. Liu, "A perceptually tuned watermarking scheme for color images," *IEEE Transactions on Image Processing*, vol. 19, pp. 2966–2982, November 2010. Article (CrossRef Link)

[10] L. Ghouti and M. A.Landolsi, "Robust color image watermarking using the spatio-chromatic Fourier transform and semi-random LDPC codes," in *Proc. of the IEEE Computer and Communication Engineering (ICCCE' 12)*, vol. 1, pp. 349–353, July 2012. Article (CrossRef Link)

[11] F.-N. Lang, J.-L. Zhou, S. Cang, H. Yu, and Z. Shang, "A self-adaptive image normalization and quaternion pca based color image watermarking algorithm," *Expert Systems with Applications*, vol. 39, pp. 12046–12060, November 2012. Article (CrossRef Link)

[12] Z. Shao, Y. Duan, G. Coatrieux, J. Wu, J. Meng, and H. Shu, "Combining double random phase encoding for color image watermarking in quaternion gyrator domain," *Optics Communications*, vol. 343, pp. 56–65, May 2015. Article (CrossRef Link)

[13] Z. Shao, J. Wu, J.-L. Coatrieux, G. Coatrieux, and H. Shu, "Quaternion gyrator transform and its application to color image encryption," in *Proc. of the 20th IEEE International Conference on Image Processing (ICIP' 13)*, pp. 4579–4582, September 2013. Article (CrossRef Link)

[14] F. Lusson, K. Bailey, M. Leeney, and K. Curran, "A novel approach to digital watermarking, exploiting colour spaces," *Signal Processing*, vol. 93, pp. 1268–1294, May 2013. Article (CrossRef Link)
[15] X.-Y. Wang, C.-P. Wang, H.-Y. Wang, and P.-P. Niu, "A robust blind color image watermarking in quaternion Fourier transform domain," *Journal of Systems and Software*, vol. 86, pp. 255–277, February 2013. Article (CrossRef Link)
[16] J. Ouyang, H. Shu, X. Wen, J. Wu, F. Liao, and G. Coatrieux, "A blind robust color image watermarking method using quaternion Fourier transform," in *Proc. of the 2013 6th International Congress on Image and Signal Processing*, CISP 2013, pp. 485–489, 2013. Article (CrossRef Link)
[17] E. D. Tsougenis, G. A. Papakostas, D. E. Koulouriotis, E. G. Karakasis, and D. A. Karras, "Color image watermarking via quaternion radial Tchebichef moments," in *Proc. of the IEEE International Conference on Imaging Systems and Techniques (IST' 13)*, pp. 101–105, 2013. Article (CrossRef Link)
[18] B. Chen, G. Coatrieux, X. Sun, J.-L. Coatrieux, and H. Shu, "Full 4-d quaternion discrete Fourier transform based watermarking for color images," *Digital Signal Processing*, vol. 28, pp. 106–119, May 2014. Article (CrossRef Link)
[19] X.-Y. Wang, P.-P. Niu, C.-P. Wang, and A.-L. Wang, "A new robust color image watermarking using local quaternion exponent moments," *Information Sciences*, vol. 277, pp. 731–754, September 2014. Article (CrossRef Link)
[20] E. D. Tsougenis, G. A. Papakostas, D. E. Koulouriotis, and E. G. Karakasis, "Adaptive color image watermarking by the use of quaternion image moments," *Expert Systems with Applications*, vol. 41, pp. 6408–6418, October 2014. Article (CrossRef Link)
[21] H.-Y. Yang, X.-Y. Wang, P.-P. Niu, and A.-L. Wang, "Robust color image watermarking using geometric invariant quaternion polar harmonic transform," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 11, pp. 1–26, February 2015. Article (CrossRef Link)
[22] Q. Su, Y. Niu, X. Liu and Y. Zhu, "A blind dual color images watermarking based on IWT and state coding," *Optics Communications*, vol. 285, no. 7, pp. 1717–1724, April 2012. Article (CrossRef Link)
[23] H. M. Al-Otum and N. A. Samara, "A robust blind color image watermarking based on wavelet-tree bit host difference selection," *Signal Processing*, vol. 90, no. 8, pp. 2498–2512, August 2010. Article (CrossRef Link)
[24] E. Vahedi,R. A. Zoroofi, and M. Shiva, "Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles," *Digital Signal Processing*, vol. 22, no. 1, pp. 153–162, January 2012. Article (CrossRef Link)
[25] I. Prathap, V. Natarajan, and R. Anitha, "Hybrid robust watermarking for color images," *Computers & Electrical Engineering*, vol. 40, no. 3, pp. 920–930, April 2014. Article (CrossRef Link)
[26] Q. Su, Y. Niu, Q. Wang, and G.Sheng, "A blind color image watermarking based on DC component in the spatial domain," *Optik - International Journal for Light and Electron Optics*, vol. 124, no. 23, pp. 6255–6260, December 2013. Article (CrossRef Link)
[27] O. Findik, I. Babaoglu, and E. Ülker, "A color image watermarking scheme based on artificial immune recognition system," *Expert Systems with Applications*, vol. 38, no. 3, pp. 1942–1946, March 2011. Article (CrossRef Link)
[28] K-C. Liu, "Wavelet-based watermarking for color images through visual masking," *AEU - International Journal of Electronics and Communications*, vol. 64, no. 2, pp. 112–124, February 2010. Article (CrossRef Link)
[29] L. Zhen, L. J. Karam, and A. B. Watson, "JPEG2000 encoding with perceptual distortion control," *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 1763–1778, July 2006. Article (CrossRef Link)

[30] Q. Su, Y. Niu, H. Zou, and X. Liu, "A blind dual color images watermarking based on singular value decomposition," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8455–8466, April 2013. Article (CrossRef Link)
[31] H. M. Al-Otum and S. S. Al-Sowayan, "Color image watermarking based on self-embedded color permissibility with preserved high image quality and enhanced robustness," *AEU - International Journal of Electronics and Communications*, vol. 65, no. 7, pp. 619–629, July 2011. Article (CrossRef Link)
[32] M. E. Moghaddam and N. Nemati, "A robust color image watermarking technique using modified Imperialist Competitive Algorithm," *Forensic Science International*, vol. 233, no. 1–3, pp. 193–200, December 2013. Article (CrossRef Link)
[33] B. Ou, X. Li, Y. Zhao, and R. Ni, "Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding," *Signal Processing*, vol. 108, no. 3, pp. 642–657, March 2015. Article (CrossRef Link)
[34] A. McCabe, T. Caelli, G. West, and A. Reeves, "Theory of spatiochromatic image encoding and feature extraction," *Journal of Optical Society of America Part A*, vol. 17, pp. 1744–1754, October 2000. Article (CrossRef Link)
[35] R. S. Hunter and R. W. Harold, "The measurement of appearance," *New York, NY: John Wiley and Sons*, 2nd ed., 1987. Article (CrossRef Link)
[36] L. Ghouti, A. Bouridane, M. K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets," *IEEE Transactions on Signal Processing*, vol. 54, no. 4, pp. 1519–1536, April 2006. Article (CrossRef Link)
[37] A. Bastug and B. Sankur, "Improving the payload of watermarking channels via LDPC coding," *IEEE Signal Processing Letters*, vol. 11, pp. 90–92, February 2004. Article (CrossRef Link)
[38] D. J. Costello and S. Lin, "Error control coding," *NJ: Prentice Hall, 2nd edition*, New Jersey, 2004.
[39] M. A. Landolsi, "A comparative performance and complexity study of short-length LDPC and turbo product codes," in *Proc. of the IEEE International Conference on Information and Communications (ICTTA' 06)*, vol. 2, pp. 2359–2364, April 2006. Article (CrossRef Link)
[40] M. Urvoy, D. Goudia, and F. Autrusseau, "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1108–1119, July 2014. Article (CrossRef Link)

Lahouari Ghouti received his Ph.D. degree in Computer Science from Queens University of Belfast (QUB), U.K., in 2005. He worked as a Research Fellow in collaboration with EPSRC-UK and UK Forensic Services. Currently, he is an Associate Professor at the Department of Information and Computer Science at King Fahd University of Petroleum and Minerals. He holds 22 US patents in the fields of Information and Multimedia security. His research interests include multimedia content identification and security. He has authored and co-authored more than 60 publications. Dr. Ghouti is a Member of the IEEE Signal Processing Society.