Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images

Yang Zhao, Patrizio Campisi, *Member, IEEE*, and Deepa Kundur, *Senior Member, IEEE*

***Abstract*—This paper proposes an approach for the combined image authentication and compression of color images by making use of a digital watermarking and data hiding framework. The digital watermark is comprised of two components: a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression. The multipurpose watermark is designed by exploiting the orthogonality of various domains used for authentication, color decomposition and watermark insertion. The approach is implemented as a DCT-DWT dual domain algorithm and is applied for the protection and compression of cultural heritage imagery. Analysis is provided to characterize the behavior of the scheme under ideal conditions. Simulations and comparisons of the proposed approach with state-of-the-art existing work demonstrate the potential of the overall scheme.**

I. Image Processing for Cultural Heritage Documents

OVER the last few years, there has been a preponderance of activity in the area of digitization and processing of cultural heritage (CH) documents. Strong motivations in favor of digitization include increased preservation of the original cultural artefacts while permitting user interactivity through advanced multimedia presentation and wider distribution channels for greater educational accessibility. Digital still images of CH can undergo standard image processing functions such as image analysis, enhancement, restoration, recognition, representation, compression and image security [1], [2]. Effective application of these functions must take into account several often distinguishing features of CH images: (1) the high resolution and volume of each frame, (2) the significance of content in both the macroscopic and microscopic details of the data, and (3) the diverse distribution chains through which the image information may be traveling. Given the growing dependence of a broad spectrum of academic applications on digital high volume CH data, we focus in this paper on image processing for the compression and the preservation of integrity of CH imagery. Specifically, we propose a framework and algorithm to combine both processes that uses digital watermarking technology.

Manuscript received February 17, 2003; revised October 20, 2003. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Ioannis Pitas.

Y. Zhao is with the Edward S. Rogers, Sr., Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: yzhao@comm.utoronto.ca).

P. Campisi is with the Dipartimento di Elettronica Applicata, Universitá degli Studi di Roma "Roma Tre," 00146 Rome, Italy (e-mail: campisi@uniroma3.it).

D. Kundur is with the Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128 USA (e-mail: deepa@ee.tamu.edu).

Digital Object Identifier 10.1109/TIP.2003.821552

A. Authentication and Integrity

Authentication is the service of ensuring whether a given block of data has *integrity*, (i.e., the associated content has not been modified), and is from the legitimate sender. Authentication is traditionally ensured through mechanisms that involve message authentication codes (MACs) and digital signatures [3] known as "hard-authenticators." In hard authentication, a MAC (also known as a message digest) or digital signature of the data to protect, called an *authenticator*, is created at the source and transmitted with the data. At the receiver, the authenticator is verified using the received data to deduce if the received information is in fact unmodified and from the alleged sender.

When the data represents an image that may travel through a set of diverse distribution chains, then it can be susceptible to content-preserving operations such as compression, transcoding and other standard format conversions which severely impede the usefulness of hard-authentication mechanisms. Any processing of the image that changes the bit representation, yet still maintains the validity of perceptual content, may be inaccurately categorized as being "inauthentic." Thus, more recently there has been a movement toward schemes that provide "soft-authentication," in which content-preserving processing is distinguished from unlawful content-changing manipulations.

One tool-set that has been recently applied to soft-authentication, which will be the partial focus of this work, is called *semi-fragile digital watermarking*.[1] Here, an authenticator which may consist of a MAC or digital signature of salient parts of an image is used to form a *watermark*. This watermark is imperceptibly embedded within the original image (commonly called the *host*). The integration of the authenticator within the image to be secured simplifies the logistical problem of MAC or digital signature data handling during image transmission. Moreover, semi-fragile watermarking can provide information on the degree and location of tampering within an image to make more application-suited decisions on credibility [4].

B. Compression

Effective lossy compression of virtual heritage imagery is necessary for efficient communication while maintaining the perceptual integrity of importance in educational applications. Color, which may often be poorly preserved in virtual heritage, plays a key role in the image understanding and interpretation.

[1]In *semi-fragile* watermarking, the watermark is embedded such that it is fragile to some pre-defined processing and robust to others.

A plethora of perceptual color coding methods have been proposed in the past. Often these techniques are in conflict with digital watermarking approaches and have the effect of reducing the bandwidth possible in which to embed the watermark. Thus, methods to combine both compression and watermarking have been proposed. One such approach, called *compressive data hiding* [6] has been proposed by Campisi *et al.* In compressive data hiding, a color image is separated into luminance and chrominance components. The chrominance is embedded into the luminance using data hiding[2], and the resulting composite grayscale image is compressed using a lossy compression algorithm optimized for grayscale images. This methodology will be used in the proposed work to simultaneously perform authentication and color image compression for virtual heritage document applications.

C. Contributions and Scope

The aim of this paper is to demonstrate the application of semi-fragile watermarking and compressive data hiding for the protection and coding of CH imagery. We provide intuitive and analytic insight into our algorithmic design and focus, in part, on the testing of these principles to real CH data.

We also investigate useful digital image watermarking system properties for CH applications; in the same vein as [2], we assert that many of the general embedding properties of imperceptibility, tamper resistance through semi-fragility and bandwidth efficiency are most applicable to CH imagery applications. Thus, we build upon previous efforts involving the protection of artwork to identify security watermark and coding co-design trade-offs.

As a result of the focus on the signal processing and application aspects of the problem, we do not provide thorough analysis on the security issues related to authentication.

Section II formulates the joint authentication and watermarking problem using a digital watermarking framework. Our proposed solution is presented and analyzed under ideal conditions in Sections III and Section IV, respectively. Simulation and test results of the algorithmic behavior are presented in Section V followed by final remarks in Section VI.

II. Problem Formulation and Preliminaries

A. Formulation and Framework

Digital watermarking research has been proposed for a diverse set of applications including copy protection, image authentication, video error correction, and color image compression. In each case existing inefficiencies in the host are exploited to provide added-value services, and the design process involves reconciling fundamental compromises. This characteristic leads us to believe that digital watermarking may present a useful paradigm for joint authentication and compression for CH imagery—a problem that also requires arbitration among competing objectives. Assuming such a framework, we restrict our system for joint authentication and compression of CH images to consist of the following components:

1) The **generating function**, f_g, which produces the watermark signal W to embed as follows:

$$W = f_g(\iota, \kappa, Y) \tag{1}$$

where κ is the secret *generation key* known only to the sender and receiver, Y is the luminance of the host image X, and ι is called the watermark "payload" which is comprised of a bit sequence independent of κ and Y. In our application, W has two parts: an *authenticator watermark* component W_a employed for security and a *chrominance watermark* component W_c to help with compression. We represent this relationship as a concatenation: $W = [W_a \| W_c]$ where $\|$ is the concatenation operator.

2) The **embedding function**, f_m, which inserts the watermark signal W into the luminance host data Y with the help of a secret *embedding key* K known only to the sender and receiver, yielding the watermarked data Y^w, as follows:

$$Y^w = f_m(Y, W, K) \tag{2}$$

such that Y^w is perceptually identical to Y.

3) The **lossy compression function**, f_l, which reduces the practical storage requirements of Y^w by removing the perceptually irrelevant information to form the compressed signal $\tilde{Y}^w$ as follows:

$$\tilde{Y}^w = f_l(Y^w) \tag{3}$$

where we assume any parameters of f_l, that control the degree of compression, are prespecified. The signal $\tilde{Y}^w$ is the compressed and secured version of Y.

4) The **extracting function**, f_x, which recovers the watermark information, $\hat{W}$, from the received watermarked data, Y^r (which may differ from $\tilde{Y}^w$ because of incidental or intentional distortions in the CH image distribution chain), using the secret key K

$$\hat{W} = f_x(Y^r, K). \tag{4}$$

5) The **recovery function**, f_r, which employs $\hat{W}$ for authentication and color recovery of the image

$$[R_a, \hat{X}_w] = f_r(Y^r, \hat{W}, \kappa') \tag{5}$$

where κ' is a key available to the receiver that is different than (or the same as) κ if asymmetric (or symmetric) encryption is employed for authentication, R_a is a statistic that allows the application-dependent authentication and tamper assessment of the received luminance image Y^r, and $\hat{X}_w$ is the overall color-recovered version[3] of Y^r.

The reader should note that there is no explicit payload detection stage in the above formulation. The reason is because W_a, containing the authenticator information, needs only to be a function of Y and κ. There is no payload *per se*. In contrast, W_c contains the chrominance information which is independent of Y and κ as no security is required; thus, W_c is effectively the

[2]In this work, we use the term "data hiding" to distinguish from "watermarking" if the task does not require security through the use of a secret key or robustness to security attacks.

[3]We define the process of color recovery as the integration of the chrominance information from $\hat{\iota}$ with the luminance image Y^r to form the overall color image $\hat{X}_w$.

payload. The watermark generation step in (1) is a generalization of this process. As a result, the payload detection for W_a is unnecessary and trivial for W_c. Therefore in our formulation, watermark extraction, authentication and color recovery can be done without an explicit payload detection step.

Based on an empirical analysis of the strengths and limitations of semi-fragile watermarking and compressive data hiding, the following helpful principles for system function design have been identified [5], [6]:

- *Authenticator Watermark*: The authenticator watermark W_a should represent a secure content-based adaptive authenticator. Furthermore, the authenticator should be a function of image features that are invariant to predefined content-preserving image processing operations denoted Ω_R while fragile to specified content modification attacks denoted Ω_F. Thus, watermark generation f_g design (to produce W_a) is equivalent to developing an effective adaptive authenticator that can distinguish Ω_R from Ω_F.
- *Uniqueness of Authenticator Watermark Generation*: Different values of κ should produce distinct authenticator watermarks W_a for the same host image X and ι; different values of ι should produce distinct W_a for the same image X and the same key κ. This guarantees key-based security of W_a and unambiguous recoverability of the payload ι.
- *Chrominance Watermark*: The component of the payload ι corresponding to the chrominance watermark W_c should contain a (possibly compressed) version of the color information such that it can be later combined with the watermarked luminance image for color recovery. No security or secrecy is required in the generation or embedding of W_c.
- *Non-invertibility of Embedding*: The keys κ and K must not be more easily identifiable if the embedding method f_m and W are both known to attackers. Thus, authenticator and embedding security come from secrecy of the key.
- *Watermark Embedding Structure*: The high resolution nature of CH documents makes it practical to partition the host into distinct components—one in which to embed the authenticator component W_a and another the chrominance component W_c—and employ different embedding approaches for each. This facilitates more straightforward control over achieving both tasks of authentication and compression. Furthermore, embedding should not affect authenticator watermark generation.
- *Chrominance Embedding and Lossy Compression*: To achieve overall compression gains, chrominance embedding and lossy compression must work together. Specifically, given a coder structure f_l, the inefficiencies of compression should be exploited as unused bandwidth available for W_c embedding. Since the chrominance information, which can be extracted from the luminance image, is no longer necessary to store separately the overall volume of information is reduced.
- *Authenticator Generation and Embedding*: For authentication applications, it is important that the watermark embedding does not affect the watermark generation. If this requirement cannot be satisfied, then it can be shown that even under ideal situations, authentication is impossible because the changes imposed on host to embed the authenticator will render the image inauthentic.
- *Blind Watermark Extraction*: The watermark extraction should naturally be blind for practicality. Otherwise there would be no necessity for watermarking nor image distribution as the authentic image would be available at the destination.
- *Robustness and Fragility*: The embedding and extracting functions f_m and f_x should together be robust to the image processing operations specified by Ω_R and possibly fragile to malicious content changing attacks defined in Ω_F. Together with proper authenticator watermark generation, this provides the necessary "soft-authentication" capability.
- *Computational Efficiency*: The watermarking components should be designed for effective hardware or software implementation for practical applicability. Therefore, only linear orthogonal separable transforms are used in the design of the different system functions.

B. Orthogonality and Dual Domains

Given the design guidelines of Section II-A, we propose the use of linear orthogonal separable transforms that work in orthogonal domains of the image for watermark generation and embedding. This approach allows the independent design and analysis of the various system functions (e.g., f_g, f_m).

A review of existing digital watermarking approaches for image authentication shows that previous techniques can be classified as employing a *single domain host dependent watermark* [7]–[15] in which the image-dependent watermark generation and embedding are "mixed" in the same domain, or as involving a *host independent watermark* [4], [16]–[26], in which the watermark is a random sequence or logo independent of the image and embedded in a given domain[4]. The former class of techniques suffers from high sensitivity or the inability to appropriately localize the degradations on the signal. The latter category requires the transmission of the watermark W itself or an equivalent signal which makes the approach susceptible to eavesdropping and sophisticated attempts of fraud. In this work, we assert that the use of orthogonal subspace domains can keep the watermark embedding, which occurs in one image subspace, from interfering with watermark generation, which is applied to another orthogonal subspace, for more controlled soft authentication while overcoming the limitations of previous work.

An image-dependent authenticator watermark W_a is generated using f_g from one image subspace domain, called the *generating domain* V_{gen} of the host Y, and then is embedded using f_m into another subspace domain, called the *embedding domain* $V_{emb,a}$ of the host Y. V_{gen} and $V_{emb,a}$ are selected such that they are orthogonal subspaces; thus, any changes to the signal component in one domain will not affect the component in the other. To authenticate, the authenticator watermark is extracted using f_x from the $V_{emb,a}$ of the received image Y^r to produce

[4]The reader should note that these references are intended to provide flavor of the work in the area and are not exhaustive.

$\hat{W}_a$ and is effectively compared to the watermark $\tilde{W}_a$ generated using f_g from V_{gen} of Y^r. If a single transform domain is employed for this approach, then the resulting coefficients are often merely partitioned into two classes: those used for generation, and those for embedding. The main disadvantage of this approach is that it may not be possible to select a single transformation domain that has attractive characteristics for both watermark generation and embedding because both f_m and f_g are forced to be localized in this space. We consider making use of *dual domains* for this purpose. The selected domains should be appropriate for their respective functions yet facilitate orthogonal generation and embedding.

Similarly, such a technique can be borrowed for compressive data hiding. If we partition a color image into the luminance and chrominance subspaces V_c and V_l, respectively, and then embed the chrominance into a subspace of the luminance (denoted $V_{emb,c}$) such that we exploit the inefficiency of f_l, compression gains can be achieved [6].

Bridging both approaches, our philosophy is to break an image into the following subspaces: V_c containing the chrominance information of the image to produce W_c, and V_l containing the luminance component. Furthermore, V_l is partitioned into subspaces V_{gen} for authenticator watermark W_a generation, $V_{emb,a}$ for W_a embedding, and $V_{emb,c}$ for W_c embedding. Ideally, all subspaces should be orthogonal, so that any signal processing involved in these domains will not interfere with one another; the reader should note that V_{gen}, $V_{emb,a}$ and $V_{emb,c}$ do not necessarily span V_l. Moreover, based on our application to CH imagery, V_{gen} should allow access to "salient" image features that can be exploited by f_g to relate to the integrity of the image. Similarly, $V_{emb,a}$ should also contain features that are related to image credibility, but that can be used to characterize tampering, and $V_{emb,c}$ should be reasonably invariant to f_l so that the chrominance information can be robustly embedded.

Thus, in this paper, we empirically investigate the use of orthogonal subspaces for the design of a multipurpose dual domain security and compression approach suitable for CH images. The Section III introduces our proposed algorithm.

III. Algorithm

A. Design Guidelines for Cultural Heritage Imagery

We attempt to devise a scheme that is applicable to a wide range of CH imagery and distribution chains. Our first step is to define the acceptable and unacceptable image distortions, Ω_R and Ω_F, respectively. Because of the breadth of situations we are trying to encompass, we do not make use of analytic means of defining Ω_R and Ω_F. Instead we use empirical reasoning based on the observation that visual integrity of the image is most important in applications, next bandwidth efficiency using compression. The authors believe that the majority of CH imagery applications will want to protect against localized *spatial* content changes such as replacement (e.g., in order to "change history"). Small bit errors due to the distribution chain or high quality compression will not be of significant security concern.

Thus, we would like our soft authentication to be forgiving of high quality compression (for example, higher than 0.5 bpp for JPEG), very small proportion (say below 1%) of random bit errors from transmission error, mild additive noise (such as salt and pepper below 1% and white Gaussian above 30 dB SNR) and mild linear filtering; these distortions collectively form Ω_R. The last two distortions are employed to model small variations in the image due to other content-preserving changes we have not considered, but may be of importance in some applications. In contrast, we would like the scheme to recognize severe compression (for example, lower than 0.5 bpp in JPEG) that impedes image quality, forgery of the entire image, addition, removal or changes in spatially localized visual features; these attacks collectively form Ω_F. Any other severe modification such as extreme filtering to impair credibility can be modeled as one of the latter distortions in Ω_F.

Keeping in mind the need for reasonable computational simplicity, we employ the 8×8 discrete cosine transform (DCT) and Haar discrete wavelet transform (DWT) as dual domains. The former helps separate relevant from irrelevant image content in localized blocks to generate salient image features and the latter has excellent spatial localization to help aid in spatial tamper characterization [4]. We believe localized spatial changes to be the most common and threatening for CH applications, so that identifying locations of change is practically useful. Furthermore, the well-known YIQ color space is used to separate the chrominance from the luminance information. Section IV demonstrates how the watermark generation in the DCT domain occurs in an orthogonal image subspace to the watermark embedding in the Haar DWT domain.

B. Watermark Generation

To generate both components of the watermark, we first transform the host color image X into the YIQ color space to obtain the luminance Y, and the chrominance images I and Q jointly representing saturation and hue. Fig. 1 summarizes the watermark generation process. The chrominance watermark is created by taking the lowest resolution bands resulting from the second level Haar DWT of both I and Q because subsampling chrominance has little visual affect on the overall color image; these bands are denoted by I_{2LL} and Q_{2LL}, respectively. Thus, the overall chrominance watermark is given by $W_c = [I_{2LL} || Q_{2LL}]$.

Generation of the authenticator watermark requires the use of a one-time only secret session key K_S known to both the sender and receiver. The repeated use of the session key is employed for protection against block analysis, traffic analysis and replay attacks [3]. In addition to K_S another key (either private or secret) is used to perform asymmetric or symmetric encryption. The choice of the encryption approach must be application-dependent.

To provide "soft-authenticator" capabilities, the algorithm we propose, detailed in both Fig. 2 and Table I, consists of several stages. The objective of the first two steps of watermark generation involving the DCT and *Feature Extraction* is to identify components in the image that are of perceptual significance. The measure we propose (that from our tests trades off saliency with computational efficiency) is the dc coefficient of the 8×8 DCT blocks of the image. Given the diversity of CH imagery, this low resolution representation provides a good metric to rep-

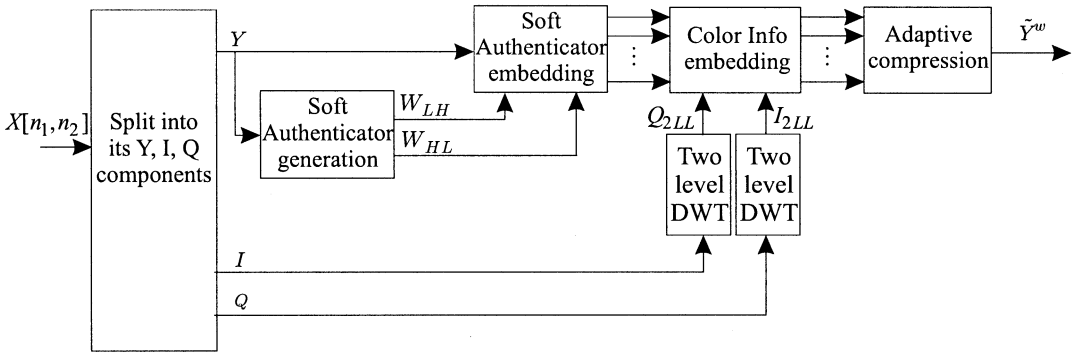

Fig. 1. Dual domain compressive data hiding and authentication watermark generation.

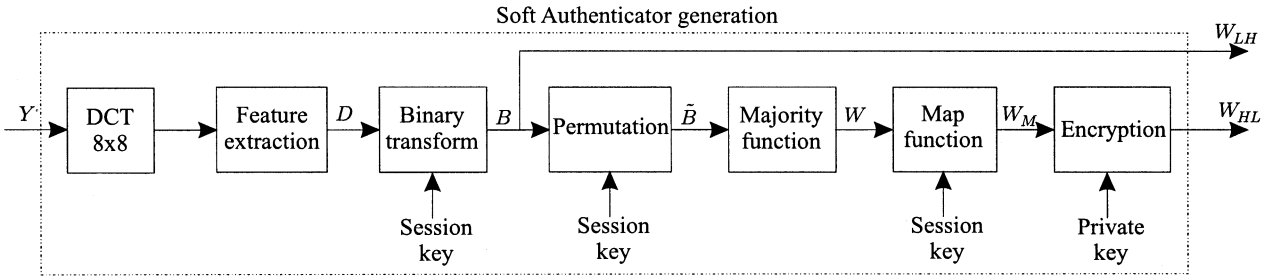

Fig. 2. Soft Authenticator watermark generation.

resent the raw spatial characteristics in the image. The *Binary Transform* stage order-pairs dc coefficients so that their relative magnitudes are guaranteed to be maintained under content-preserving operations such as JPEG or SPIHT compression. Our tests show that for JPEG quality factors higher than 70% and moderate SPIHT compression, the sign of the difference between dc values in different 8×8 blocks is preserved as long as the magnitude of their difference is above 16. The sign of the differences between the ordered pairs is coded in a binary fashion. Table I provides more details. It is worth pointing out that in presence of tampering the matrix B, which is image dependent, will change thus allowing the decoder to reveal that tampering has occurred. Furthermore, in principle B may present a small bias; this may suggest to change the detection for optimality due to the bias. Although, our experimentations have never revealed a serious bias problem, this requires further investigation. The binary output of this stage is one component of the authenticator watermark denoted W_{LH}. We believe intuitively and have verified through simulations that W_{LH} should not change value with high probability under modifications defined in Ω_R, but should change with high probability for attacks in Ω_F (see Table II). Furthermore, the location of changes in W_{LH} will point to possible 8×8 luminance image blocks that have been modified for tamper assessment capabilities.

The other authenticator component is generated by continuing to process W_{LH}. For more security against fraud or forgery a *Permutation* is applied to W_{LH}. The *Majority Function* has the goal of reducing the size of the output of the permuted binary transform while coding it to make it more robust to content preserving operations experienced by CH documents during distribution. If the output of the majority function is zero (or one), then the corresponding input row or column contains, on the average, ordered dc coefficient pairs in which the first element of the pair is greater (or lower) than the second the majority of the time. Thus, the resulting string contains compressed information about the relative local luminance activity between 8×8 DCT blocks of the image. The primary objective of the *Map Function* stage is to convert the output of the previous step to an appropriate size for encryption and subsequent watermarking. The final *Encryption* stage creates a component denoted W_{HL} which allows for sender authentication.

An approach similar to the one described in this Section for extracting the bits of the authenticator watermark was proposed in [32].

To summarize, W_{HL} provides crucial cryptographic security and W_{LH} provides attack characterization capability to balance the requirements of tamper assessment. Therefore, $W_a = [W_{LH} \| W_{HL}]$ and $W_c = [I_{2LL} \| Q_{2LL}]$, where W_{LH}, W_{HL}, I_{2LL} and Q_{2LL} are embedded in orthogonal bands of the luminance Haar DWT as discussed in Section III-C.

C. Watermark Embedding

The embedding process takes place in the Haar DWT domain which we consider a "dual" to the DCT domain used for watermark generation; Section IV provides analysis to show how the process in each domain is orthogonal. Fig. 3 presents the overall scheme. A two level Haar DWT is applied to Y and the resulting Y_{2LH} and Y_{2HL} bands are respectively embedded with W_{LH} and W_{HL} using a vector quantization-like method to produce Y^w_{2LH} and Y^w_{2HL}. A quantization based strategy is one of the most popular methods for semi-fragile watermarking because it allows for the embedding of a reasonably long payload (in comparison to spread spectrum based methods) while

TABLE I
SOFT AUTHENTICATOR WATERMARK GENERATION

1) *DCT:* Take the 8×8 block DCT of the $M_x \times M_y$ luminance component Y to produce the coefficients $f_{D_{i,j}}(u,v)$ where (i,j) for $1 \leq i \leq \lceil \frac{M_x}{8} \rceil$, $1 \leq j \leq \lceil \frac{M_y}{8} \rceil$ denotes the particular block and (u,v) for $1 \leq u,v \leq 8$ is the frequency index where $(1,1,)$ represents the dc coefficient.
2) *Feature Extraction:* Compose a matrix of dc block coefficients D as follows: $D(i,j) = f_{D_{i,j}}(1,1)$ for $1 \leq i \leq \lceil \frac{M_x}{8} \rceil$, $1 \leq j \leq \lceil \frac{M_y}{8} \rceil$.
3) *Binary Transform:* Initialize B as a matrix of zeros. Use the session key K_S to pair up every element $D(i,j)$ with another element $D(i',j')$ such that (i',j') is in a 3×3 neighborhood around (i,j). If $0 < |D(i,j) - D(i',j')| < 16$ then find another pair member as follows. Consider a line connecting (i,j) to (i',j'). Rotate this line clockwise by $\frac{\pi}{4}$ radians to find another possibility for $D(i',j')$, and repeat until a $D(i',j')$ such that $|D(i,j) - D(i',j')| \geq 16$ or $|D(i,j) - D(i',j')| = 0$ can be found. Assuming a $D(i',j')$ is found such that $|D(i,j) - D(i',j')| \geq 16$, the following relations will be preserved under JPEG compression of 70% and moderate SPIHT compression: $D(i,j) > D(i',j')$ and $D(i,j) < D(i',j')$. Thus, these features (which we use to generate the watermark) are robust to reasonable levels of compression. If a proper $D(i',j')$ cannot be found even after scanning all eight directions, leave $B(i,j)$ as initially set to zero. Note: different coefficients may have the same pair member.
   Create the $\lceil \frac{M_x}{8} \rceil \times \lceil \frac{M_y}{8} \rceil$ binary matrix B as follows:

$$B(i,j) = \begin{cases} 0 & \text{if } D(i,j) \geq D(i',j') \\ 1 & \text{otherwise} \end{cases} \tag{6}$$

   Let the first part of the $\lceil \frac{M_x}{8} \rceil \times \lceil \frac{M_y}{8} \rceil$ authenticator watermark denoted W_{LH} be equal to B.
4) *Permutation:* For security, apply an element-level permutation on B making use of K_S to form the "random" $\lceil \frac{M_x}{8} \rceil \times \lceil \frac{M_y}{8} \rceil$ matrix $\tilde{B}$.
5) *Majority Function:* Reduce the size of B by taking its "raw" characteristics to produce W as follows:

$$W(k) = \begin{cases} 1 & \text{if } \sum_{j=1}^{\lceil \frac{M_y}{8} \rceil} \tilde{B}(k,j) > \lceil \frac{M_y}{8} \rceil / 2 \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

   for $k = 1, \ldots, \lceil \frac{M_x}{8} \rceil$ and

$$W(k) = \begin{cases} 1 & \text{if } \sum_{i=1}^{\lceil \frac{M_x}{8} \rceil} \tilde{B}(i, k - \frac{M_x}{8}) > \lceil \frac{M_x}{8} \rceil / 2 \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

   for $k = \lceil \frac{M_x}{8} \rceil + 1, \ldots, \lceil \frac{M_x}{8} \rceil + \lceil \frac{M_y}{8} \rceil$
6) *Map Function:* Map the $\lceil \frac{M_x}{8} \rceil + \lceil \frac{M_y}{8} \rceil$ length sequence W to a binary matrix W_M of dimensions $\lceil \frac{M_x}{8} \rceil \times \lceil \frac{M_y}{8} \rceil$ suitable for encryption and watermark embedding by using K_S. W_M is obtained by arranging a version of the vector W, randomized according to the session key, repeatedly from row to row until the matrix W_M is filled in.
7) *Encryption:* Encrypt W_M using the appropriate key K_R to produce a binary matrix W_{HL} of the same dimension. This encryption may be assymetric or symmetric.

TABLE II
CHANGES IN THE AUTHENTICATOR WATERMARK W_{LH} DUE TO IMAGE MODIFICATIONS DEFINED IN Ω_R AND IN Ω_F EVALUATED THROUGH THE METRIC R_D DEFIND AS $R_D = \sum_{i,j}^{I,J} \hat{W}_{LH}(i,j) \oplus W_{LH}(i,j)/IJ$, BEING $\hat{W}_{LH}$ THE AUTHENTICATOR WATERMARK OF THE MODIFIED IMAGE

Modifications defined in Ω_R	R_D
"Mild compression (JPEG 70%)"	0.03
"1% random bit errors"	0.03
"1% salt and pepper noise"	0.05
"Gaussian noise (SNR=30dB)"	0.03
Modifications defined in Ω_F	R_D
"Severe compression (JPEG 10%)"	0.20
"Forgery of the entire image"	0.54
"Changes in spatially localized visual features"	0.85

having a convenient implementation structure. Semi-fragile watermarking through this approach to selected image features, provides robustness against perturbations of the features below a predefined threshold related to the quantization step size δ. Any modifications that exceed the threshold are detected.

There are two well-known types of quantization: scalar and vector. In *scalar quantization*, the quantization is applied independently to each element, usually an image coefficient in the spatial, DCT or DWT domain, among others. This allows the sharp detection of microscopic changes to locate modifications on a coefficient scale. In *vector quantization*, the quantization is applied together to groups of elements such as an image block or tile (although the effect on individual elements of the same group may vary significantly). Vector quantization tolerates a limited number of elements with higher distortion, or a larger number of elements with lower deviations. This kind of flexibility, we assert, allows for better integration of authentication watermarking with compression. For reasons of space, we do not provide a formal justification, although analytic arguments can be found in [5]. We detail our vector quantization-based technique in Table III.

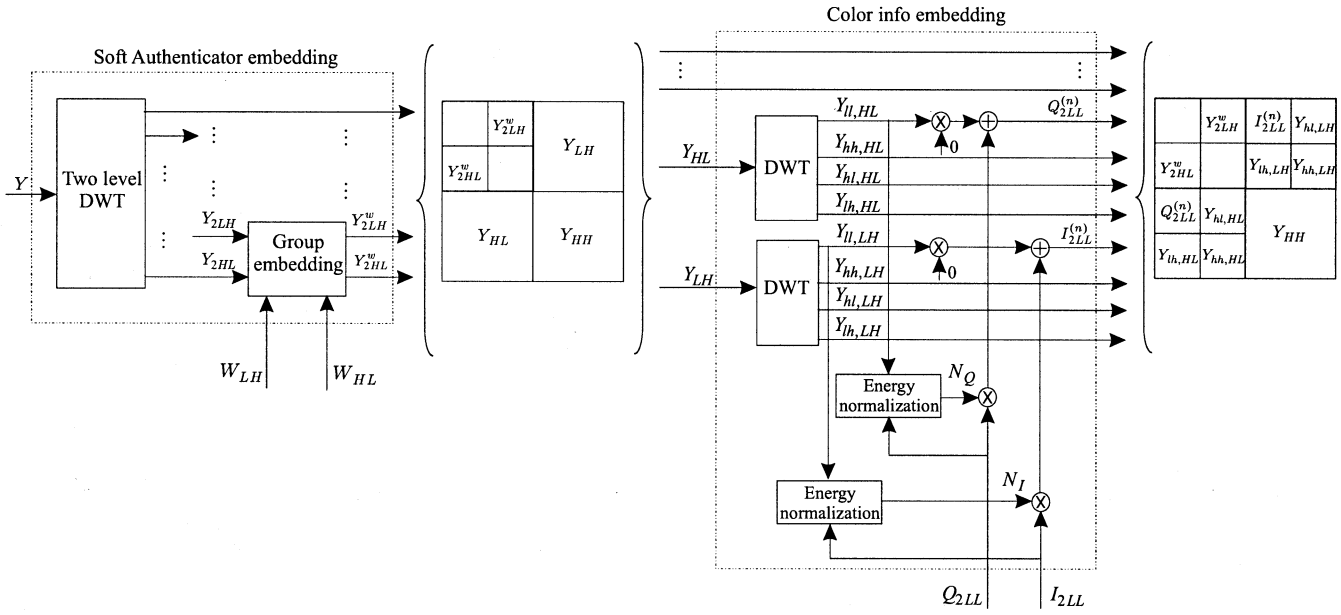

Fig. 3. Embedding of the Soft Authenticator and of the color information.

TABLE III
EMBEDDING STRATEGY

1) *Two Level Haar DWT:* Take the two level Haar DWT of Y to obtain the $\lceil \frac{M_x}{4} \rceil \times \lceil \frac{M_y}{4} \rceil$ second level LH band and HL bands denoted Y_{2LH} and Y_{2HL}, respectively, as well as the $\lceil \frac{M_x}{2} \rceil \times \lceil \frac{M_y}{2} \rceil$ first level LH and HL bands denoted Y_{LH} and Y_{HL}, respectively.
2) *Group Embedding:* Embed the binary watermarks W_{LH} and W_{HL} in Y_{2LH} and Y_{2HL}, respectively, such that every 2×2 block contains one watermark bit; the sum of the absolute element values in each 2×2 block $S_g(i,j)$ is modified to produce Y^w_{2LH} and Y^w_{2HL} as the follows:

$$S_g(i,j) = \sum_{m=1}^{2}\sum_{n=1}^{2} |Y_{2LH/HL}(n+2(i-1), m+2(j-1))| \tag{9}$$

$$q(i,j) = \lfloor \frac{S_g(i,j)}{4\delta} \rfloor \tag{10}$$

$$Y^w_{2LH/HL}(n+2(i-1), m+2(j-1)) = \begin{cases} Y_{2LH/HL}(n+2(i-1), m+2(j-1)) & \text{if } \mathrm{mod}(q(i,j),2) = W_{LH/HL}(i,j) \\ Y_{2LH/HL}(n+2(i-1), m+2(j-1)) + \mathrm{sgn}(Y_{2LH/HL}(n+2(i-1), m+2(j-1)))\delta & \text{if } \mathrm{mod}(q(i,j),2) \neq W_{LH/HL}(i,j) \end{cases} \tag{11}$$

where $n, m = 1, 2$, $\mathrm{sgn}(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ -1 & \text{if } x < 0 \end{cases}$ and δ is a user-specified quantization factor.

3) *Haar DWT:* Take a first level Haar DWT on the $\lceil \frac{M_x}{2} \rceil \times \lceil \frac{M_y}{2} \rceil$ dimensional Y_{LH} and Y_{HL} bands to produce $\lceil \frac{M_x}{4} \rceil \times \lceil \frac{M_y}{4} \rceil$ sub-bands Y_{llLH} and Y_{llHL} as shown in Fig. 3.
4) *Chrominance Embedding:* Normalize the energies of I_{2LL} and Q_{2LL} to the values of the corresponding host sub-bands, Y_{llLH} and Y_{llHL}, as not to impair the perceptual appearance of the reconstructed image, and replace Y_{llLH} and Y_{llHL} with the normalized I_{2LL} and Q_{2LL} (Please note as discussed in more detail in [6], the normalization values have to be transmitted to the decoder by some other means since they are necessary to properly reconstruct the color information).
5) *Image Recomposition:* Recompose the image by taking the appropriate inverse discrete wavelet transforms (IDWTs) to produce the watermarked spatial domain luminance image Y^w.

The subsampled chrominance components, I_{2LL} and Q_{2LL}, are embedded by simply replacing the specific Haar domain LL bands of Y_{LH} and Y_{HL}, respectively[5], thus obtaining Y^e_{LH} and Y^e_{HL}. The rationale behind this choice relies on the observation that, in order to obtain a good trade-off between robustness and transparency, many watermarking techniques (e.g., see [28] and references therein) use "middle frequency" coefficients which makes subbands Y_{LH} and Y_{HL} (and not Y_{HH}) intuitively suitable for embedding.

For CH imaging applications, perceptual transparency is one of the highest priorities. The watermark embedding method,

[5] I_{2LL} and Q_{2LL} are high volume so standard quantization- or spread spectrum- based embedding are not suitable. Simple band replacement is found to be a good solution [6].

TABLE IV
PSNR (DB) VALUES AND WATSON'S DISTORTION METRIC OF THE LUMINANCE COMPONENT (Y) FOR EMBEDDING WITH THE AUTHENTICATOR WATERMARK, THE CHROMINANCE WATERMARK, AND BOTH

	PSNR			Watson's metric		
Image	auth	IQ	auth + IQ	auth	IQ	auth + IQ
"Terrace"	44.2	38.8	37.7	0.02	0.03	0.05
"Cover"	44.1	34.9	34.4	0.02	0.05	0.06
"Horse"	44.5	36.5	35.8	0.02	0.04	0.05

performed as detailed in Table III, has been tested to be perceptual transparent by using both a subjective evaluation criteria such as human visual perceptibility measures and objective metrics like Peak Signal to Noise Ratio (PSNR), given by

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \text{ [dB]} \tag{12}$$

where

$$MSE = \frac{1}{M_x M_y}\sum_{i=1}^{M_x}\sum_{j=1}^{M_y}(Y(i,j) - Y^w(i,j))^2 \tag{13}$$

is the mean square error between the $M_x \times M_y$ host image Y and the watermarked result Y^w where (i,j) denotes the specific pixel value. To characterize the perceptual distortion from watermark embedding, we consider two different metrics: the PSNR and the Watson's distortion metric [34]. Specifically they are evaluated between the host and the watermarked image containing only the authenticator (i.e., the chrominance information is not embedded) denoted by "auth", between the host and the watermarked image containing only the chrominance information (i.e., authenticator is not embedded) denoted by "IQ", and between the host and watermarked image containing both the authenticator and chrominance data denoted by "auth + IQ". Results are presented in Table IV. The obtained values for both the PSNR and the Watson's metric indicate that there is no perceptual change in the quality of the watermarked images for each test case.

D. Adaptive Compression

The final secured and compressed image ready for distribution is produced by applying a lossy coding algorithm f_l to the overall watermarked image. To preserve the authenticator and chrominance information, we employ an adaptive compression scheme that makes use of the method of set partitioning in hierarchical tree (SPIHT) [29] and takes into account the diverse nature of the luminance signal component within the different subbands

$$\{Y^e_{LH}, Y^e_{HL}, Y_{HH}, Y_{2LL}, Y^w_{2LH}, Y^w_{2HL}, Y_{2HH}\} \tag{14}$$

where Y^w_{LL} is the LL subband containing the authenticator watermark that is reconstructed using a first level Haar IDWT applied to Y_{2LL}, Y^w_{2LH}, Y^w_{2HL}, Y_{2HH}.

Each subband of (14) is separately coded as demonstrated in Fig. 4. A wavelet-based coder is used instead of a DCT-based mechanism to provide better rate-distortion performance and to allow a progressive coding approach [30]. It is well known

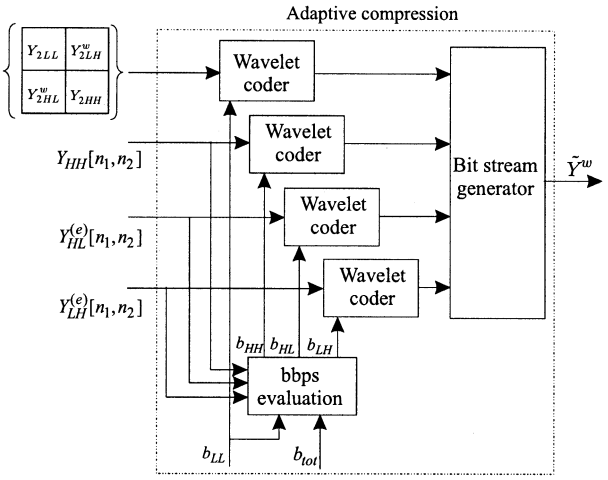

Fig. 4. Adaptive compression scheme.

that the magnitude of the wavelet coefficients varies from band to band; in particular, lower frequency subbands usually have a larger magnitudes than their higher frequency counterparts, which suggests that the compressed bit rate must be suited to each specific subband. Let us consider

$$\{b_{LL}, b_{HH}, b_{HL}, b_{LH}\} \tag{15}$$

which represent the bit per pixel (bpp) values for each of the subbands of the first level wavelet decomposition we perform. Moreover, let b_{tot} be the desired bpp for the overall compressed color image, which is related to the bpps in (15) as follows:

$$b_{tot} = b_{LL} + b_{HH} + b_{HL} + b_{LH}. \tag{16}$$

The proposed criterion for adaptive compression consists of specifying the global bit rate b_{tot} and the bit rate b_{LL} for the Y^w_{LL} subband. The bit rate b_{LL} has to be carefully set as it plays the most significant role in the decoded image appearance and authentication success. Furthermore, it represents the global bpp allowable for the Y^w_{LL} subband which contains the authenticator. Low values of b_{LL} can impair the appearance of the decoded image and the authentication capabilities of the proposed approach. The remaining bpps b_{HH}, b_{HL}, b_{LH} are automatically assigned by the coder in such a way that a higher bit rate is assured to the subbands having higher energy. Specifically

$$b_{LH} = \frac{\mathcal{E}_{LH}}{\mathcal{E}_{HH}} \cdot b_{HH} \tag{17}$$

$$b_{HL} = \frac{\mathcal{E}_{HL}}{\mathcal{E}_{HH}} \cdot b_{HH} \tag{18}$$

where $\mathcal{E}_\gamma$ $(\gamma \in (LH, HL, HH))$ represent the energies of the different subbands. After having chosen b_{tot} and b_{LL}, according to the user's needs, the bit rates for each subband are obtained from (16)–(18).

Once the values of the bpps in (15) have been set, an analogous approach is employed to obtain the bpps employed to code the second level subbands Y_{2LL}, Y^w_{2LH}, Y^w_{2HL}, Y_{2HH}. The values employed for our simulations are reported in Section V.

TABLE V
WATERMARK EXTRACTION

1) *Two level Haar DWT:* Take the two level Haar DWT transform on the received $M_x \times M_y$ luminance Y^r to obtain the second level bands Y^r_{2LH} and Y^r_{2HL}; and the first level bands Y^r_{LH} and Y^r_{HL}.
2) *Group Extraction:* Extract each watermark bit from every 2×2 block of Y^r_{2LH} and Y^r_{2HL}. W^e_{LH} and W^e_{HL} are extracted from Y^r_{2LH} and Y^r_{2HL}, respectively, as follows:

$$\begin{aligned} S_g(i,j) &= \sum_{m=1}^{2}\sum_{n=1}^{2} |Y_{2LH/HL}(n+2(i-1), m+2(j-1))| \\ q(i,j) &= \lfloor \frac{S_g(i,j)}{4\delta} \rfloor \\ W^e_{LH/HL}(i,j) &= \begin{cases} 0 & \text{if } mod(q(i,j),2) = 0 \\ 1 & \text{if } mod(q(i,j),2) = 1 \end{cases} \end{aligned} \tag{19}$$

3) *Decryption:* Use the public key of the sender K_U to decrypt W^e_{HL} to obtain W^d_{HL}.
4) *Haar DWT:* Take a first level Haar DWT on the bands Y^r_{LH} and Y^r_{HL} to obtain Y^r_{llLH} and Y^r_{llHL} which contain the chrominance information.

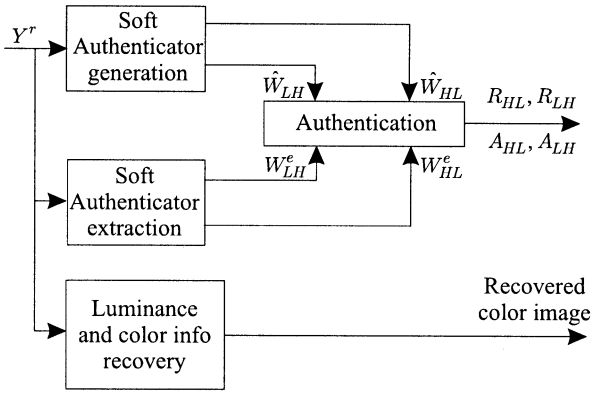

Fig. 5. Watermark extraction.

E. Watermark Extraction, Authentication, and Color Recovery

At the receiver, the image authentication and color recovery are performed. The receiver is assumed to have κ' which includes the associated session key K_S and decryption key to match K_R at the sender. If asymmetric or symmetric cryptography is used then, the receiver must possess the appropriate public key K_U or secret key K_R, respectively. In Fig. 5, the whole procedure at the receving side is summarized. The first step of authentication involves watermark extraction detailed in Table V. The authentication watermark is extracted from the Y^r_{2LH} and Y^r_{2HL} bands of Y^r. The actual extraction procedure is given by (19) in which the magnitude of the sum of the coefficients of each 2×2 block in Y^r_{2LH} and Y^r_{2HL} is effectively placed in an appropriate "bin" to estimate the watermark bit embedded. Sums in even indexed bins decode to a zero and sums in odd numbered bins decode to a one. The extracted watermarks from Y^r_{2LH} and Y^r_{2HL} are denoted W^e_{LH} and W^e_{HL}, respectively. These marks must be effectively compared to a corresponding set generated from Y^r for authentication and tamper assessment. This comparison process differs if symmetric or asymmetric encryption is employed as discussed in Sections III-E1 and 2.

1) Asymmetric Authentication: Watermarks denoted $\hat{W}_{LH}$ and $\hat{W}_M$ are generated from Y^r in the same fashion as W_{LH} and W_{HL}, respectively, were from Y in Section III-B except for $\hat{W}_M$ the final stage of *Encryption* in Fig. 2 is not applied, so we essentially obtain an estimate of W_M; that is, only Steps 1 to 6 of Table I are applied to Y^r to generate $\hat{W}_M$. There are two stages to the comparison process: authentication, verification, and tamper assessment. For the first, W^e_{HL} is decrypted with K_U to produce W^d_{HL}. If $W^d_{HL} = \hat{W}_M$ (for every bit) then the image is authenticated successfully. Tamper assessment attempts to determine some characteristics of the distortions applied to the image and is especially useful if authentication fails, but an application-based decision needs to be made about the parts of the image that may be credible.

The overall characterization process is conducted by computing *authentication matrices* A_{LH} and A_{HL} defined as follows:

$$A_{LH}(i,j) = \hat{W}_{LH}(i,j) \oplus W^e_{LH}(i,j) \tag{20}$$
$$A_{HL}(i,j) = \hat{W}_M(i,j) \oplus W^d_{HL}(i,j) \tag{21}$$

where $\oplus$ is the exclusive OR binary operator and $1 \le i \le \lceil M_x/8 \rceil$, $1 \le j \le \lceil M_y/8 \rceil$. Visual inspection of the $A_{LH}(i,j)$ and $A_{HL}(i,j)$ can provide some information on the localization of tampering as discussed in Section V.

To further assess tampering, we introduce the notions of a credible, processed and fabricated image. A *credible* image is defined as one in which the essential content is intact (e.g., through perceptual coding). This definition is application-specific since in some situations a different degree of content change may be acceptable. An image is *processed* if the distortions result in extracted watermarks that do not exactly match the generated. This can occur for both small and severe levels of tampering. An image is considered *fabricated* if the entire content of the image is not credible; replacing the original image with a completely new signal or even distorting the original to a severe extent will fall under this class.

Quantitatively, we propose the use of an authentication statistic $R_a = [R_{LH} \| R_{HL}]$ where the error rates R_{LH} and R_{HL} are defined as

$$R_{LH} = \frac{\sum_{i=1}^{\lceil M_x/8 \rceil} \sum_{j=1}^{\lceil M_y/8 \rceil} A_{LH}(i,j)}{\lceil \frac{M_x}{8} \rceil \cdot \lceil \frac{M_y}{8} \rceil} \tag{22}$$

$$R_{HL} = \frac{\sum_{i=1}^{\lceil M_x/8 \rceil} \sum_{j=1}^{\lceil M_y/8 \rceil} A_{HL}(i,j)}{\lceil \frac{M_x}{8} \rceil \cdot \lceil \frac{M_y}{8} \rceil}. \tag{23}$$

Using a user specified decision threshold $0 < \tau < 0.5$, a tamper categorization on the received image is made as follows (please note that Level 3 is a composite classification distinguishing the level of content change):

Level 1: $R_{LH} = R_{HL} = 0$: image content is credible and no modifications have been made; authentication of the sender is verified.

Level 2: $R_{LH}, R_{HL} < \tau$ image content is credible, but the image has been processed.

Level 3:

a) $R_{LH} < \tau$ and $R_{HL} > \tau$ some image content is not credible; R_{LH} can be used to characterize tampering.

b) R_{LH}, $R_{HL} > \tau$ image content is not credible and moreover the image is entirely fabricated.

c) $R_{LH} > \tau$ and $R_{HL} < \tau$ image content is not credible and moreover the image is entirely fabricated.

A classification of Level 1 corresponds to the situation that negligible modification of the image has taken place, and the content is completely intact. The fact that $R_{HL} = R_{LH} = 0$ supports this conclusion. The authentication watermark generated from the DCT domain exactly matches the extracted watermark from the DWT domain. Furthermore, sender authentication is possible because the successful decryption using K_U verifies the sender's correct identity. This is possible with high probability only if the correct watermarks have been generated and extracted and hence no significant tampering of the image has taken place.

Level 2 and 3 consider cases in which the extracted and generated authentication watermark do not match exactly due to processing on the image. The inconsistency can be due to errors in the authentication watermark extraction and/or generation processes. Errors in W^e_{LH} or W^e_{HL} detect image tampering as reflected by the embedding process. The location of errors provide spatial information on the modification regions. Given that both W^e_{LH} and W^e_{HL} are in the same image resolution, we expect that their average errors due to spatial tampering will be the same and in the same regions. Errors in the decrypted version of W^d_{HL} are only possible if there is one or more errors in W^e_{HL} or the public key K_U used for decryption does not match that of the private key. In both cases, there will be with high probability 50% error in the decrypted watermark because of the nonlinear nature of the cryptographic processing. An error in generation of $\hat{W}_{LH}$ from the received image implies that the content (as reflected by the DCT domain watermark generation of Fig. 2) is modified. Similarly, errors in $\hat{W}_M$ detects modifications in content, but due to the *Majority Function* this quantity is more robust to changes than $\hat{W}_{LH}$. Thus, it can exhibit fewer errors than $\hat{W}_{LH}$ when there are minor levels of tampering.

Because our methodology is blind, the receiver does not have access to W_{LH} and W_{HL} to assess errors, so as discussed in relation to R_{LH} and R_{HL}, a comparison is conducted between $\hat{W}_{LH}$ and W^e_{LH}, as well as $\hat{W}_M$ and W^d_{HL}. The case that $R_{LH} < \tau$ implies that small content changes have taken place affecting either or both the corresponding embedding and generation processes. Since the differences are minor, R_{LH} is useful to deduce location of tampering. When $R_{LH} > \tau$, our system indicates a major content change. It is most likely that both the watermark generation and extraction have resulted in errors. This implies that the entire content is not credible which we consider a fabrication attempt. $R_{HL} < \tau$ is a result of small errors in $\hat{W}_M$. Thus, the locations of tampering are reflected in R_{HL}. It is highly improbable that the mismatch reflected in R_{HL} is a result of errors in W^d_{HL} which is the result of a decryption and, therefore, any (even a single) bit error in W^e_{HL} will completely scramble W^d_{HL} from its true value. Thus, if the error were due to errors in W^d_{HL} instead of just $\hat{W}_M$, one would expect $R_{HL} \approx 0.5 > \tau$ with high probability. Finally the case of $R_{HL} > \tau$ may reflect a content change that has propagated to W^e_{HL} (which may not be major, but will result in a scrambled W^d_{HL}) and/or $\hat{W}_{HL}$. The high errors in any case will result in a large value for R_{HL}. Another possibility is that the sender is illegitimate. Thus, by only observing R_{HL} we may conclude whether there is a content change (the degree of which is unknown) or the sender is illegitimate.

Using the entire authentication statistic $R_a = [R_{LH} \| R_{HL}]$ we may combine the arguments presented and come to the conclusions presented for the Level 1, 2, and 3 categories above. The reader should note that the Level 3c case of $R_{LH} > \tau$ and $R_{HL} < \tau$ is highly improbable (it never happened in the performed simulations); it has contradictory meaning that the image content has not been modified, but the content is not credible which we credit to a statistical fluke in cases there is a great deal of tampering. Therefore, the image is categorized as being fabricated. In addition, the algorithm has been designed such that high quality compression will result in a small affect on the authentication process, so it can be classified as Level 2. Moderate or severe compression will render the image classified at Level 3. If more robustness to compression is required, we propose the use of message digests using symmetric encryption instead of digital signatures as discussed in Section III-E2.

2) Symmetric Authentication: In this approach, watermarks denoted $\hat{W}_{LH}$ and $\hat{W}_{HL}$ are generated from Y^r exactly as W_{LH} and W_{HL}, respectively, are from Y in Section III-B. This is possible because the secret key K_R is known at the receiver. The overall characterization process is conducted by computing the following authentication matrices A_{LH} and A_{HL} given by

$$A_{LH}(i,j) = \hat{W}_{LH}(i,j) \oplus W^e_{LH}(i,j) \tag{24}$$

$$A_{HL}(i,j) = \hat{W}_{HL}(i,j) \oplus W^e_{HL}(i,j) \tag{25}$$

where $\oplus$ is the exclusive OR binary operator and $1 \le i \le \lceil M_x/8 \rceil$, $1 \le j \le \lceil M_y/8 \rceil$. The only difference from our

asymmetric method is that, here, the A_{HL} matrix is based on comparing the extracted message digest from the generated one instead of employing decrypted versions of the digital signature.

Using the same definitions for credible, processed and fabricated image, the authentication statistic $R_a = [R_{LH} \| R_{HL}]$ [where R_{LH} and R_{HL} are given in (22) and (23)], can be used to classify the received image as follows:

Level 1: $R_{LH} = R_{HL} = 0$ image content is credible and no modifications have been made; authentication of the sender is verified.
Level 2: $R_{LH}, R_{HL} < \tau$ image content is credible, but the image has been processed.
Level 3:

a) $R_{LH} < \tau$ and $R_{HL} > \tau$ image is not credible. R_{LH} can be used to characterize tampering; the sender is not legitimate;
b) R_{LH}, $R_{HL} > \tau$ image content is not credible and moreover the image is entirely fabricated;
c) $R_{LH} > \tau$ and $R_{HL} < \tau$ image content is not credible and moreover the image is entirely fabricated;

where, once again, a user-defined threshold $0 < \tau < 0.5$ is used. For authentication using message digests, unless the sender is not legitimate, $R_{LH} \approx R_{HL}$ with high probability; in fact, because $\hat{W}_{HL}$ is more robust to change than $\hat{W}_{LH}$ by design we would expect $R_{HL} < R_{LH}$ which is verified in simulations. For the asymmetric case, this was not true.

Therefore, some of the classifications have slightly different meanings; the reader should especially note the difference for Level 3a above from symmetric authentication. Level 1, 3b, and 3c classifications all have the same meaning as for the asymmetric case. Due to the lower sensitivity of R_{HL} (minor errors in W^e_{HL} do not result in $R_{HL} \approx 0.5$ as in the asymmetric case), Level 2 classification is possible for a larger class of distortions for the same value of τ. For Level 3a, because we expect with high probability that $R_{LH} < R_{HL}$ if the secret keys at the sender and the receiver are matched, we expect that $R_{HL} > \tau$ is an indication that the sender may not be legitimate (i.e., the sender did not use the correct secret key K_R).

The implication of these new classifications to our problem of compression and classification of CH imagery, is that the authentication scheme is robust to a higher level of compression than for the asymmetric case while still providing authentication. Thus, greater compression efficiencies are possible. The difference is that a message digest opposed to a digital signature is used. Both symmetric and asymmetric authentication approaches can be appropriately tuned for a given application through the proper selection of τ as discussed in Section III-E3.

3) Threshold: The threshold $\tau < 0.5$ controls distinction between Level 2 (processed, but credible image) and Level 3 (not credible) image classification; that is, selection of τ provides a user-defined opportunity to tune the classification process for a given application. The assignment for τ must be based on an application-specific definition of image credibility. The specific end-use of CH based imagery will decide this value. For example, for historical academic purposes in which conclusions are formed based on image data, it is essential that the content be exactly intact. The smallest artefact can change our perception of history. Therefore, $\tau \ll 1$. In contrast, if the imagery is to be used for educational purposes, such as a grade school classroom, then only severe changes may need to be detected and even $\tau \leq 0.45$ may be acceptable. Although a threshold of 0.45, which is used in our simulations of Section V, may seem high, we have tested the algorithm for ten fabricated images (ones in which no watermark is embedded) and have found that $0.49 < R_{LH}, R_{HL} < 0.52$, so that even $\tau = 0.45$ will with high probability be able to detect content change appropriately.

4) Color Recovery: Finally, the chrominance information from the Y^r_{llLH} and Y^r_{llHL} bands of Y^r (as discussed in Table V) is used to reconstruct the color image. Color recovery is straightforward and involves renormalizing the chrominance watermarks and combining them using the YIQ color space. Some color inaccuracies can occur in the reconstruction of the chrominance components whether the compression they undergo is too severe. However, since their compression factors are decided by the operator, the color inaccurancies can be easly avoided. As discussed in [6], the normalization values required have to be transmitted to the decoder by some other means since they are necessary to properly reconstruct the color information. They can be encrypted and transmitted to the receiver on a separate channel. As a different solution, they can be transmitted by robustly watermarking them in some parts of the image (which we do not address in this paper), or as part of an image-dependent key on behalf of a family of images with similar color characteristics.

IV. Dual Domains for Orthogonality

To analyze the theoretical feasibility of pairing the DCT-DWT domains, we characterize the Haar DWT watermark embedding process and predict its effect on the DCT watermark generation. We, specifically, demonstrate how watermark embedding in the Haar DWT domain does not interfere with watermark generation in the DCT domain, so that the authenticator generated from the original host image is the same as the authenticator from the watermarked image.

We consider the Haar DWT decomposition and let $Y(i,j)$ be the (i,j)th pixel of the luminance Y where $1 \leq i \leq M_x, 1 \leq j \leq M_y$. The two dimensional first level Haar DWT coefficients of the bands $Y_{LL}, Y_{LH}, Y_{HH}, Y_{HL}$ can be expressed as [31]

$$\begin{bmatrix} Y_{LL}(i,j) & Y_{LH}(i,j) \\ Y_{HL}(i,j) & Y_{HH}(i,j) \end{bmatrix} = \frac{1}{2}\Bigg(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} Y(2i-1, 2j-1) + \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \times Y(2i-1, 2j) + \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} Y(2i, 2j-1) + \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} Y(2i, 2j) \Bigg). \tag{26}$$

TABLE VI
COMPARISONS OF THE AUTHENTICATION CAPABILITIES OF THE PROPOSED COMBINED AUTHENTICATION-COMPRESSION METHOD

Algorithms	Sub attack	Signal processing attacks P_f %					
	P_m %	No attack	Hist.Equal.	Salt&Pepper	Gaussian	JPEG 70%	Low-pass Filtering
1	3.2	0.0	23	1	2.5	3.4	15
2	1.0	1.1	31	19.5	1.1	6.7	58
3	0.0	0.0	45	80	75	7.2	58
4	0.8	0.0	47	0.3	12	45	53
dual domain	0.1	0.0	20	0.7	2.5	0.8	34

Similarly, the two-dimensional second level Haar DWT coefficients of the bands $Y_{2LL}, Y_{2LH}, Y_{2HH}, Y_{2HL}$ are given by [31]

$$\begin{aligned}\begin{bmatrix} Y_{2LL}(i,j) & Y_{2LH}(i,j) \\ Y_{2HL}(i,j) & Y_{2HH}(i,j) \end{bmatrix} = \frac{1}{2}\Bigg(& \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \\ & \times Y_{LL}(2i-1, 2j-1) \\ & + \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \\ & \times Y_{LL}(2i-1, 2j) \\ & + \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \\ & \times Y_{LL}(2i, 2j-1) \\ & + \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \\ & \times Y_{LL}(2i, 2j) \Bigg).\end{aligned} \tag{27}$$

It is also well known that the 8×8 block dc coefficients of the original host luminance Y can be expressed as

$$\begin{aligned} f_{D_{k,l}}(1,1) &= \frac{1}{64} \sum_{u=1}^{8} \sum_{v=1}^{8} Y_{k,l}(u,v) \\ &= \frac{1}{64} \sum_{u=1}^{8} \sum_{v=1}^{8} Y(8(k-1)+u, 8(l-1)+v) \end{aligned} \tag{28}$$

where $Y_{k,l}$ is the (k,l)th 8×8 block of the original host luminance image where $1 \leq k \leq \lceil M_x/8 \rceil$, $1 \leq l \leq \lceil M_y/8 \rceil$, and $f_{D_{k,l}}(1,1)$ the corresponding dc coefficient.

From (26) and (27), it is possible to show that the Y_{2LL} band of the Haar DWT domain is actually the scaled sum of pixels in a corresponding 4×4 image block. That is

$$Y_{2LL}(i,j) = \frac{1}{4} \sum_{u=1}^{4} \sum_{v=1}^{4} Y(4(i-1)+u, 4(j-1)+v). \tag{29}$$

From the relationship between (28) and (29), it can be seen that the 8×8 DCT domain dc coefficients are collectively a subspace of the Y_{2LL} band. Since the Y_{2LL} band is orthogonal to the Y_{2HL}, Y_{2LH}, Y_{llHL}, and Y_{llLH} bands of the Haar DWT, any changes to these bands is guaranteed not to affect Y_{2LL} and its subspaces including the DCT dc coefficient domain.

Therefore, embedding authenticator and chrominance information in Y_{2HL} and Y_{2LH}, Y_{llHL}, and Y_{llLH} bands of DWT domain does not affect the 8×8 DCT dc domain. Since the watermark generation is only based on these latter image features, we conclude that authenticator embedding will not affect authenticator generation.

TABLE VII
CONFUSION MATRIX INDICATING THE ERROR RATE BETWEEN ALL THE THREE LEVELS CONSIDERED BY THE PROPOSED SYSTEM

	Attack	Level 1	Level 2	Level 3
Level 1	No Attack	100	0	0
Level 2	Hist. Equal.	0	80	20
	1% Salt & Pepper noise	0	99	1
	Gaussian noise (SNR=30dB)	0	97	3
	Mild compression (JPEG 70%)	0	99	1
	Low-pass Filtering	0	66	34
Level 3	Sub-attacks	0	23	77

V. SIMULATIONS

In this section, the effectiveness of the proposed method is investigated by comparing its performance to existing techniques and demonstrating the fundamental tradeoffs between security and compression efficiency. Three types of tests are conducted. Since, to the best of the authors' knowledge, no other joint authentication and color compression scheme exists for still imagery, the first two experiments involve comparison with well known semi-fragile image authentication watermarking, and color image compression schemes, respectively. These tests are administered individually to assess the performance of each component of our method. Our last set of simulations, however, demonstrate the trade-offs of integrating both authentication with compression. CH artwork images acquired from an ancient book *"Le Livre des Mille Nuits et une Nuit"* are used to assess the performance of the proposed combined authentication-compression method.

A. Soft Authentication

The performance of the proposed approach, in terms of authentication capabilities, is tested in comparison to the following popular algorithms:

1) "Combined Watermarking for Image Authentication and Protection" [26].
2) "Invertible Authentication Watermark for JPEG Images" [11].
3) "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation" [32].
4) "A Class of Authentication Digital Watermarks for Secure Multimedia Communication" [14].

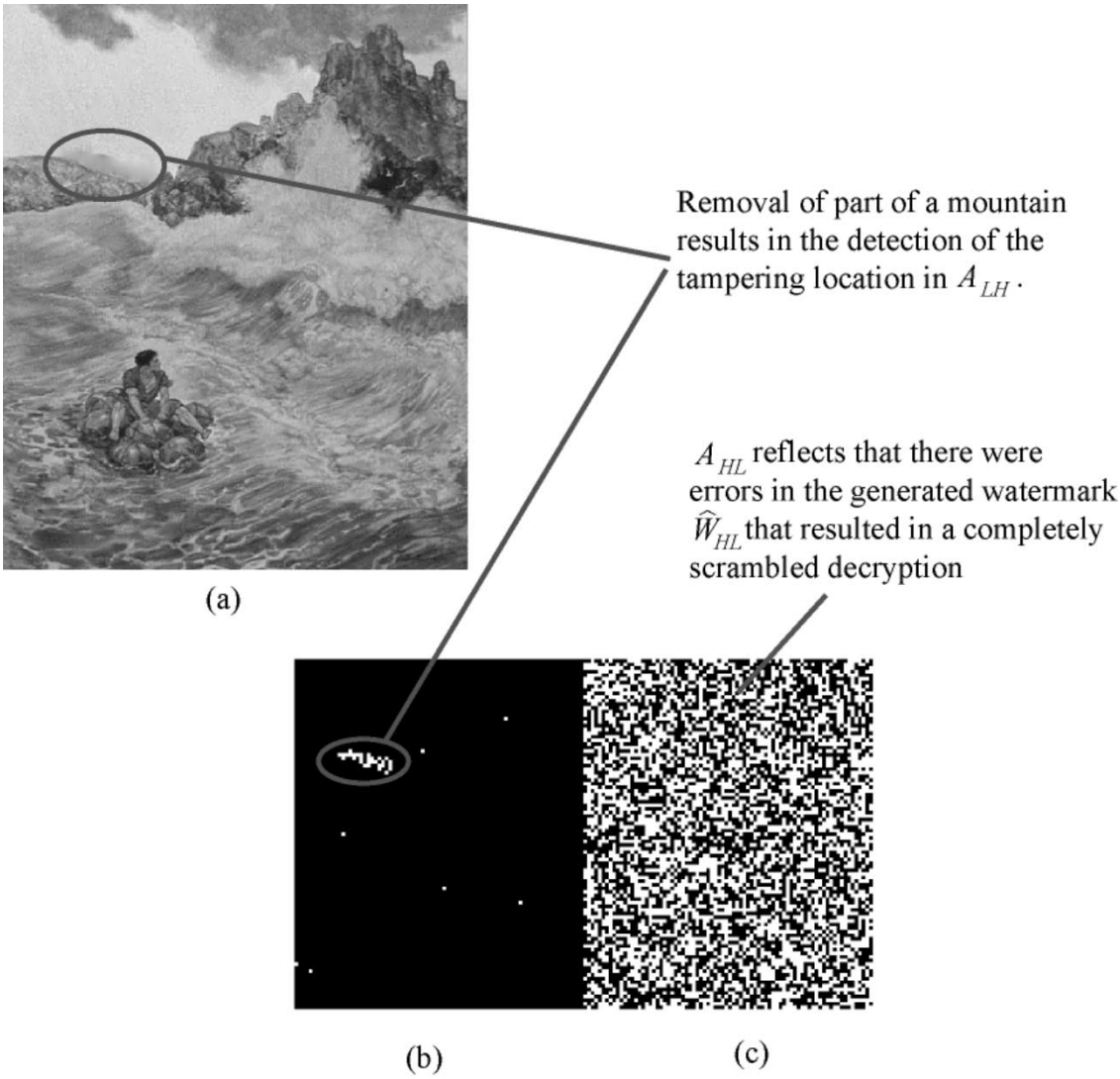

Fig. 6. Tamper detection for the asymmetric approach of dual domain authentication. (a) The original image (not shown) has been modified by removing a part of the mountain as shown, (b) the authentication matrix A_{LH} identifies the location of the localized tampering, and (c) the authentication matrix A_{HL} is completely scrambled indicating that authentication is not possible.

These methods have been selected for their influence in the area of semi-fragile watermarking and compatibility for comparison to our proposed approach.

To assess the authentication performance, two figure of merit are used: the missed detection rate P_m, and the false alarm rate P_f; these standard measures are used to assess baseline performance of authentication watermarking schemes [33]. The first measure, P_m is defined as the likelihood that a malicious attack (from Ω_F) is not detected by the given scheme. In our proposed approach this means that a tampered image is falsely classified as Level 1 or 2 (when it should really be Level 3). Similarly, P_f is the likelihood that a scheme gives in incorrect indication of malicious tampering in the absence of a malicious attack. In the proposed scheme, it refers to an erroneous Level 3 classification when there is no distortion or the modification is from Ω_R.

The error rates are computed over ten different test images each watermarked ten times using different session keys K_S (that affect Steps 3, 4 and 6 of the watermark generation algorithm of Table I); this means that different projective line strategies (for Step 3), permutations (for Step 4), and mapping functions (for Step 6) of Table I are employed to obtain an average feel for our approach. The symmetric authentication approach was implemented for these tests. The quantization factor is set to $\delta = 12$ which results in a PSNR of 38 dB.

The attacks for which the error rates are computed include those from Ω_R and Ω_F. All tests were conducted using MATLAB. Specifically, the content-preserving manipulations are well known attacks and include mild compression which we define as JPEG compression at 70% quality factor (which corresponds to a bit rate of 0.5 bpp), additive white Gaussian noise ($\mathrm{SNR} = 30$ dB), 3×3 Weiner filtering (using the function `weiner2` in MATLAB), additive salt and pepper noise (at 1%). In addition, we also tested the approach on histogram equalization (using the function `histeq` in MATLAB) which is an attack addressed to a fairly large extent in the semi-fragile watermarking research community [33]. The histogram attack can result in visual degradation of CH imagery and because it is not included in Ω_R or Ω_F of our formulation, it is presented here only for completeness and comparison to the tests in [33]. Although we also do not consider the modification of scaling in

Fig. 7. Terrace image. From top left, clockwise sense: original color image (24 bpp), authenticated-compressed image (0.2 bpp), JPEG2000 compressed image (0.2 bpp), SPIHT compressed image (0.2 bpp).

either Ω_R or Ω_F, we have tested our proposed scheme on this attack to gain a feel for the performance. For authentication, the received image must be resized to its original dimensions before watermark extraction since the watermark is embedded in synchronized 8×8 DCT blocks. Our tests for a number of different images have found that mild scaling, in which the

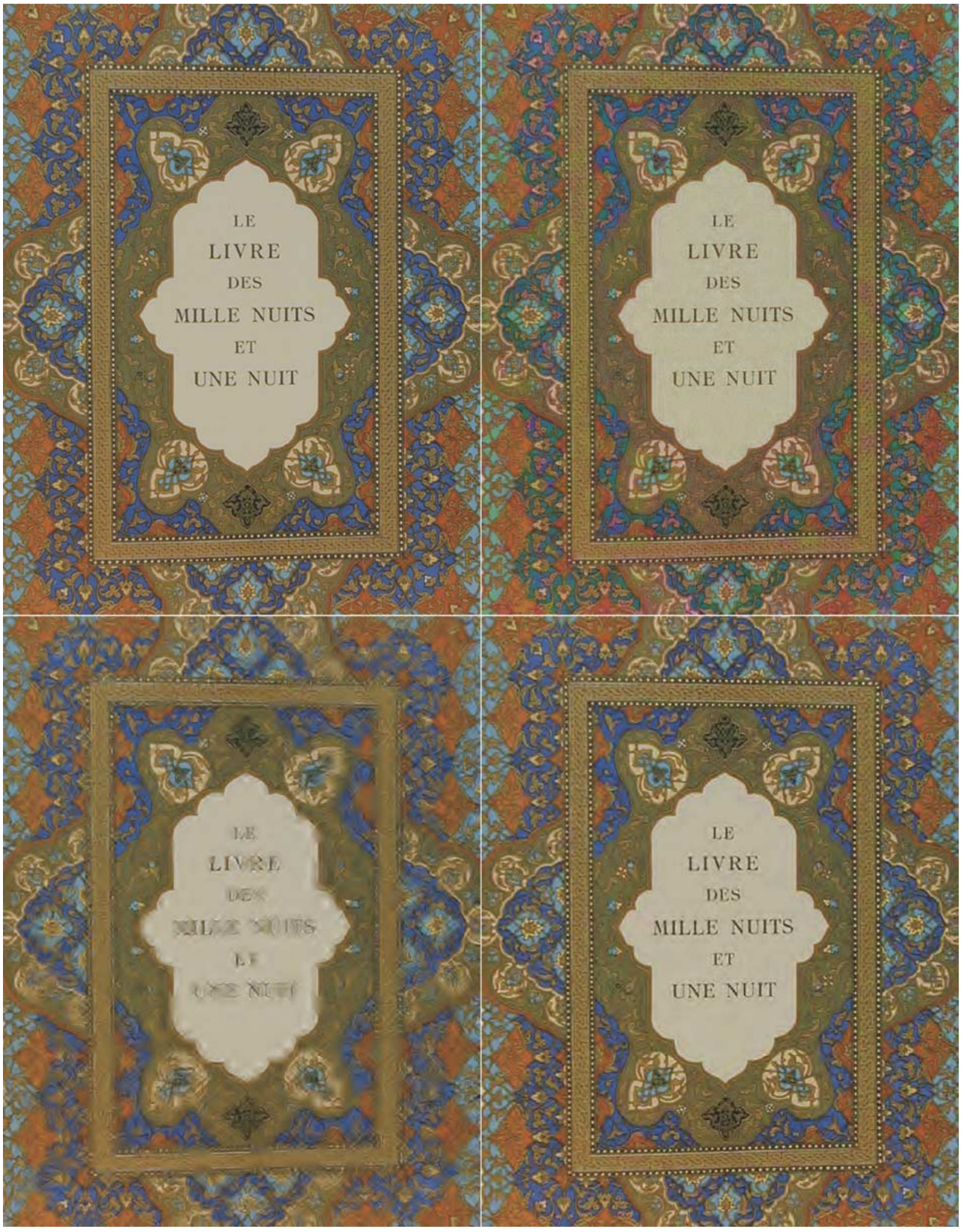

Fig. 8. Cover image. From top left, clockwise sense: original color image (24 bpp), authenticated-compressed image (0.3 bpp), JPEG2000 compressed image (0.3 bpp), SPIHT compressed image (0.3 bpp).

dimensions are both scaled down by a factor of two, results in $R_{LH} \leq 0.3$. Heavier scaling that results in more severe loss of details naturally gives $R_{LH} \approx 0.5$.

The results for malicious modifications involving sophisticated content substitution are also presented. The substitution attack [33] replaces a watermarked image portion with its orig-

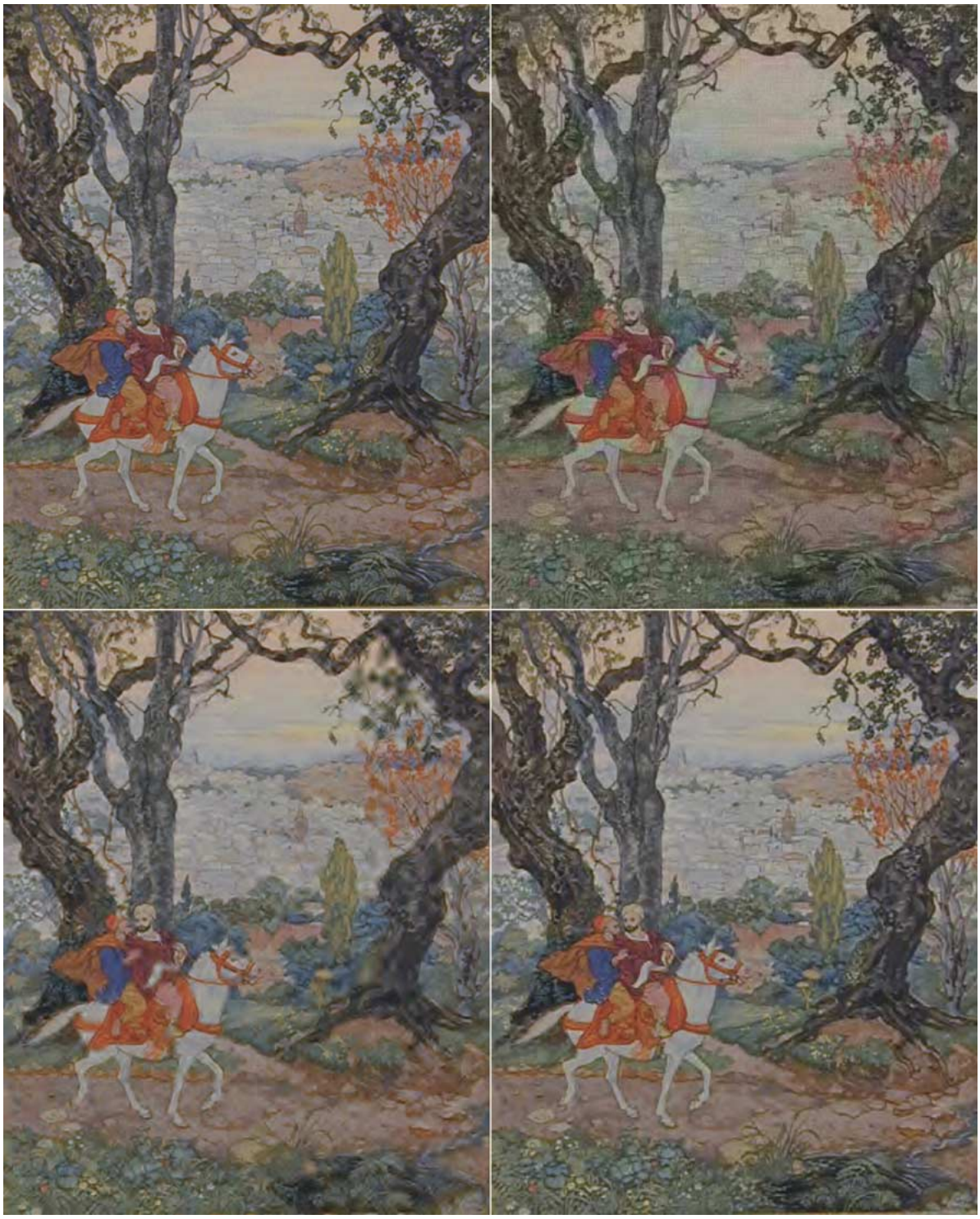

Fig. 9. Horse image. From top left, clockwise sense: original color image (24 bpp), authenticated-compressed image (0.4 bpp), JPEG2000 compressed image (0.4 bpp), SPIHT compressed image (0.4 bpp).

inal version such that the visual quality is identical, but the displacing component does not contain any watermark.

The results, reported in Table VI for $\tau = 0.45$, show the overall better performance of the proposed dual domain authentication approach. Our method ranks number one for three of the seven attacks, and number two for the remaining four of the seven attacks. The other methods are each appropriate for different attacks, but do not exhibit the attractive global behavior of the proposed scheme. Furthermore, if a content change occurs, the proposed test cases are correctly able to identify it and its location.

Moreover in Table VII a confusion matrix indicating the error rate between all the three levels considered by the proposed system is reported.

The asymmetric approach was also tested and its greater sensitivity compared to the symmetric approach. Fig. 6 demon-

TABLE VIII
BIT RATES EMPLOYED FOR THE DIFFERENT SUBBANDS IN THE "ADAPTIVE COMPRESSION" STAGE

	b_{tot}	b_{LL}					b_{LH}	b_{HL}	b_{HH}
"Terrace"	0.2	0.1	b_{2LL}	b_{2LH}	b_{2HL}	b_{2HH}	0.0375	0.0375	0.025
			0.05	0.01875	0.01875	0.0125			
"Cover"	0.3	0.15	b_{2LL}	b_{2LH}	b_{2HL}	b_{2HH}	0.04	0.06	0.05
			0.075	0.02	0.03	0.025			
"Horse"	0.4	0.2	b_{2LL}	b_{2LH}	b_{2HL}	b_{2HH}	0.075	0.075	0.05
			0.1	0.0375	0.0375	0.025			

TABLE IX
NMSE EVALUATION FOR THE COMPRESSED IMAGE OBTAINED USING THE COMBINED AUTHENTICATION-COMPRESSION METHOD (A&C), SPIHT COMPRESSION, JPEG COMPRESSION, AND JPEG2000 COMPRESSION

Image	bpp	A&C	SPIHT	JPEG	JPEG2000
"Terrace"	0.2	0.075	0.086	0.09	0.065
"Cover"	0.3	0.15	0.17	0.19	0.13
"Horse"	0.4	0.09	0.11	0.12	0.08

TABLE X
BLOCK ERROR RATES R_{LH} AND R_{HL} FOR THE COMBINED AUTHENTICATION-COMPRESSION METHOD (A&C), FOR THE AUTHENTICATION METHOD FOLLOWED BY SPIHT COMPRESSION, JPEG COMPRESSION, AND JPEG2000 COMPRESSION, AT A FIXED BIT RATE

		R_{LH}				R_{HL}			
Image	bpp	A&C	SPIHT	JPEG	JPEG2000	A&C	SPIHT	JPEG	JPEG2000
"Terrace"	0.2	0.17	0.53	0.63	0.52	0.14	0.54	0.55	0.53
"Cover"	0.3	0.23	0.52	0.61	0.52	0.21	0.51	0.61	0.52
"Horse"	0.4	0.18	0.52	0.56	0.49	0.17	0.52	0.51	0.50
"Terrace"	1	0.12	0.3	0.29	0.26	0.09	0.32	0.24	0.28
"Cover"	1.5	0.15	0.24	0.25	0.23	0.14	0.25	0.28	0.26
"Horse"	2	0.13	0.14	0.11	0.11	0.12	0.15	0.12	0.11

strates the performance of the scheme in locating spatial tampering. The authentication matrix A_{LH} is able to detect the location of tampering, but authentication is not possible since the A_{HL} is completely scrambled. An application-based decision may be made to assess whether the components of the image that do not exhibit tampering are still of use. Other examples of tampering by removing a leaf from Fig. 9 or the addition of the letter "I" in front of the word "Nuit" in Fig. 8 demonstrate similar results. The proposed technique can locate tampering, but authentication is not possible. In comparison, the symmetric approach for the same test images provides similar A_{LH} results, but $A_{HL} \approx A_{LH}$ also localizes the tampering.

B. Color Image Compression

To evaluate the performance of compressive data hiding for CH imagery, we compare our results visually and quantitatively to the following well known image compression algorithms: SPIHT, JPEG2000 and JPEG which do not have authentication capability. Our quantitative figure of merit to assess performance is selected because it is a widely used similarity measure between the perceptual characteristics of two color images. The normalized mean square error (NMSE) is defined as

$$NMSE = \frac{\sum_{i=1}^{M_x}\sum_{j=1}^{M_y} \| \mathbf{X}[i,j] - \hat{\mathbf{X}}[i,j] \|^2}{\sum_{i=1}^{M_x}\sum_{j=1}^{M_y} \| X[i,j] \|^2} \tag{30}$$

where $\| \cdot \|$ represents the Euclidean norm of the corresponding vector argument, M_x and M_y represent the color image dimensions, and $\mathbf{X}[i,j]$ and $\hat{\mathbf{X}}[i,j]$ are the original color image vector and the transformed one, respectively, at pixel $[i,j]$.

In Figs. 7–9, the authenticated color images, compressed at different bit rates 0.2 bpp, 0.3 bpp, 0.4 bpp, using the proposed approach, are shown along with their original counterparts. The bpp values employed to code the different subbands of the images under examinations are reported in Table VIII for the different compression rates employed in the performed simulations. For the sake of comparison in Figs. 7–9 the SPIHT and JPEG2000 compressed version of the examined color images are also shown. Simulations have also been performed using the JPEG coder but the compressed images have not been reported for sake of brevity. In all cases, it is clear that our proposed algorithm has good perceptual performance.

Table IX provides an evaluation of the performances, in terms of NMSE, of the proposed authentication-compression method in comparison with SPIHT, JPEG, and JPEG2000 coders is reported. From the experimental results it is evident that our combined approach outperforms SPIHT and JPEG, in term of compression capabilities, whereas comparable or better results are obtained using the JPEG2000 coder. This quantitative performance evaluation is in agreement with a subjective evaluation performed on the images displayed in Figs. 7–9.

C. Joint Authentication and Compression

Combining both authentication and compression, we hypothesize that there is a trade-off in performance between authentication capability and compression quality. The higher the compression rate, the greater the affect on the authentication component. The portion of the luminance image that can be used

for embedding the watermark decreases as the compression rate is increased. Thus, the authentication and chrominance watermarks loose bandwidth resulting in errors.

For symmetric authentication, Table X reports block error rates R_{LH} and R_{HL} for a number of different situations involving our dual domain authentication cascaded by a compression stage (with a given fixed bit rate). The proposed algorithm for joint dual domain authentication and compression (using our adaptive strategy) is compared to our dual domain authentication alone cascaded with SPIHT, JPEG and JPEG2000 at various fixed bit rates. The results demonstrate that the authentication assessment is least affected by our proposed adaptive compression strategy. Thus, our overall scheme appears to demonstrate a more optimal compromise than just selecting an arbitrary lossy compression algorithm f_l. Furthermore, for $\tau = 0.35$, our symmetric scheme is able to handle compression above or at 1 bpp. Naturally, lower values of τ provide greater authentication security, and as a result require higher quality compression rates.

Our adaptive compression algorithm was designed to affect the authentication and chrominance watermark embedded bands to a lower degree than the others. Thus, judicious compression has, in part, contributed to the effective blend of compression and security.

VI. Conclusions

This paper discusses an approach to combine image authentication with compression for the security of CH imagery within a digital watermarking paradigm. The overall algorithm makes use of orthogonal dual domains and compressive data hiding for an integrated algorithm. Application of the approach to real CH imagery provides an indication of the potential of the approach and its improved performance over existing research. Through this investigation, we have observed the following general design compromises.

- Image subspace orthogonality can be exploited in a digital watermarking framework to provide a flexible multipurpose algorithm for both security and compression. Various components can be individually optimized for performance with little interference, but the partitioning of subspaces must be well-suited for the intended application.
- Through the use of a dual domain, external watermark information does not have to be transmitted to the receiver, however, this advantage in convenience and security against eavesdropping comes at the expense of ambiguity in the tamper assessment. In addition, there exists a trade-off between making a semi-fragile watermark robust to content-preserving operations and fragile to malicious attack.

Given the empirical nature of our design process in this paper, future work involves developing analytic methods of selecting appropriate compromises among complexity, convenience, security, robustness, and fragility.

In addition, further work will propose improvements, at the expense of complexity, to the security of the embedding method to sophistcated image processing attacks.

References

[1] A. C. Addison and M. Gaiani, "Virtualized architectural heritage: New tools and techniques," *IEEE Multimedia*, vol. 7, no. 2, pp. 26–31, April–June 2000.

[2] V. Cappellini, F. Bartolini, R. Caldelli, A. De Rosa, A. Piva, M. Barni, and M. Wada, "Copyright protection for CH multimedia data through digital watermarking techniques," in *Proc. 11th IEEE Int. Workshop on Database and Expert Systems Applications*, September 2000, pp. 935–939.

[3] W. Stallings, *Network Security Essentials: Applications and Standards*: Prentice Hall, 2000.

[4] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper-proofing and authentication," *Proc. IEEE Special Issue on Identification and Protection of Multimedia Information*, vol. 87, pp. 1167–1180, July 1999.

[5] Y. Zhao, "Dual Domain Semi-Fragile Watermarking for Image Authentication," M.A.Sc. thesis, Univ. Toronto, Toronto, ON, Canada, 2003.

[6] P. Campisi, D. Kundur, D. Hatzinakos, and A. Neri, "Compressive data hiding: An unconventional approach for improved color image coding," *EURASIP J. Appl. Signal Process. Special Issue on Emerging Applications of Multimedia Data Hiding*, vol. 2002, no. 2, pp. 152–163, Feb. 2002.

[7] M. Goljan and J. Fridrich, "Protection of digital image using self embedding," in Proc. Symposium on Content Security and Data Hiding in Digital Media, May 1999.

[8] J. Fridrich, A. C. Baldoza, and R. J. Simard, "Robust digital watermarking based on key-dependent basis function," in Proc. 2nd Information Hiding Workshop, April 1998.

[9] J. Fridrich, "Combining low frequency and spread spectrum watermarking," in *Proc. SPIE, Mathematics of Data/Image Coding, Compression, and Encryption*, vol. 3456, July 1998, pp. 2–12.

[10] ——, "Image watermarking for tamper detection," *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, pp. 404–408, October 1998.

[11] M. Goljan and J. Fridrich, "Invertible authentication watermark for JPEG images," *Proc. IEEE Int. Conf. on Information Technology: Coding and Computing*, pp. 223–227, April 2001.

[12] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, pp. 427–431, October 1998.

[13] ——, "A blind wavelet based digital signature for image authentication," in *Proc. 9the European Signal Processing Conference*, September 1998, pp. 21–24.

[14] ——, "A class of authentication digital watermarks for secure multimedia communication," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1754–1764, November 2001.

[15] J. Dittmann, "Content-fragile watermarking for image authentication," in *Proc.SPIE, Security and Watermarking of Multimedia Content III*, vol. 4314, Jan. 2001, pp. 175–184.

[16] M. Yeung and F. Mintzer, "An invisible watermark technique for image verification," *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, pp. 680–683, October 1997.

[17] J. Fridrich, M. Goljan, and A. C. Baldoza, "New fragile authentication watermark for images," *Proc. IEEE Int. Conf. on Image Processing*, vol. 1, pp. 446–49, September 2000.

[18] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," *Proc. IEEE Int. Conf. on Image Processing*, vol. 3, pp. 219–222, September 1996.

[19] P. W. Wong, "A public key watermark for image verification and authentication," *Proc. IEEE Int. Conf. on Image Processing*, vol. 1, pp. 455–459, October 1998.

[20] ——, "Watermarking for image integrity and ownership verification," in Proc. IS&T PIC Conf., May 1998.

[21] J. J. Eggers, J. K. Su, and B. Girod, "A blind watermark scheme based on structured codebooks," in *IEE Conf. on Secure Images and Image Authentication*, April 2000, pp. 4/1–4/21.

[22] J. J. Eggers and B. Girod, "Blind watermarking applied to image authentication," *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol. 3, pp. 1977–1980, May 2001.

[23] J. C. Boncelet, L. M. Marvel, and G. W. Hartwig, "Compression compatible fragile and semi-fragile tamper detection," in *Proc. SPIE, Security and Watermarking of Multimedia Contents II*, vol. 3971, January 2000.

[24] L. M. Marvel, C. G. Boncelet Jr, and C. T. Retter, "Spread spectrum image steganography," *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075–1083, August 1999.
[25] D. Kundur and D. Hatzinakos, "Toward a telltale watermarking technique for tamper-proofing," *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, pp. 409–13, October 1998.
[26] C.-S. Lu, H.-Y. M. Liao, and C.-J. Sze, "Combined watermarking for image authentication and protection," *Proc. IEEE Int. Conf. on Multimedia and Expo.*, vol. 3, pp. 1415–1418, August 2000.
[27] C. S. Liu and H. Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," in Proc. ACM Multimedia and Security Workshop, 2000.
[28] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, December 1997.
[29] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions on Circuits and System for Video Technology*, vol. 6, no. 3, pp. 243–250, June 1996.
[30] J. Li, P.-Y. Cheng, and C.-C. J. Kuo, "A wavelet transform approach to video compression," in *Proc. SPIE, Wavelet Applications II*, vol. 2491, April 1995, pp. 1107–1118.
[31] K. Sayood, *Introduction to Data Compression*, 2nd ed: Morgan Kaufmann Publishers, 2000.
[32] C. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transactions on Circuits and Systems of Video Technology*, vol. 11, no. 2, pp. 153–168, February 2001.
[33] O. Ekici, B. Coskin, U. Naci, and B. Sankur, "Comparative assessment of semi-fragile watermarking techniques," in *Proc. SPIE, Multimedia Systems and Applications IV*, vol. 4518, August 2001.
[34] A. B. Watson, "DCT quantization matrices optimized for indivudual images," in *Proc. SPIE, Human Vision, Visual Processing, and Digital Display IV*, vol. 1913, 1993.

Yang Zhao received the B.A.Sci. degree from Shanghai University, Shanghai, China, in 1998, and the M.A.Sc degree from the Electrical and Computer Engineering Department, University of Toronto, Toronto, ON, Canada, in 2003.

She received the National Bao Steel Scholarship 1997 in China and the University of Toronto Fellowship in 2001 and 2002. Her research topic was multimedia authentication and network security. She has a wide variety of interests in signal processing, Internet security, and economics.

Patrizio Campisi (M'99) received the "Laurea" degree in electrical engineering (summa cum laude) from the University of Roma "La Sapienza," Roma, Italy, and the Ph.D. degree in electrical engineering from the University of Roma "Roma Tre," in 1995 and 1999, respectively.

He is an Assistant Professor with the Department of "Elettronica Applicata," University of Roma "Roma Tre," where he has been also Lecturer for the graduate course "Signal Theory" since 1998. From September 1997 until April 1998, he was a Visiting Research Associate with the Communication Laboratory, University of Toronto, Toronto, ON, Canada, and from July 2000 until December 2000, he was a Postdoctoral Fellow with the same laboratory. From October 1999 to October 2001, he held a postdoctoral position at the University of Roma "Roma Tre." From March 2003 to June 2003 he was a Visiting Researcher with the Beckman Institute, University of Illinois at Urbana-Champaign. His research interests are in the area of digital signal and image processing with applications to multimedia communications.

Dr. Campisi has been a member of the Technical Committees of several IEEE conferences (ICME 2002, ICME 2003, ISPA 2003, and MMSP 2004). He was the organizer for the special session on "texture analysis and synthesis" for the IEEE International Symposium on Image and Signal Processing and Analysis 2003 (ISPA 2003). He is a Member of the IEEE Communications and Signal Processing Society and the Italian Professional Engineers Association.

Deepa Kundur (S'93–M'99–SM'03) was born in Toronto, ON, Canada. She received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering in 1993, 1995, and 1999, respectively, from the University of Toronto.

In January 2003, she joined the Electrical Engineering Department at Texas A&M University where she is a Member of the Wireless Communications Laboratory and holds the position of Assistant Professor. From September 1999 to December 2002, she was an Assistant Professor at the Edward S. Rogers, Sr., Department of Electrical and Computer Engineering at the University of Toronto where she held the title of Bell Canada Junior Chair-holder in Multimedia. Her research interests include multimedia and network security, video cryptography, data hiding and steganography, covert communications, and nonlinear and adaptive information processing algorithms.

Dr. Kundur has been on numerous technical program committees and has given tutorials at ICME 2003 and Globecom 2003 in the area of digital rights management. She is a Guest Editor for the PROCEEDINGS OF THE IEEE Special Issue on Enabling Technologies for Digital Rights Management. She was recently the recipient of the 2002 Gordon Slemon Teaching of Design Award and the 2002 Best Electrical Engineering Professor Award (Spring) presented by the ECE Club.