Transactions Letters

An Algorithm for Removable Visible Watermarking

Yongjian Hu, *Member, IEEE*, Sam Kwong, *Senior Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE*

***Abstract*—A visible watermark may convey ownership information that identifies the originator of image and video. A potential application scenario for visible watermarks was proposed by IBM where an image is originally embedded with a visible watermark before posting on the web for free observation and download. The watermarked image which serves as a "teaser." The watermark can be removed to recreate the unmarked image by request of interested buyers. Before we can design an algorithm for satisfying this application, three basic problems should be solved. First, we need to find a strategy suitable for producing large amount of visually same but numerically different watermarked versions of the image for different users. Second, the algorithm should let the embedding parameters reachable for any legal user to make the embedding process invertible. Third, an unauthorized user should be prevented from removing the embedded watermark pattern. In this letter, we propose a user-key-dependent removable visible watermarking system (RVWS). The user key structure decides both the embedded subset of watermark and the host information adopted for adaptive embedding. The neighbor-dependent embedder adjusts the marking strength to host features and makes unauthorized removal very difficult. With correct user keys, watermark removal can be accomplished in "informed detection" and the high quality unmarked image can be restored. In contrast, unauthorized operation either overly or insufficiently removes the watermark due to wrong estimation of embedding parameters, and thus, the resulting image has apparent defect.**

***Index Terms*—Image watermarking, removable watermarking, visible watermark.**

I. Introduction

A VISIBLE watermark conveying perceptual IPR (intellectual property rights) information of digital image/video is generally designed to be irreversible so that it can survive unintentional modifications or malicious attacks (e.g., [1]–[4]). However, there are some potential applications where a visible watermark needs to be removable or reversible. The IBM Tokyo research laboratory once gave the following example [5]. In online image distribution, an image is visually watermarked before posting on the web. This watermarked image content serves as a "teaser" where the watermark acts as an advertisement as well as a restriction. The interested buyers can remove the embedded watermark pattern to recreate the unmarked image using a retrieval, or called as "vaccine," program that is available for an additional fee. Although the concept of reversible visible watermarks was proposed by IBM in 1997 [5], unfortunately, to the best of the authors' knowledge, the development of such a watermarking technique has rarely been reported in the literature.

A topic related to removable watermarks is reversible invisible watermarking (e.g., [6]–[12]). The motivation behind these researches lies in data tamper-proofing. Early techniques such as fragile watermarking deter strict integrity control due to permanent alteration to image pixel values. To circumvent this problem, the watermarking process is required to be reversible. Most reversible embedding methods either adopt additive spread spectrum techniques or modify some host features to insert the information payload. The concept of invertible authentication was first presented by Honsinger *et al.* [6]. To avoid salt and pepper noise in [6], Fridrich *et al.* [7] proposed a technique based on lossless compression and encryption of bit planes. The other techniques include [8], [9] and [10]. In [8], Vleeschouwer *et al.* extended the patchwork method and used circular histogram to hide the binary message. The recent work in reversible invisible watermarking is [11], which is the extension of Tian's algorithm in [12] and uses difference expansion of vectors, instead of pairs, to increase the hiding capacity.

Generally, an algorithm for invisible watermarking can hardly be extended for visible watermarking by simply increasing embedding strength. These two types of algorithms are often designed according to different requirements of robustness, using perceptual models in different ways and for different application scenarios. In visible watermarking, we usually need large bit rate and strong strength to exhibit a visible watermark pattern. In invisible watermarking, however, small bit rate and weak strength are preferred to avoid visibility.

In this letter, we present a user-key-dependent removable visible watermarking system (RVWS). Let $\mathbf{I}_h$ and $\mathbf{I}_m$ denote the host image and the watermark, respectively. The goal of watermark removal is to obtain the unmarked image $\mathbf{I}_u$ from the watermarked image $\mathbf{I}_c$. In the mentioned application, however, we have to build the RVWS in a more complicated way. The algorithm should be able to embed $\mathbf{I}_m$ into $\mathbf{I}_h$ and create thousands of visually same but numerically different watermarked versions of the image, i.e., $\{\mathbf{I}_{c_1}, \mathbf{I}_{c_2}, \ldots, \mathbf{I}_{c_n}\}$. On the other side, in order not to obscure image details and increase robustness, the degree of marking needs to be variable with host features. In other words, the embedding algorithm is image-adaptive. Furthermore, the pixel-by-pixel varying parameters of the

Manuscript received March 19, 2004; revised May 05, 2005. This work was supported in part by City University Strategic Grant 7001697, in part by the Natural Science Foundation of Guangdong Grants 04020004 and 013164, and in part by the National Science Foundation of China Grants 60403045, 60325208, and 60133020. This paper was recommended by Associate Editor A. Kot.

Y. Hu is with the College of Automation Science and Engineering, South China University of Technology, Guangzhou 510640, China (e-mail: eeyjhu@scut.edu.cn).

S. Kwong is with the Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong (e-mail: cssamk@cityu.edu.hk).

J. Huang is with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China (e-mail: isshjw@zsu.edu.cn).

Digital Object Identifier 10.1109/TCSVT.2005.858742

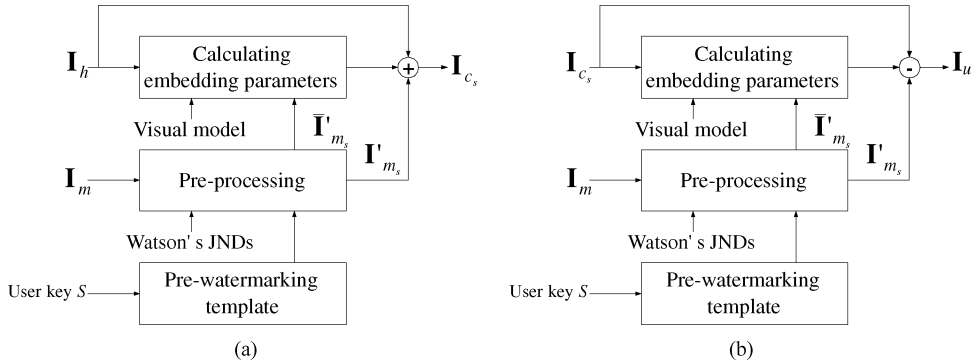

Fig. 1. Framework of RVWS. (a) Watermark embedding. (b) Watermark removal.

embedder are required to be easily transferred to any legal user for recreating $\mathbf{I}_u$ while the original host image is forbidden in the receiver end. Obviously, these characteristics make the proposed algorithm different from any one in the literature.

Ideally, the host image would be losslessly restored if the watermark is completely removed, i.e., $\mathbf{I}_u = \mathbf{I}_h$. However, distortion-free recovery is difficult due to the requirement of large bit rate and strong strength in visible watermarking. Therefore, in this work, we only aim at the following objectives: 1) propose a user-key-controlled RVWS and implement it in discrete wavelet transform (DWT) domain and 2) introduce a preventive scheme against unauthorized operations such as removing the embedded watermark by using incorrect user keys.

The letter is organized as follows. Section II discusses the strategy for constructing the RVWS. In Section III, we focus on the technique for implementing the RVWS in DWT domain. We also discuss our scheme to prevent unauthorized watermark removal in detail. In Section IV, we give some experiments to validate the proposed algorithm and analyze its performance. We draw the conclusion in Section V.

II. Strategy for Constructing RVWS

The way of pixel-to-pixel embedding is commonly used in visible watermarking. One advantage is that we do not need to save spatial position information of watermark pixels in the resulting watermarked image. Before performing watermark addition, we establish a relationship of pixel-to-pixel correspondence between the host image and the watermark. This scheme has been commonly applied in both spatial and transform domain methods. The addition rule can be generally described as

$$\mathbf{I}_c = f(\mathbf{I}_h, \mathbf{I}_m, \delta) \tag{1}$$

or described in a manner of pixel-to-pixel addition as

$$i_c = w_h i_h + w_m i_m \tag{2}$$

where f is the embedding function; δ represents the set of parameters of the embedder; i_h, i_m and i_c are scalars corresponding to $\mathbf{I}_h$, $\mathbf{I}_m$, and $\mathbf{I}_c$, respectively. δ can be practically described with w_h and w_m, which are pixel-wise varying weighting factors for the host image and the watermark, respectively.

The embedding of all elements in $\mathbf{I}_m$ into the host image is obviously not suitable for constructing the RVWS. In this letter, two factors will be taken into account when creating watermarked versions: the selection of watermark pixels to be embedded and the way of calculating embedding parameters. According to [13], revealing all the details of the watermark in the composite image is unnecessary and the watermark pattern can be displayed with the embedding of partial watermark pixels. This letter then suggests that different watermarked versions $\mathbf{I}_{c_s}$ are created with different subsets of $\mathbf{I}_m$, i.e., $\mathbf{I}'_{m_s}$. The subscript $s(=1,2,\ldots,n)$ represents different individuals. $\mathbf{I}'_{m_s}$ is controlled by the user key. We put two constraints on the selection of $\mathbf{I}'_{m_s}$. First, to ensure different watermarked versions to look like each other, $\mathbf{I}'_{m_s}$ must contain the basic subset consisting of visually significant pixels of $\mathbf{I}_m$. Second, to make a watermarked version numerically different from others, a user-key-dependent pre-watermarking template is used to put small amount of random pixels into $\mathbf{I}'_{m_s}$ to make $\mathbf{I}'_{m_1} \neq \mathbf{I}'_{m_2} \neq \cdots \neq \mathbf{I}'_{m_n}$. Apparently, $\mathbf{I}'_{m_s} \subset \mathbf{I}_m$. Let $\overline{\mathbf{I}}'_{m_s}$ denote the subset which contains the watermark pixels not to be embedded. We then have $\overline{\mathbf{I}}'_{m_s} = \mathbf{I}_{m_s} - \mathbf{I}'_{m_s}$.

Reversibility requires watermark insertion and removal to be symmetric. Thus, δ needs to be resumable in the receiver end. However, the original host image is restricted in the process of removal. This implies that we can only use deliberately arranged host information to achieve adaptive embedding. As stated above, $\mathbf{I}'_{m_s}$ is to be embedded instead of $\mathbf{I}_m$, so that partial host pixels will be kept unchanged in the watermarked image. Let those unchanged host pixels constitute $\overline{\mathbf{I}}'_{h_s}$. Obviously, the pixels in $\overline{\mathbf{I}}'_{h_s}$ are spatially correspondent to the watermark pixels in $\overline{\mathbf{I}}'_{m_s}$. We then suggest that $\overline{\mathbf{I}}'_{h_s}$ can be used to provide the host features information for the calculation of embedding parameters. Thus, with $\mathbf{I}_m$ and the correct user key, $\overline{\mathbf{I}}'_{h_s}$ is known in the process of removal, so that the embedding parameters can be regained. We call the removal process with obtainable embedding parameters "informed detection". In this letter, we define the "vaccine" program as a retrieval data packet containing three components: $\mathbf{I}_m$, the user key and the shared removing codes.

The framework of the proposed RVWS is depicted in Fig. 1. The Watson's just noticeable differences (JNDs) [14] are borrowed to choose visually significant pixels from $\mathbf{I}_m$. More explanation about Fig. 1 will be given in the next section.

III. DWT-Domain RVWS

We propose a technique to implement the RVWS in DWT domain. For simplicity, the symbols defined in spatial domain will

be directly used to denote their transform domain counterparts. Wavelet decomposition of an image can be expressed as

$$x^{(0)} = \{y^{(1)}, y^{(2)}, \ldots, y^{(K)}, x^{(K)}\} \tag{3}$$

where $x^{(K)}$ represents the low-frequency subband LL, $y^{(k)}$ the high-frequency subbands at scale k. $x^{(0)}$ refers to the original image. $y^{(k)} = \{y^{(k)}(.|1), y^{(k)}(.|2), y^{(k)}(.|3)\}$ corresponds to three high-frequency subbands in orientations LH, HL, and HH. $k(= 1, 2, \ldots, K)$ denotes the decomposition scale. Let wavelet coefficients y_h, y_m and y_c correspond to the transform images $\mathbf{I}_h$, $\mathbf{I}_m$ and $\mathbf{I}_c$, respectively. Equation (2) is rewritten as follows:

$$y_c = w_h y_h + w_m y_m. \tag{4}$$

Note that the coordinate (i, j) is not indicated unless confusion arises. Before embedding, we perform wavelet decomposition on both the host image and the watermark. Due to different characteristics in low and high-frequency subbands, the RVWS is divided into two parts: low-frequency subband watermarking and high-frequency subbands watermarking. With the framework shown in Fig. 1, we describe these two parts in detail separately.

A. Low-Frequency Subband Watermarking

Let $\mathbf{I}_{ml}$ denote the set of low-frequency coefficients of $\mathbf{I}_m$. $\mathbf{I}'_{ml}$ and $\bar{\mathbf{I}}'_{ml}$ represent the sets of low-frequency coefficients to be and not to be embedded, respectively. $\bar{\mathbf{I}}'_{ml} = \mathbf{I}_{ml} - \mathbf{I}'_{ml}$.

In this letter, we use one user s to explain the watermarking process. In order to determine $\mathbf{I}'_{ml_s}$, we introduce a user-key-controlled prewatermarking template $\mathbf{T}_{l_s}$. $\mathbf{T}_{l_s}$ is a pseudo-random matrix with binary element that follows uniform distribution. It has the same size of LL. We use $\mathbf{T}_{l_s}$ as a mask and put it on the low-frequency subband of the watermark, LL_m. All coefficients corresponding to "1" are chosen to constitute $\mathbf{I}'_{ml_s}$. Note that the Watson's perceptual model is not used in low-frequency subband watermarking. The seed of generating $\mathbf{T}_{l_s}$ is the user key. Since a user key uniquely corresponds to one specific user, we use s to indicate either the user or the key.

In order to design adaptive embedding, the calculation of w_h and w_m is based on a visual model which can describe the characteristics of the host low-frequency subband image, LL_h. We use the unchanged host coefficients, which spatially correspond to the watermark coefficients in $\bar{\mathbf{I}}'_{ml_s}$, to construct a temporary subband image, LL'_h. LL'_h is introduced for calculating the value of the visual model. Intuitively, those unchanged host coefficients correspond to "0" in $\mathbf{T}_{l_s}$. Each coefficient in LL'_h, $x'^{(K)}_h(i, j)$, can be calculated in the following way. For the sake of simplicity, we ignore the superscript (K).

If $x'_h(i, j)$ corresponds to "0" in $\mathbf{T}_{l_s}$

$$x'_h(i, j) = x_h(i, j);$$

Elseif $x'_h(i, j)$ corresponds to "1" in $\mathbf{T}_{l_s}$ but some of its 8 nearest neighbors correspond to "0"

$$x'_h(i, j) = \bar{x}_{h_b};$$

Elseif $x'_h(i, j)$ and all of its 8 nearest neighbors correspond to "1" in $\mathbf{T}_{l_s}$

$$x'_h(i, j) = \bar{x}_h$$

where $x_h(i, j)$ represents a coefficient in LL_h. $\bar{x}_h$ represents the mean of all unchanged coefficients in LL_h. $\bar{x}_{h_b}$ represents the mean of unchanged coefficients in the 8 nearest neighbors of the current position.

Then the value of luminance masking model [13], $L(i, j)$, can be calculated as follows:

$$L(i, j) = \exp(-(x'_h(i, j) - \bar{x}'_h)^2) \tag{5}$$

where $x'_h(i, j)$ and $\bar{x}'_h$ represent a coefficient and the mean of all coefficients in LL'_h, respectively. Thus, the embedding factors can be determined with the value of the visual model as follows:

$$w_h(i, j) = L'(i, j) \tag{6}$$

$$w_m(i, j) = 1 - L'(i, j) \tag{7}$$

where $L'(i, j)$ is the scaled $L(i, j)$ and its value falls into a narrow range [0.9,0.95] to avoid heavy embedding. Using $w_h(i, j)$ and $w_m(i, j)$, we can embed all coefficients in $\mathbf{I}'_{ml_s}$ into LL_h. In the process of watermark removal, when the "vaccine" program is provided, we can determine $\mathbf{I}'_{ml_s}$, so that the embedding parameters can be resumed and the "informed detection" can be accomplished in the low-frequency subband image.

It is noted that the proposed embedding scheme only embeds a compressed version of low-frequency watermark subband image; besides, w_h and w_m derived from LL'_h only approximately reflect the characteristics of LL_h. However, the experiments demonstrate that the watermarked images still have acceptable visual quality.

B. High-Frequency Subbands Watermarking

High-frequency subbands watermarking is similar to low-frequency subband watermarking but more complex. We use one subband to explain the situation. Let $\mathbf{I}_{mh}$ denote the set of all high-frequency watermark coefficients. Let $\mathbf{I}'_{mh}$ and $\bar{\mathbf{I}}'_{mh}$ denote the sets to be and not to be embedded, respectively. Then $\bar{\mathbf{I}}'_{mh} = \mathbf{I}_{mh} - \mathbf{I}'_{mh}$.

$\mathbf{I}'_{mh_s}$ is composed of the union of $\mathbf{I}'_{mh_p}$ and $\mathbf{I}''_{mh_s}$, where $\mathbf{I}'_{mh_p}$ is the set of visually important watermark coefficients selected by the Watson's JNDs and $\mathbf{I}''_{mh_s}$ is the set determined using the user-key-controlled high-frequency prewatermarking template $\mathbf{T}_{h_s}$. $\mathbf{I}''_{mh_s}$ is used to ensure $\mathbf{I}'_{mh_1} \neq \mathbf{I}'_{mh_2} \neq \cdots \neq \mathbf{I}'_{mh_n}$. $\mathbf{T}_{h_s}$ is constructed in a similar way as in low-frequency subband watermarking. Putting $\mathbf{T}_{h_s}$ on the high-frequency subband, the coefficients corresponding to "1" are chosen to constitute $\mathbf{I}''_{mh_s}$. Practically, $\mathbf{I}'_{mh_s} = \mathbf{I}_{mh_s} \cup \mathbf{I}'_{mh_p}$ and $\mathbf{I}''_{mh_s} \cap \mathbf{I}'_{mh_p} \neq \phi$.

The calculation of w_h and w_m in high-frequency subbands watermarking is also based on a visual model. We consider the effects of both luminance masking and local spatial characteristics. For simplicity of discussion, we first give the formulas for calculating w_h and w_m as follows:

$$L'_h(i, j) = L'\left(\frac{i}{2^{K-k}}, \frac{j}{2^{K-k}}\right) \tag{8}$$

$$w_h(i, j) = \sigma'(i, j) L'_h(i, j) \tag{9}$$

$$w_m(i,j) = \frac{1}{\sigma'(i,j)}(1 - L'_h(i,j)) + K_c n \qquad (10)$$

where $L'_h(i,j)$ refers to the value of luminance masking. K and k represent the decomposition scale and the current scale, respectively. In (9) and (10) [4], $\sigma'(i,j)$ describes local spatial characteristics, however, it no longer depends on the current coefficient but its neighbors for the reason of reversibility and anti-illegal-removal. The second item in (10) is mainly designed for preventing unauthorized watermark removal. K_c is a constant and $n(= 0, \ldots, 8)$ is the number of unchanged host coefficients in the 8 nearest neighbors centered at the current coefficient.

We define $\sigma(i,j)$ as the coefficient magnitude and $\sigma'(i,j)$ is scaled $\sigma(i,j)$. The use of (9) and (10) shows that our watermark embedding scheme abides by the principle of embedding more watermark energy in featureless regions and less in edges and rapidly changing regions. Let $y_h(i,j)$ denote a host coefficient to be manipulated. $\sigma(i,j)$ can be calculated in the following way.

If $y_h(i,j)$ has some unchanged coefficients in its 8 nearest neighbors

$$\sigma(i,j) = \bar{y}_{h_3};$$

Elseif $y_h(i,j)$ has no unchanged coefficients in its 8 nearest neighbors but some in its 24 nearest neighbors,

$$\sigma(i,j) = \bar{y}_{h_5};$$

Else

$$\sigma(i,j) = \bar{y}_h$$

where $\bar{y}_{h_3}$ and $\bar{y}_{h_5}$ represent the means of absolute values of unchanged host coefficients in the 8 and 24 nearest neighbors centered at $y_h(i,j)$, respectively. $\bar{y}_h$ denotes the mean of absolute values of all unchanged host coefficients in the high-frequency subband. The value of $\sigma'(i,j)$ is kept in the range [0.9,1] to ensure moderate alteration to host coefficients.

The second item in (10) reflects the influence on watermark embedding from the neighboring unchanged coefficients. Because n is a user-key-controlled random number, the effect against unauthorized removal is significant. Due to the special components of $\mathbf{I}'_{mh_s}$, the number of marked coefficients is often larger than that of unchanged ones, so that n is frequently smaller than 5. It can be estimated that the sum of w_h and the first item in (10) is usually around 0.9, so we let $K_c = 0.02$.

In the receiver end, given the "vaccine" program, we can obtain $\mathbf{I}'_{mh_s}$ and $\bar{\mathbf{I}}'_{mh_s}$. σ' can be estimated, and then, w_h and w_m can be recalculated, so that the watermark removal can be accomplished.

IV. Experiment and Discussion

The proposed algorithm has been tested on several standard images. We use 9-7 wavelet and perform 4-level wavelet decomposition. Two watermarked images and their difference image

Fig. 2. Watermarked images (left and center) produced with two different user keys and their difference image (right). The gray value in the difference image is amplified for being displayed on screen.

TABLE I
PSNR (dB) of Recovered Images. LR and ILR Denote Legally and Illegally Recovered Images, Respectively

		$s=1$	$s=2$	$s=3$	$s=4$	$s=5$
Lena	LR	44.15	44.16	44.15	44.14	44.15
	ILR	38.34	38.25	38.15	38.15	38.16
Sailboat	LR	44.15	44.15	44.16	44.16	44.16
	ILR	36.85	36.82	36.70	36.83	36.72
Peppers	LR	44.11	44.13	44.14	44.13	44.13
	ILR	38.05	37.94	37.88	38.04	37.93
Girl	LR	43.54	43.56	43.47	43.51	43.50
	ILR	38.79	38.60	38.68	38.66	38.57
F-16	LR	44.16	44.15	44.15	44.16	44.15
	ILR	37.89	37.78	37.77	37.91	37.84

are shown in Fig. 2. Just as expected, the two watermarked versions look like each other. However, the difference image in the right discloses their numerical distinction. It can be easily found that the gray value difference exists almost everywhere in the image. The reason is that, in both low and high-frequency subbands, the calculation of weighting factors depends on the user key mechanism, so that $\mathbf{I}'_{m_s}$ is embedded with changing weighting factors as users are different.

Usually, a legally recovered image $\mathbf{I}_u$ has good visual quality. As shown in Table I, the peak signal-to-noise ratio (PSNR) is around 44 dB. However, an unauthorized user can not obtain $\mathbf{I}_u$ with satisfactory quality. We compare the close-ups of legally and illegally restored images in Fig. 3. In the left close-up, moss-like unevenly darken areas spread across the entire image. They are especially visible in regions with middle gray intensity, such as face and shoulder. This visible distortion results from the fact that an unauthorized user, without the correct user key, can not accurately determine $\mathbf{I}'_{m_s}$ and thus blindly estimate w_h and w_m. Consequently, the watermark is overly subtracted in some coefficients and insufficiently subtracted in the others from the watermarked image. Although the PSNR is around 37 dB, the defect can be clearly seen on screen and certainly ruins the commercial value of the reconstructed image. The PSNR can not well reflect human perception in this case.

We now examine the performance of the RVWS. From the PSNR values of normally recovered images (see Table I)

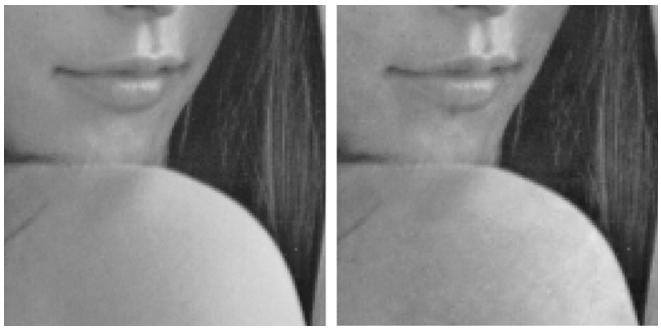

Fig. 3. Close-ups of two recovered images. (Left) Legally obtained image. (Right) Illegally obtained one.

TABLE II
OVERFLOW AND UNDERFLOW AT GRAY BOUNDARY. OF AND UF DENOTE THE NUMBER OF OVERFLOW AND UNDERFLOW POINTS, RESPECTIVELY

		$s=1$	$s=2$	$s=3$	$s=4$	$s=5$
Lena	OF	0	0	0	0	0
	UF	0	0	0	0	0
Sailboat	OF	1	1	0	0	0
	UF	0	0	0	0	0
Peppers	OF	0	0	0	0	0
	UF	182	169	132	154	180
Girl	OF	5803	5776	5886	5646	5864
	UF	19	13	27	20	17
F-16	OF	0	0	0	0	0
	UF	0	0	0	0	0

we know that data loss occurs during watermark insertion and removal. Theoretically, data loss may result from several sources such as forward and backward DWT transforms, integer rounding operation, and overflow and underflow at gray boundary. In Table II, we find that, except images with large dark regions (e.g., Peppers) or large bright regions (e.g., Girl), overflow or underflow does not occur often in images with middle gray intensity. Table I further shows that the PSNR values of normally recovered Peppers and Girl are not too much different from others. This indicates that the effect of overflow and underflow is limited in the proposed RVWS. On the other side, the error from forward and backward wavelet transform is usually trivial even 9-7 wavelet is used. Therefore, we deduce that most errors come from integer rounding operation. Practically, when the wavelet coefficients are modified and the inverse DWT is applied, the watermarked image pixels must be rounded to integer values to form a digital image.

V. CONCLUSION

The issue of removable visible watermarking has been rarely studied in the literature. This letter proposes a new algorithm for RVWS based on the requirements of a promising application. The RVWS is completely dependent on a user key mechanism. Using the user key, we can not only implement the RVWS conveniently but also ensure security of the RVWS. The easy transfer of the "vaccine" program through the Internet enables the pixel-wise varying parameters of the embedder to be resumable in the receiver end and thus makes the detection informed. The image-adaptive embedding parameters, determined by both local host characteristics and the number of unchanged neighboring host coefficients, make unauthorized watermark removal almost impossible. The experimental results have demonstrated that the legally obtained image has very high visual quality. Future efforts will focus on two aspects: finding a more suitable transform to avoid rounding operation and setting a reasonable boundary condition to make overflow/underflow value invertible during addition. One way to avoid rounding error is to use integer wavelet transform. However, it needs to be further investigated.

REFERENCES

[1] G. W. Braudaway, K. A. Margerlein, and F. C. Mintzer, "Protecting public-available images with a visible image watermark," in *Proc. SPIE Conf. Optical Security and Counterfeit Deterrence Techniques*, vol. 2659, Feb. 1996, pp. 126–132.

[2] J. Meng and S. F. Chang, "Embedding visible video watermarks in the compressed domain," in *Proc. IEEE Int. Conf. Image Processing*, vol. 1, Oct. 1998, pp. 474–477.

[3] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in *Proc. IEEE Int. Conf. Multimedia and Expo.*, vol. 2, 2000, pp. 1029–1032.

[4] Y. J. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking," *IEE Electron. Lett.*, vol. 37, no. 9, pp. 1219–1220, Sep. 2001.

[5] F. C. Mintzer, J. Lotspiech, and N. Morimoto. (1997, Dec.) Safeguarding digital library contents and users: Digital watermarking. *D-Lib Magazine* [Online]. Available: http://www.dlib.org/dlib/december97/ibm/12lotspiech.html

[6] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. Patent application, Docket No 77 102/E-D, 1999.

[7] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in *Proc. SPIE 2001, Security and Watermarking of Multimedia Contents III*, vol. 4314, P. W. Wong and E. J. Delp, Eds., pp. 197–208.

[8] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimedia*, vol. 5, no. 3, pp. 97–105, Mar. 2003.

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proc. IEEE Int. Symp. Circuits and Systems*, vol. 2, Bangkok, Thailand, May 2003, pp. 912–915.

[10] A. van Leest, M. van der Veen, and F. Bruekers, "Reversible image watermarking," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, Sep. 2003, pp. 731–734.

[11] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[12] J. Tian, "Wavelet-based reversible watermarking for authentication," in *Proc. SPIE Security and Watermarking of Multimedia Contents III*, vol. 4675, P. W. Wong and E. J. Delp, Eds., pp. 679–690.

[13] Y. J. Hu, J. Huang, S. Kwong, and Y. K. Chan, "Image fusion based visible watermarking using dual-tree complex wavelet transform," in *Proc. Int. Workshop Digital Watermarking*, vol. LNCS 2939, 2003, pp. 86–100.

[14] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor, "Visibility of wavelet quantization noise," *IEEE Trans. Image Process.*, vol. 6, no. 8, pp. 1164–1175, Aug. 1997.