Multimed Tools Appl (2013) 66:179–200
DOI 10.1007/s11042-011-0788-z

A new aspect in robust digital watermarking

Gaurav Bhatnagar · Q. M. Jonathan Wu · Balasubramanian Raman

Published online: 1 April 2011

Abstract Generally, in watermarking scheme the size of the watermark is very small when compare to host image. On the contrary, this is an attempt in which a new watermarking scheme is presented where the size of host image is very small when compare with watermark image. The core idea of the proposed scheme is to scale up the size of host image equal to the size of watermark via over-sampling and then decompose it using stationary wavelet transform. A gray scale watermark is embedded in the low frequency sub-band at the finest level using singular value decomposition. To prevent ambiguity and enhance the security, a binary watermark is also embedded in loss-less manner. Finally, a reliable watermark extraction scheme is developed for extracting both the watermarks. The experimental results demonstrate better visual imperceptibility and resiliency of the proposed scheme against intentional or un-intentional variety of attacks.

Keywords Digital watermarking · Stationary wavelet transform · Oversampling · Normalized mass matrix · Singular value decomposition

1 Introduction

In the past decade, the global rife access of internet technologies makes the communication and circulation of digital multimedia contents like images, audio

G. Bhatnagar (✉) · Q. M. J. Wu
Department of Electrical and Computer Engineering,
University of Windsor, Windsor, ON, Canada N9C 1M2
e-mail: goravdma@gmail.com

Q. M. J. Wu
e-mail: jwu@uwindsor.ca

B. Raman
Department of Mathematics, Indian Institute of Technology Roorkee,
Roorkee, 247 667, India
e-mail: balarfma@iitr.ernet.in

and video very easy. However, this convenience also causes substantial increase in illegal operations such as duplication, modification, forgery, copy-right protection and others in digital media. Therefore, the protection of digital media has become an imperative issue. Recently, digital watermarking has drawn much attention of research community to resolve these pressing problems. Digital watermarking is a technique for inserting an information into a digital media. The embedding/insertion is made in such a way that it must not cause serious degradation to the original digital media. A variety of watermarking algorithms have been proposed in the literature. These algorithms can be broadly classified in two categories according to the embedding domain: spatial and transform domain. Spatial domain approaches [17, 20, 27] are the simplest and the earliest algorithms based on the modification of pixel intensities. These algorithms are less robust against the attacks. On the other hand, transform domain approaches insert the watermark into transform coefficients, such as discrete Fourier transform (DFT) [26, 29], discrete cosine transform (DCT) [1, 4, 8, 15, 25], wavelet transform [2, 9, 16, 18, 23, 32, 33] coefficients etc.

Solachidis and Pitas [29] have presented the statistical analysis of the behavior of a blind robust watermarking system based on pseudo random signals embedded in the magnitude of the Fourier transform of the host data. Pun [26] has proposed a novel DFT-based watermarking system for images. After decomposing the host image into Fourier domain, the watermark is embedded in the Fourier coefficients with highest magnitudes except for those in the lowest one, for minimal loss in image fidelity. The blind watermark detection is achieved by computing a similarity measure between the input watermark and the Fourier coefficients of the attack image. Cox et al. [8] have presented the most popular watermarking schemes based on the Spread Spectrum Communication. The watermark is embedded into the first k highest magnitude DFT/DCT coefficients of the image and extraction is done by comparing the DFT/DCT coefficients of the watermarked and the original image. Barni et al. [1] have proposed a watermarking algorithm, which operates in the frequency domain, embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. The watermark can be reliably extracted blindly by exploiting the statistical properties of the embedded sequence. Hsu and Wu [15] have proposed the use of permuted watermark, permuted by a pseudo-random number traversing method. Finally, permuted watermark is embedded into the middle frequency of 8×8 DCT coefficient block. Piva et al. [25] have used DCT domain of full image to embed the watermark rather than some DCT coefficients. After embedding, the watermarked image is tuned according to the normalized variance of the small block.

Xia et al. [33] have added a pseudo-random sequence to the largest wavelet coefficients of the detail bands where perceptual considerations are taken into account by setting the amount of modification proportional to the strength of the coefficient itself. Watermark detection is achieved through comparison with the original un-watermarked image. Barni et al. [2] have proposed a method based on the characteristics of the human visual system operating in wavelet domain. Based on the texture and the luminance content of all image sub-bands, a mask is accomplished pixel by pixel. Zheng and Li [35] have embedded binary logos by segmenting the image into small blocks and embedding one bit of each block. Hsu and Wu [16] have presented a multilevel wavelet transformation technique in which both the host and watermark images are transformed in wavelet domain and the wavelet coefficients of watermark are added to the corresponding wavelet coefficients of host image. Wang et al. [32] have proposed a key dependent wavelet transform for watermarking. They used randomly generated orthonormal filter bank as a major part of key. Kundur and Hatizinakos [18] have proposed the use of gray scale logo as watermark. They addressed a multiresolution fusion based watermarking method for embedding gray scale logos into wavelet transformed images via salience factor. Dawei et al. [9] have proposed a new technique in which wavelet transform applies locally, based on chaotic logistic map, and embeds the watermark. This technique shows very good robustness to geometric attacks but it is sensitive to common attacks like filtering and sharpening. The detailed survey on wavelet based watermarking techniques can be found in [23].

Recently, a new transform, singular value decomposition (SVD)-based [6, 12, 13, 22] watermarking technique and its variants have been proposed. These approaches work on the simple concept of finding the SVD of a cover image or the SVD of each block of the cover image, and then modify the singular values to embed the watermark. Gorodestki et al. [13] have proposed a scheme in which the host image is first segmented into blocks of size 4 × 4 and the largest singular value of each block is quantized to embed one bit of data. Liu and Tan [22] have proposed an algorithm based on SVD. In this algorithm, authors find the singular values of the host image and then modify it by adding the watermark. SVD transform is again applied on the resultant matrix to find the modified singular values. These singular values are combined with the known component to get the watermarked image. Inverse process is used for the extraction of watermark. Chandra et al. [6] has described a method for embedding singular values of the watermark into the singular values of entire image. Recently, some researchers have presented hybrid watermarking schemes in which they have combined SVD with other existing transforms. SVD based scheme withstands a variety of attacks but it is not resistant to geometric attacks like rotation, cropping etc. Hence, for improving the performance, hybridization is needed. Ganic et al. [11] have presented hybrid-watermarking scheme based on DWT and SVD. After decomposing the cover image into four bands, SVD is applied on each band, and modify the singular values of each band with the singular values of the visual watermark. Sverdlov et al. [31] have used the same concept taking DCT and SVD. DCT coefficients are mapped into four quadrants via ZIG-ZAG scan and modify the singular values of each quadrant. Li et al. [21] have proposed the same hybrid DWT-SVD domain watermarking scheme by exploiting the properties of human visual system. Chang et al. [7] have proposed a new technique in which embedding is done in D and U components.

In this paper, a new aspect of watermarking is introduced for images. Unlike existing watermarking schemes, proposed scheme deals with the situation where the size of watermark is greater than the size of host image. First, the size of host image is scaled-up equal to the size of watermark via oversampling. Then over-sampled image is decomposed by the means of stationary wavelet transform. Then a gray scale watermark is embedded in the low frequency sub-band at finest level using singular value decomposition. Recently, some researchers show that SVD based schemes fails under ambiguity attacks [34, 36]. To prevent ambiguity and enhance the security, a binary watermark is embedded in the modified over-sampled image with the help of normalized mass matrix [3]. Finally, inverse stationary wavelet transform is performed to get the watermarked image. At the extraction end, initially binary watermark is extracted and then it is compared with the original one. The gray scale watermark is extracted if and only if the similarity between original and extracted binary watermark is greater than prescribed threshold. One of the possible practical situations for the proposed algorithm, comes from defense. Let us suppose one map is transmitted from one army station to another. The one way is to segment whole map into several parts and all parts are transmitted by using any of the existing method (where the size of host image is larger than watermark). In this case the complexity for transmitting map is very high and of course transmitting cost too. So as the possible solution, proposed algorithm transmits the whole map in only one attempt with minimum complexity and cost.

This paper is organized as follows: The description of used terminologies i.e. stationary wavelet transform, oversampling, chaotic map and singular value decomposition are explained in Section 2. The normalized mass matrix is illustrated in the Section 3 followed by the proposed embedding and extraction schemes in Section 4. The experimental results are presented in Section 5. Finally, the concluding remarks are given in Section 6.

2 Preliminaries

In this section, we provide the main terminologies which are used in the proposed algorithm to achieve the desired goal. These terminologies are as follows:

2.1 The stationary wavelet transform (SWT)

The discrete wavelet transform is the most useful and frequently used technique for frequency analysis of signals that are localized in time of space. Generally, it decomposes signals into basis functions that are dilations and translations of a single prototype wavelet function. The major inconvenience of this representation is that it does not conserve the invariance by translation which is an essential property in signal/image processing. In order to preserve the invariance by translation, stationary wavelet transform [24] is introduced by many researchers independently with different names, e.g. the undecimated wavelet transform, the invariant wavelet transform, À *trous* wavelet transform, the redundant wavelet transform and discrete wavelet frames (DWFs). The basic idea is to implement an algorithm which, in essence, removes the down-sampling operator from the usual implementation of the DWT. Low and high pass filters are applied to the signal at each level without decimation, to produce the two sequence at the next level, each have the same length as original signal. Hence, SWT is nothing but the modification in the basic scheme of the wavelet transform, each time wavelet decomposition is performed with up-sampled filters. For up-sampling of filters, a operator $\uparrow 2$ is introduced, this operator alternates a sequence with zeros, i.e. if $y = \uparrow 2(x)$ then $y_{2i} = x_i$ and $y_{2i+1} = 0$. Let us consider $g_0,\ h_0$ be the original filters used in the DWT scheme. Then for the next level, the filters are calculated in the following way:

$$g_{j+1} = \uparrow 2\ (g_j), \quad h_{j+1} = \uparrow 2\ (h_j) \tag{1}$$

Figure 1 shows the SWT analysis of a signal. SWT gives a better approximation than the wavelet transform since, it is redundant, linear and shift invariant. These properties provide the SWT to be realized using a recursive algorithm. Therefore, the SWT is very useful algorithm for analyzing the signal.

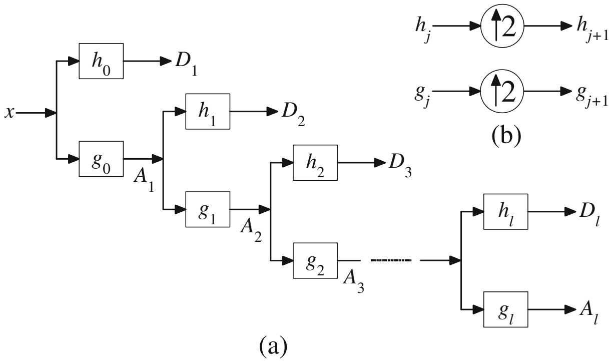


Fig. 1 **a** *l*-level stationary wavelet transform of a signal; **b** filter computation from *j*th to $j+1$th level

2.2 Oversampling

The concept of oversampling is introduced by [28] for multiple description image coding. The core idea behind oversampling is to introduce redundancy in the image. For this purpose, first DCT is applied on the image and then the desired number of rows and columns are added in the DCT transformed image. Finally, inverse DCT is applied on the modified image to get the oversampled image. These newly added rows and columns consist of zeros. Hence, the process of over-sampling is done by zero-padding in the DCT domain. The complete process is depicted in Fig. 2. To construct the original image back, the reverse process is used. First, DCT is performed on over-sampled image and then left most $M \times N$ coefficients are retained. Finally, inverse DCT is performed on retained coefficients to construct the original image. The complete process of inverse oversampling is shown in Fig. 2c. The visual assessment of oversampling is depicted in Fig. 3. In figure Barbara image of size 128 × 128 is oversampled to the sizes 512 × 256 and 512 × 512, respectively.

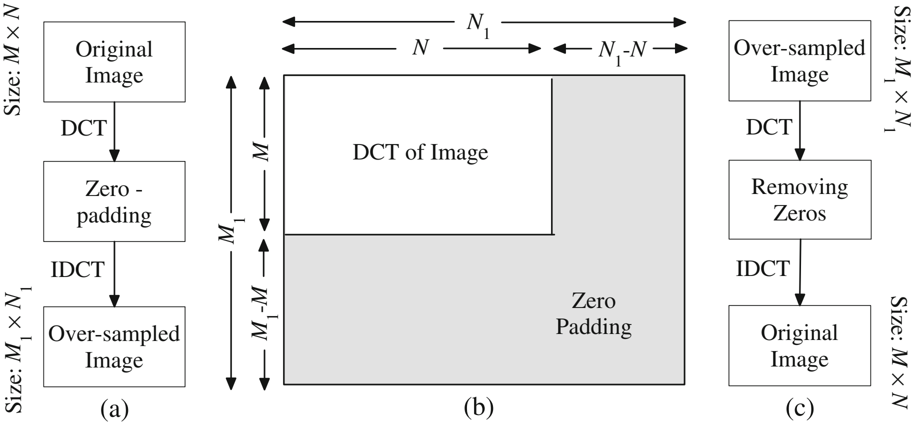


Fig. 2 **a** Process for oversampling; **b** zero-padding in DCT domain; **c** process for inverse oversampling

Figure 3d and e show the reconstructed Barbara images from both the oversampled images.

2.3 Singular value decomposition

Let A be a general real (complex) matrix of order $m \times n$. The singular value decomposition (SVD) [30] of A is the factorization

$$A = U * S * V^T \tag{2}$$

where U and V are *orthogonal(unitary)* and $S = diag(\sigma_1, \sigma_2, \ ..., \sigma_r)$, where σ_i, $i = 1(1)r$ are the singular values of the matrix A with $r = \min(m, n)$ and satisfying $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$. The first r columns of V are the *right singular vectors* and the first r columns of U are the *left singular vectors*.

Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or rectangular. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain intrinsic algebraic image properties. All the properties of SVD are summarized as follows:

- Stability: When a small perturbation is added to the matrix, large variance of its singular values does not occur.
- To some extent, singular values possess algebraic and geometric invariance.
- Rotation: given an image I and its rotated (with arbitrary angle) I^r, both have the same singular values.
- Translation: given an image I and its translated I^t, both have the same singular values.

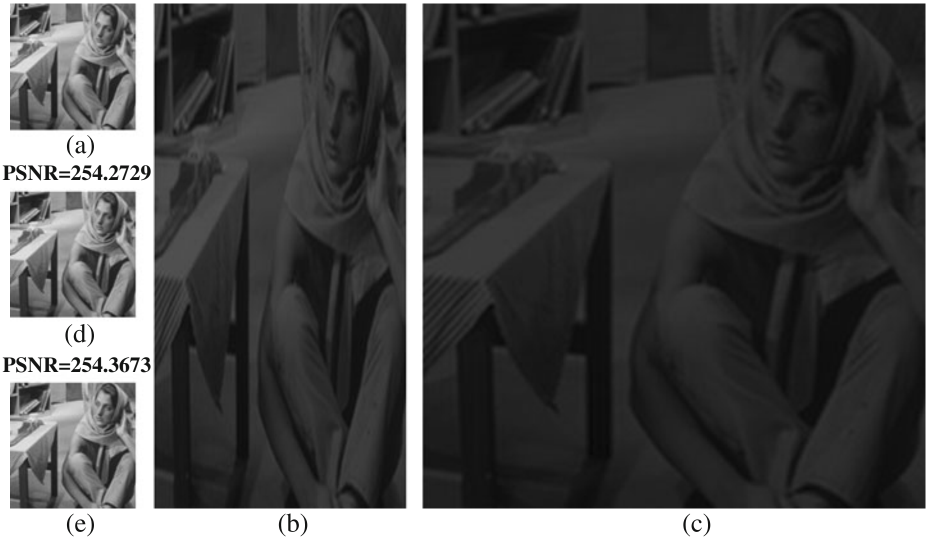


Fig. 3 Visual assessment of oversampling: **a** original Barbara image of size 128 × 128; **b** oversampled image of size 512 × 256; **c** oversampled image of size 512 × 512; **d** reconstructed Barbara image from **b**; **e** reconstructed Barbara image from **c**

- Scaling: given an image I and its scale I^s, if I has the singular values σ_i, then I^s has the singular values $\sigma_i * \sqrt{L_R L_C}$ where L_R and L_C are the scaling factors of rows and columns respectively. If rows (columns) are mutually scaled, I^s has the singular values $\sigma_i * \sqrt{L_R}(\sigma_i * \sqrt{L_C})$.

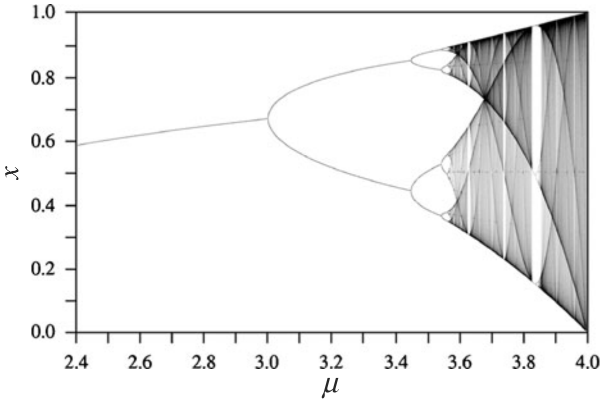
2.4 Chaotic map

Chaos is an aperiodic dynamic process having numerous excellent properties such as the ergodicity, sensitive dependence on initial conditions, random-like behaviors etc. [10, 19]. Due to these properties, chaos theory is suitable and nowadays widely used in cryptography [5]. Generally, chaos theory is represented by the chaotic system which is in the form of maps. The simplest maps are one-dimensional maps which have the advantages of high-level efficiency and implicit nature. Logistic map is one of the examples of one-dimensional map which is being widely used now. The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The map was popularized by the biologist Robert May by modifying logistic equation (the Verhulst model: a model of population growth) to a discrete quadratic recurrence relation. Mathematically, logistic map is described as

$$x_{i+1} = \tilde{F}(x_i, \mu) \Rightarrow x_{i+1} = mux_i(1 - x_i), i = 0, 1, ... \tag{3}$$

where $x_n \in (0, 1)$, $\mu > 0$ is the parameter which control the chaotic nature of the map and x_0 is the initial condition for the map. Thus, given initial condition x_0 and parameter μ, one sequence $\{x_i\}_{i=0}^{\infty}$ is obtained and refers to the orbit of the map corresponding to (x_0, μ). In order to see the restrictions on μ, the bifurcation diagram of logistic map is considered which is depicted in Fig. 4. Bifurcation diagram is a plot shows the possible long-term values (equilibria/fixed points or periodic orbits) of a system as a function of a parameter (μ) in the system. For $\mu \in [0, 1]$, the trivial solution is the only fixed point where as a non-trivial fixed point is the

Fig. 4 Bifurcation diagram for logistic map



solution when $\mu \in (1, 3]$. The map exhibits the phenomenon of periodic doubling for $\mu \in (3, 3.57]$ and the chaos appears when $\mu \in (3.57, 4]$. Therefore this range is said to be chaotic region for logistic map. Finally, for $\mu = 4$, the generated chaos values cover the whole range of (0, 1).

3 Normalized mass matrix

The concept of normalized mass matrix is introduced by [3] for digital watermarking. Authors have used the fact comes from the heart of physical science that every existing object in the universe has its own mass. Mass of an image is first defined by [14]. Mass is the determining factor of the substance contained in the object. If a discrete rectangular co-ordinate system is considered then every individual point of the system has unique mass. Let us suppose, the system contains n points having co-ordinates $(x_i,\ y_i)$ and mass m_i, where $i = 1(1)n$. Then the total mass of the system is defined as:

$$M = \sum_{i=1}^{n} m_i \tag{4}$$

In a similar way, the mass is also defined for grayscale images because grayscale images are regarded as discrete rectangular system. Let I be a grayscale image of size $m \times n$ and the corresponding rectangular system is defined as follows (Fig. 5):

- (0, 0) i.e. the origin corresponds to left corner of the image.
- (m, n) corresponds to the right upper corner of the image.
- $I(i,\ j)$ be the intensity at position $(i,\ j)$.

Now, the mass at each position or pixel is given by the corresponding intensity. Hence, total mass of the image is given by

$$M = \sum_{i=1}^{m} \sum_{j=1}^{n} I(i,\ j) \tag{5}$$

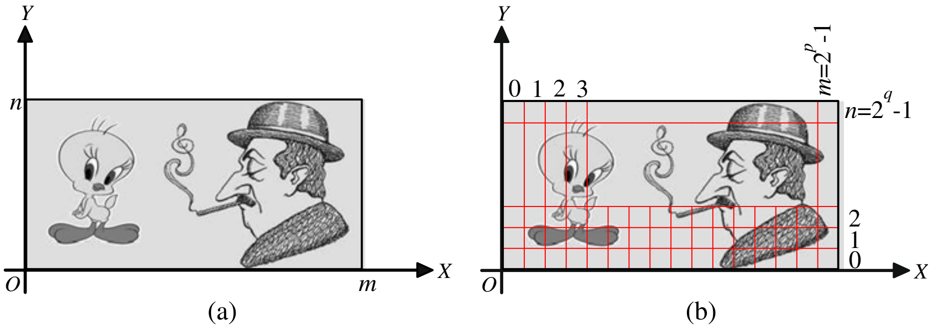


Fig. 5 **a** Image in coordinate system; **b** discretization of an image

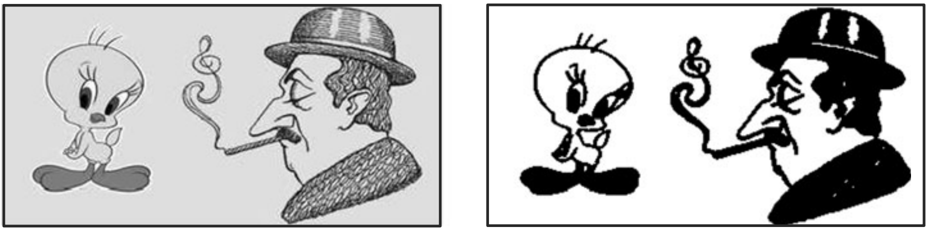

(a) (b)

Fig. 6 **a** Original image; **b** corresponding normalized mass matrix

The normalized mass matrix of an image is calculated by following three steps:

Step 1 Find the existing average mass within the moving window of size $S_p \times S_p$ centered at the pixel. Let us denote the average mass matrix by $\widetilde{M}$.

$$\widetilde{M}_{i,j} = \frac{1}{S_p \times S_p} \sum_{x=i-\frac{S_p}{2}}^{i+\frac{S_p}{2}} \sum_{y=j-\frac{S_p}{2}}^{j+\frac{S_p}{2}} I(x, y) \tag{6}$$

Step 2 Calculate total average mass of the image

$$M = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} I(i, j) \tag{7}$$

Step 3 Finally, normalized mass matrix is formed by the following equation

$$\mathcal{M}_{i,j} = \begin{cases} 1, & \widetilde{M}_{i,j} \geq M \\ 0, & \widetilde{M}_{i,j} < M \end{cases} \tag{8}$$

Figure 6 gives the visual assessment of the normalized mass matrix of an image.

4 Proposed watermarking algorithm

In this section, we discuss some motivating factors in design of our approach to watermarking. The proposed algorithm uses two watermarks out of which one is gray scale logo whereas second is binary image. The initial watermarks used for embedding are bigger in the size when compared with the host image. With out loss of generality, assume that G represents the host image of size $M \times N$, W_1 and W_2 represent the initial watermarks of size $M_1 \times N_1$ and the host image is smaller than the watermarks by a factor 2^{Q_1} and 2^{Q_2} along both the directions, where Q_1 and Q_2 are any integers greater than or equal to 1.

4.1 Watermark embedding algorithm

The embedding algorithm to embed gray scale logo and binary image is formulated as follows:

1. The size of host image is scaled-up equal to the size of watermarks via oversampling, denoted by $G_o = F$.
2. Perform L-level stationary wavelet transform on F, which is denoted by f_l^{θ}, where $\theta \in \{ \text{A, H, V, D} \}$ and $l \in [1, L]$.
3. *Embedding gray scale logo*: The gray scale logo (W_1) is embedded in the low frequency sub-band at the finest level i.e. f_L^A and the process is formulated as follows:

   (a) Perform SVD on both f_L^A and W_1

   $$f_L^A = U_{f_L^A}\ S_{f_L^A}\ V_{f_L^A}^T, \quad W_1 = U_{W_1}\ S_{W_1}\ V_{W_1}^T \tag{9}$$

   (b) Modify the singular values of the sub-band with the help of watermark singular values as

   $$S_{f_L^A}^* = S_{f_L^A} + \alpha\ S_{W_1} \tag{10}$$

   where α gives the watermark strength.

   (c) Perform inverse SVD to construct modified sub-band

   $$f_L^{A,\text{ new}} = U_{f_L^A}\ S_{f_L^A}^*\ V_{f_L^A}^T \tag{11}$$

4. Perform L-level inverse stationary wavelet transform on the modified oversampled image $G_o^{\text{new}} = F^{\text{new}}$.
5. *Embedding binary image*: The binary image (W_2) is embedded as follows:

   (a) Adopting k_0, μ and $\ell(> M_1 \times N_1)$ as keys, iterate logistic map ℓ times to generate a stochastic sequence, say k.

   (b) Map K into the stochastic integer sequence as

   $$K^{\text{int}} = (\ell * K) \mod 255 \tag{12}$$

   where $(*)$ is the basic rounding operation.

   (c) Stack the last $m \times n$ values of stochastic integer sequence (K^{int}) in an array, say $\mathcal{K}$.

   (d) The modified oversampled image (G_o^{new}) is mapped to a reference image with the help of $\mathcal{K}$ as

   $$G_{o,\text{ref}}^{\text{new}} = \left(G_o^{\text{new}} + \mathcal{K}\right) \mod 255 \tag{13}$$

   (e) Find the normalized mass matrix corresponding to $G_{o,\text{ref}}^{\text{new}}$, denoted by $\mathcal{M}_{G_o^{\text{new}}}$

   (f) Produce the extraction key using bit-wise exclusive-OR operation as:

   $$K_{ext} = XOR(\mathcal{M}_{G_{o,\text{ref}}^{\text{new}}}, W_2) \tag{14}$$

   After the extraction key K_{ext} is constructed, the embedding process is completed. Obviously, G_o^{new} also remains unchanged during this embedding.

6. Perform inverse over-sampling process to get the watermarked image G^{new}.

4.2 Watermark extraction algorithm

The objective of the watermark extraction algorithm is to obtain the estimate of the original watermark. For binary watermark extraction, only key K is required whereas for gray scale logo extraction, host and watermarked images, V_{W_1} and U_{W_1} are required. Hence, the binary watermark extraction is blind and gray-scale watermark extraction is non-blind. The main reason behind the non-blind extraction is the embedding of the gray-scale logo/image as watermark. Generally in the blind watermarking scheme, a binary or Gaussian noise type watermark is embedded. Further, We cannot predict actual intensity at any pixel by just comparing the correlation (between watermarked and watermark image) with the prescribed threshold as we do in the blind watermarking scheme which uses a binary or Gaussian noise type watermarks. Hence, the gray-scale watermark extraction is non-blind. The extraction process is formulated as follows:

1. The size of watermarked image is scaled-up equal to the size of watermarks via over-sampling, denoted by $Gw_o = Fw$.
2. *Extracting binary image*: The binary image is extracted as follows:
   (a) By adopting Steps 5(a)–(d), the array $\mathcal{K}$ is obtained.
   (b) The reference image is obtained from watermarked oversampled image and $\mathcal{K}$ as
   $$Fw_{\text{ref}} = (Fw + \mathcal{K}) \mod 255 \tag{15}$$
   (c) Find the normalized mass matrix corresponding to Fw_{ref}, denoted by $\mathcal{M}_{Fw_{\text{ref}}}$.
   (d) The binary watermark is extracted using bit-wise exclusive-OR operation as:
   $$W_2^{\text{ext}} = XOR(\mathcal{M}_{Fw_{\text{ref}}}, K_{\text{ext}}) \tag{16}$$
3. *Extracting gray scale logo*: This extraction is performed if and only if the similarity between extracted (from previous step) and original binary watermark is greater than the prescribed threshold. Extraction process is described as follows:
   (a) Perform L-level stationary wavelet transform on Fw, which is denoted by fw_l^θ, where $\theta \in \{ \text{A, H, V, D} \}$ and $l \in [1, L]$.
   (b) Select the low frequency sub-band at the finest level i.e. fw_L^A to extract the gray scale logo.
   (c) Perform SVD on fw_L^A
   $$fw_L^A = U_{fw_L^A}\, S_{fw_L^A}\, V_{fw_L^A}^T \tag{17}$$
   (d) Extract the singular values of gray scale logo as
   $$S_{W_1}^{\text{ext}} = \frac{S_{fw_L^A} - S_{f_L^A}}{\alpha} \tag{18}$$
   (e) Perform inverse SVD to construct the extracted gray scale logo.
   $$W_1^{\text{ext}} = U_{W_1}\, S_{W_1}^{\text{ext}}\, V_{W_1}^T \tag{19}$$

5 Results and discussions

5.1 Experimental setup

The robustness of the proposed watermarking algorithm is demonstrated using MATLAB platform and different grayscale images namely Barbara, Lena, Mandril and Parrot of size 128 × 128 are used as the host images. For gray scale logo watermarks, Peacock, Cock, Tweety and Man images of size 512 × 512 are used whereas Circle, IEEE logo, CVGIP LAB logo and Star are used as binary watermarks. Peacock and Circle watermarks are embedded into Barbara image while Cock and IEEE watermarks are embedded into Lena image. Tweety and CVGIP LAB watermarks are embedded into Mandril image. Man and star watermarks are embedded into Parrot image. The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio). The watermarked Barbara, Lena, Mandril and Parrot images are having 34.8963, 31.1209, 32.3523 and 33.6999 PSNR values (in dB), respectively. In Fig. 7, all original host, watermarked, original watermark and extracted watermark images are shown. From the figure, it is clear that there is not any perceptual degradation between the original and the watermarked images according to human perception. The value of watermark strength (α) is calculated by attempting several experiments on the host image considering human visual system. For this purpose, watermark images are prepared with the different values of α and some human observers are asked to view the series of watermarked images and rate them. The value of α is taken to be optimal for which most of the observers fail to distinguish the original and watermarked image. For further analysis, Barbara and Lena images are used, since these images are having maximum and minimum PSNR values among all test images.

To verify the presence of the watermark, the correlation coefficient between the original and the extracted singular values is given by

$$\rho(w, \bar{w}) = \frac{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1} (w(i) - \mu_w)\,(\overline{w}(i) - \overline{\mu}_w)}{\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1} (w(i) - \mu_w)^2}\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1} (\overline{w}(i) - \overline{\mu}_w)^2}} \tag{20}$$

where w, $\overline{w}$, μ_w and $\overline{\mu}_w$ are the original, extracted, mean of original and extracted watermarks. ρ is the number that lies between $[-1, 1]$. If the value of ρ is equal to 1 then the extracted singular values are just equal to the original one, if it is -1 then the constructed watermark looks like a negative thin film. According to statistics, the principle range for correlation coefficient is [0, 1]. Hence, the Negative Image Transform (NIT) is performed on the extracted watermark whenever ρ takes negative value, in order to get ρ in the principle range. The NIT with intensity levels in the range $[0, L - 1]$ is given by the expression $s = L - 1 - r$, where r is the original intensity and s is the transformed intensity. In the proposed scheme, the gray-scale watermark extraction is performed if and only if the similarity between extracted and original binary watermark is greater than the prescribed threshold (T_s) i.e. if

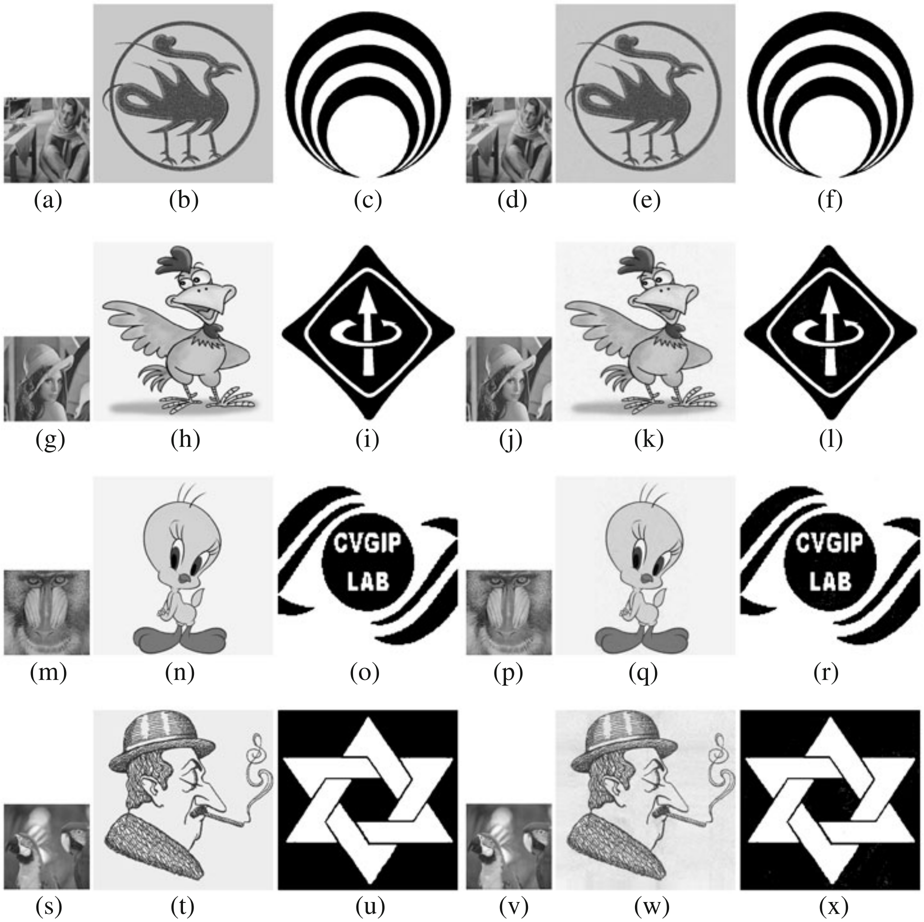


Fig. 7 **a**, **g**, **m**, **s** Original host; **b**, **h**, **n**, **t** original gray-scale watermark; **c**, **i**, **o**, **u** original binary watermark; **d**, **j**, **p**, **v** watermarked; **e**, **k**, **q**, **w** extracted gray-scale watermark; **f**, **l**, **r**, **x** extracted binary watermark images

$\rho(W_2, W_2^{\text{ext}}) > T_s$. In our experiments, the threshold for binary watermark extraction is $T_s = 0.6$.

5.2 Threshold determination

In the proposed watermarking algorithm, the threshold value plays an important role for the extraction of gray-scale watermark. Since, the gray-scale extraction is performed if and only if the similarity between extracted and original binary watermark is greater than the prescribed threshold. To determine the threshold, the most common criterion is the Neyman-Pearson criterion i.e. the probability minimization of missing the watermark subject to a given false detection rate. In this way, robustness against attacks is augmented and detection is accomplished without any knowledge about the watermark strength. Given an image and a watermark, only three cases are possible.

Case A image is not watermarked.
Case B image is watermarked with a watermark other than given watermark.
Case C image is watermarked with the given watermark.

Now, after applying statistical decision theory one threshold is obtained subject to some assumptions on the random variables forming the observation variable. But in the proposed algorithm, Neyman–Pearson criterion and statistical theory can not applied to construct the threshold for binary watermark extraction. The main reason behind our words is the loss-less embedding. The meaning of loss-less embedding is that all the pixel of the host image remains unchanged during embedding. By using Neyman–Pearson criterion, we always lie in the Case A i.e. the image is not watermarked. As a result, an appropriate threshold is not obtained for binary watermark extraction using conventional theory. Hence, one must look for some other method to obtain an appropriate threshold. Here, a new method is proposed for these types of situation where the embedding is loss-less.

The core idea of the proposed solution is to determine threshold experimentally. For this purpose, n random binary matrices are generated and embedded in the host image by the proposed algorithm. In each case, the watermark is extracted and ρ is calculated between the original binary watermark and the extracted binary matrix. Then the maximum value of ρ is considered as a desired threshold T_s. In this manner, the obtained threshold value should maintain a balance between binary watermark extraction and robustness.

In experiments, 25,000 binary matrices are generated randomly and embedded in the host image by the proposed algorithm. In each case, the watermark is extracted

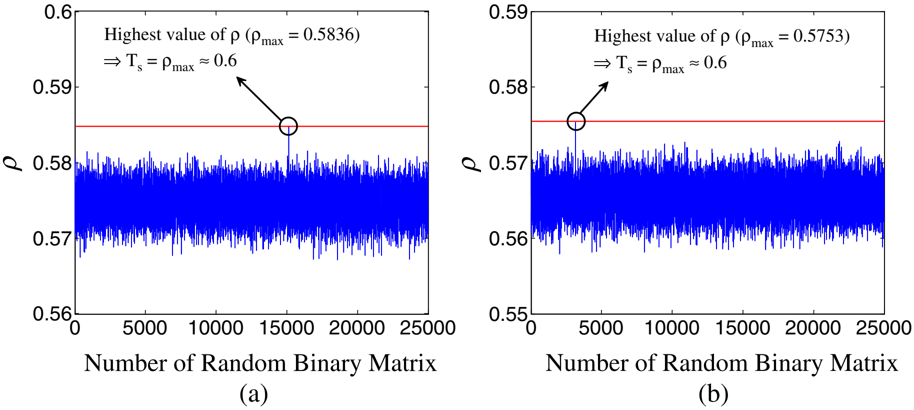


Fig. 8 Selection procedure for threshold with **a** Barbara; **b** Lena images

and ρ is calculated between the original and the extracted binary matrix. Finally, a graph is plotted (see Fig. 8) by taking the number of binary matrices on x-axis and the corresponding ρ on y-axis. The corresponding highest value (i.e. the highest peak on plot) is taken as the optimal value for threshold. Hence, for the proposed method the threshold value is taken to be 0.6.

5.3 Attack analysis

We investigate the robustness of the algorithm by considering average and median filtering, Gaussian noise addition, JPEG compression, resize, cropping, rotation, histogram equalization, row and column deletion, sharpen and contrast adjustment attacks on the watermark image. The used parameters in the experiments for all attacks mentioned above are summarized in Table 1. After these attacks on the watermarked image, extracted watermarks are compared with the original one. The rest of attack analysis is done by considering Barbara image because it has maximum PSNR among all experimental images. In Fig. 9, attacked watermarked Barbara images are shown. The detailed description of attack analysis is as follows.

The most common manipulation in digital image is filtering. The watermarked image is filtered by average and median filtering considering 13 × 13 window and watermark is then extracted from attacked images. Another most common method to estimate the robustness of watermark is the addition of noise. In many cases, the degradation and distortion of the image are due to noise addition. Robustness against additive noise is estimated by degrading watermark image by adding 100% Gaussian noise randomly. The meaning of 100% noise is that the means of additive gaussian noise is zero and variance is 1. It is clear from the Fig. 9c that almost all information is lost after this attack but the extracted watermarks are still recognizable. To check the robustness against Image Compression, the watermarked image is attacked by JPEG compression attack. The extracted watermark logo from compressed Watermarked host image using JPEG compression with compression ratio 100. Enlargement or reduction is commonly performed to fit the image into the desired size and there is information loss of the image including embedded watermarks. Hence, the proposed technique is also tested for resizing attack. For doing this task, the size of watermarked host image is first reduced to 2 × 2 and then carried back to its

Table 1 Parameters used in experiments

Attacks	Parameters
Average filtering	13 × 13
Median filtering	13 × 13
Gaussian noise addition	100%
JPEG compression	100:1
Resizing	128 → 4 → 128
Cropping	2.5% area remaining
Rotation	30°
Row–col deletion	Randomly delete 20 rows and columns
Sharpen	increased by 80%
Contrast adjustment	decreased by 80%

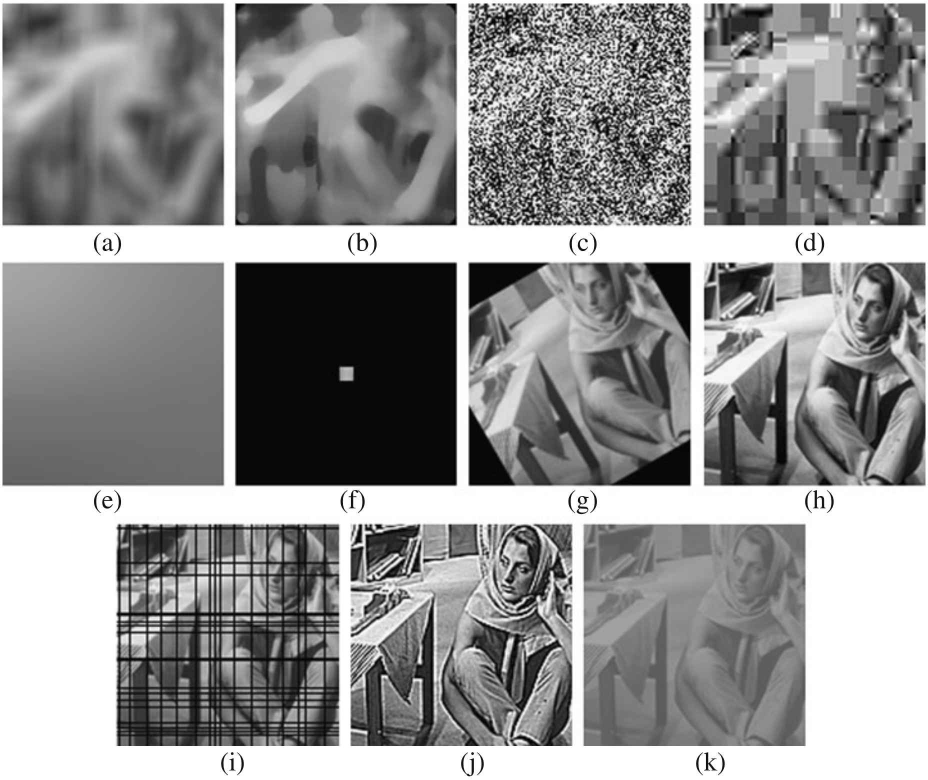


Fig. 9 Watermarked images after **a** average filtering (13 × 13); **b** median filtering (13 × 13); **c** Gaussian noise addition (100%); **d** JPEG compression (100:1); **e** resize (128 → 4 → 128); **f** cropping (2.5% area remaining); **g** rotation (30°); **h** histogram equalization; **i** row–column deletion (randomly delete 20 rows and 20 columns); **j** sharpen (increased by 80%); **k** contrast adjustment (decreased by 80%)

original size i.e. 128 × 128 followed by the watermark extraction. Image cropping is another most common manipulation in digital image. To check the robustness against Image Cropping, the 97.5% area of the watermarked image is cropped and then watermark is extracted. Figure 9e and f gives the attacked images after resizing and cropping where lot of information has lost but extracted watermarks are recognize well. In the case of cropping, grayscale watermark is distorted but one can easily get the overview of the watermark. The proposed technique is also tested for rotation attack. For this purpose, the watermarked image is rotate with 30° (see Fig. 9g). The proposed algorithm is also checked against row and column deletion attack. In row and column deletion attack, some rows and columns are randomly selected followed by their deletion. In the experiments, we have selected and deleted 20 rows and 20 columns randomly. Further, the proposed watermarking scheme is also tested for histogram equalization, sharpen and contrast adjustment attacks. For sharpen attack, the sharpness of the watermarked image is increased by the 80% whereas

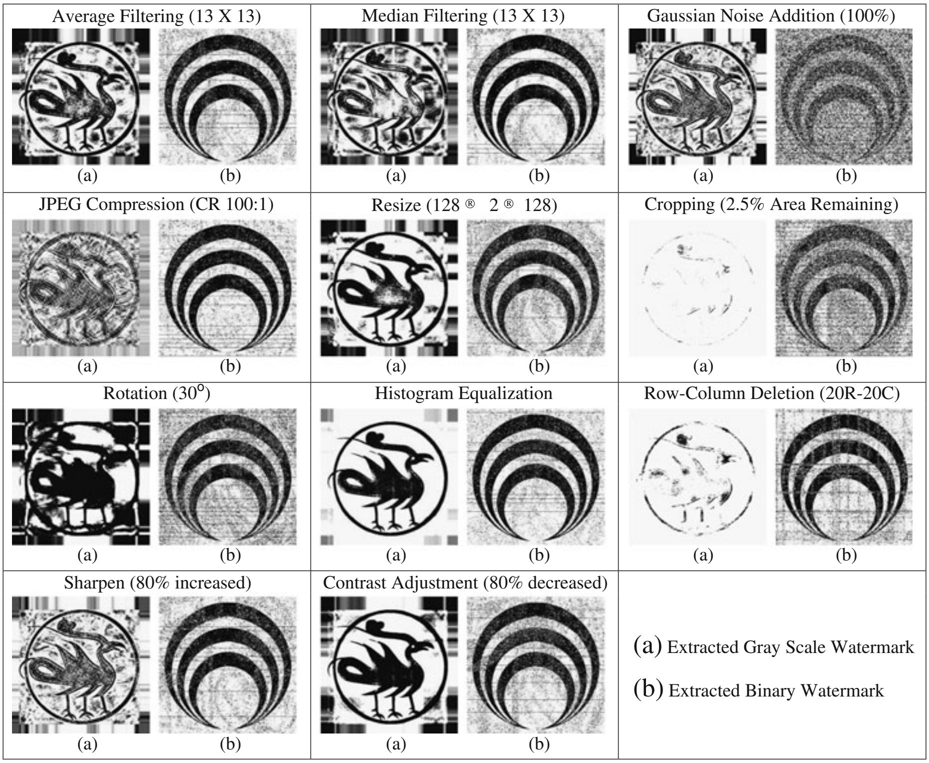

Average Filtering (13 X 13)
(a)
(b)
Median Filtering (13 X 13)
(a)
(b)
Gaussian Noise Addition (100%)
(a)
(b)
JPEG Compression (CR 100:1)
(a)
(b)
Resize (128 ® 2 ® 128)
(a)
(b)
Cropping (2.5% Area Remaining)
(a)
(b)
Rotation (30°)
(a)
(b)
Histogram Equalization
(a)
(b)
Row-Column Deletion (20R-20C)
(a)
(b)
Sharpen (80% increased)
(a)
(b)
Contrast Adjustment (80% decreased)
(a)
(b)
(a) Extracted Gray Scale Watermark
(b) Extracted Binary Watermark

Fig. 10 Extracted **a** gray-scale; **b** binary watermarks from Barbara image after attacks

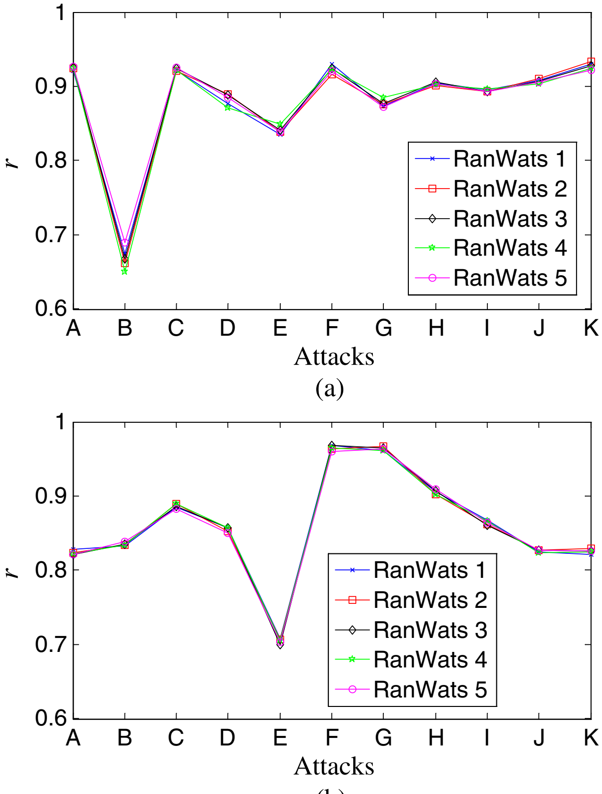
Table 2 Correlation coefficients for the extracted watermarks

Attacks	Images							
	Barbara		Lena		Mandrill		Parrot	
	Binary	Gray scale	Binary	Gray scale	Binary	Gray scale	Binary	Gray scale
No attack	0.9983	0.9999	0.9989	0.9998	0.9989	0.9999	0.9985	0.9997
Average filtering	0.9250	0.8220	0.9285	0.8205	0.9291	0.8265	0.9249	0.8237
Median filtering	0.6956	0.8309	0.6501	0.8365	0.6856	0.8362	0.6719	0.8278
Gaussian noise addition	0.9274	0.8825	0.9134	0.8865	0.9213	0.8859	0.9210	0.8823
JPEG compression	0.8716	0.8518	0.8847	0.8515	0.8770	0.8544	0.8814	0.8579
Resizing	0.8418	0.7060	0.8303	0.7024	0.8394	0.7026	0.8443	0.7049
Cropping	0.9241	0.9642	0.9198	0.9637	0.9279	0.9668	0.9268	0.9689
Rotation	0.8813	0.9670	0.8758	0.9647	0.8746	0.9665	0.8808	0.9641
Histogram equalization	0.9012	0.9090	0.9058	0.9044	0.9078	0.9049	0.9082	0.9074
Row–column deletion	0.8936	0.8651	0.8975	0.8659	0.8942	0.8681	0.8956	0.8606
Sharpen	0.9083	0.8261	0.9057	0.8255	0.9024	0.8252	0.9091	0.8266
Contrast adjustment	0.9250	0.8244	0.9249	0.8240	0.9255	0.8215	0.9249	0.8243

the contrast of the watermarked image is decreased by 80% for contrast adjustment attack. The extracted watermarks after all these attacks are given in Fig. 10 and the corresponding correlation coefficient values are given in Table 2. Table 2 shows the improved performance in terms of imperceptibility and robustness against different kind of attacks.

5.4 Effect of watermark images on the robustness

In this section, we essentially prove that the change in the watermark images cannot cause any serious effect on the robustness. For this purpose, different watermarks are embedded in the same host image (Barbara image) followed by the attack analysis. Four grayscale watermarks are selected namely Peacock, Cock, Tweety and Man images whereas Circle, IEEE logo, CVGIP LAB logo and Star are selected as binary watermarks. One grayscale and one binary watermark are randomly selected from these watermarks and embedded in the Barbara image followed by the attack analysis and the comparison among them. This process is done five times i.e. grayscale and binary watermarks are selected randomly five times in the Barbara image followed by the attack analysis. Let us assume these pairs of watermarks are denoted by {RanWats i : $i = 1, 2, 3, 4, 5$}. After attacks on the watermarked



(a)

(b)

Fig. 11 Effect of watermark images on the robustness: correlation coefficients of extracted **a** gray-scale; **b** binary watermarks from Barbara image after attacks (*A* average filtering, *B* median filtering, *C* Gaussian noise addition, *D* JPEG compression, *E* resizing, *F* cropping, *G* rotation, *H* histogram equalization, *I* row–column deletion, *J* sharpen, *K* contrast adjustment; {RanWats $i : i = 1, 2, 3, 4, 5$} is the randomly selected watermarks pair)

Table 3 Trend for grayscale and binary watermarks on the robustness of proposed technique

Attacks	Attack parameters	Trend for watermark extraction	
		Binary	Grayscale
Average filtering	13 × 13	$\rho \in [0.920, 0.930]$	$\rho \in [0.820, 0.835]$
Median filtering	13 × 13	$\rho \in [0.668, 0.690]$	$\rho \in [0.820, 0.835]$
Gaussian noise addition	100%	$\rho \in [0.910, 0.930]$	$\rho \in [0.873, 0.890]$
JPEG compression	100:1	$\rho \in [0.869, 0.880]$	$\rho \in [0.850, 0.861]$
Resizing	128 → 4 → 128	$\rho \in [0.829, 0.837]$	$\rho \in [0.700, 0.710]$
Cropping	2.5% area remaining	$\rho \in [0.908, 0.926]$	$\rho \in [0.960, 0.973]$
Rotation	30°	$\rho \in [0.871, 0.884]$	$\rho \in [0.961, 0.970]$
Row–col deletion	Randomly delete 20R & 20C	$\rho \in [0.893, 0.912]$	$\rho \in [0.860, 0.871]$
Sharpen	Increased by 80%	$\rho \in [0.898, 0.903]$	$\rho \in [0.820, 0.832]$
Contrast adjustment	decreased by 80%	$\rho \in [0.921, 0.930]$	$\rho \in [0.821, 0.835]$

images, both the watermarks are extracted and compared with the original ones. The behavior of the proposed technique with the different watermarks is depicted in the Fig. 11. Figure 11a shows the trend for grayscale watermark whereas Fig. 11b shows the trend for binary watermark extraction. It is clear from the figure that there is very less/negligble perturbation in the extracted watermarks due to the change in the watermark images. The complete trend for both grayscale and binary watermarks extraction is depicted in the Table 3.

6 Conclusions

In this paper, a new watermarking scheme is presented for dealing the situation where the size of watermark is very big when compare to host image. To prevent ambiguity and enhance the security, two watermarks are embedded in the host image where both the watermarks are visually meaningful image instead of noise type Gaussian sequences. Among these watermarks one is gray-scale and another is binary image. Finally, a reliable watermark extraction is developed, to extract both the watermarks. Robustness of this method is carried out by a variety of attacks. It is observed that the quality of the image degradation is directly proportional to the quality of the extracted logo. Moreover no attacker can extract the data without accessing the original image. Hence, we can say that the security of the proposed method lies in the original image.

References

1. Barni M, Bartonlini F, Cappellini V, Piva A (1998) A DCT domain system for robust image watermarking. Signal Process 66(3):357–372
2. Barni M, Bartonlini F, Piva A (2001) Improved wavelet based watermarking through pixel wise masking. IEEE Trans Image Process 10(5):783–791
3. Bhatnagar G, Raman B (2008) Robust watermarking scheme based on multiresolution fractional Fourier transform. In: Proc. of Indian conference on computer vision, graphics and image processing, Bhubaneshwar, India, pp 1–8
4. Bors AG, Pitas I (1998) Image watermarking using block site selection and DCT domain constraints. Optics Exp 3(12):512–523

5. Carroll JM, Verhagen J, Wong PT (1992) Chaos in cryptography: the escape from the strange attractor. Cryptologia 16(1):52–72
6. Chandra DVS (2002) Digital image watermarking using singular value decomposition. In: Proc. of IEEE midwest sym. on circuits and systems, Phoenix, AZ, pp 264–267
7. Chang CC, Tsai P, Lin CC (2005) SVD-based digital image watermarking scheme. Pattern Recogn Lett 26(10):577–1586
8. Cox IJ, Killian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
9. Dawei Z, Guanrong C, Wenbo L (2004) A chaos-based robust wavelet-domain watermarking algorithm. Journal of Chaos Solitons Fractals 22(1):47–54
10. Devaney RL (2003) An introduction to chaotic dynamical systems. Westview Press, Colorado
11. Ganic E, Eskicioglu AM (2005) Robust embedding of visual watermarks using DWT-SVD. J Electron Imag 14:043004
12. Ganic E, Zubair N, Eskicioglu AM (2003) An optimal watermarking scheme based on singular value decomposition. In: Proc. of the IASTED international conference on communication, network, and information security, Uniondale, NY, pp 85–90
13. Gorodetski VI, Popyack LJ, Samoilov V, Skormin VA (2001) SVD-based approach to transparent embedding data into digital images. In: Proc. of international workshop on mathematical methods, models and architectures for computer network security. St. Petersburg, Russia
14. Han H, Yao H, Liu S, Liu Y (2005) A fragile image watermarking based on mass and centroid. Lect Notes Comput Sci 3333:441–448
15. Hsu CT, Wu JL (1996) Hidden signatures in images. In: Proc. of international conference of image processing, Lausanne, vol 3, pp 223–226
16. Hsu CT, Wu JL (1998) Multiresolution watermarking for digital images. IEEE Trans Circuits Syst 45(8):1097–1101
17. Hwang MS, Chang CC, Hwang KF (1999) A watermarking technique based on one-way hash functions. IEEE Trans Consum Electron 45(2):286–294
18. Kundur D, Hatizinakos D (2004) Towards robust logo watermarking using multi-resolution image fusion. IEEE Trans Multimedia 6(1):185–197
19. Lasota A, Mackey MC (1997) Chaos, fractals, and noise-stochastic aspects of dynamics. Springer, New York
20. Lee YK, Chen LH (2000) High capacity image steganographic model. IEE Proc Vis Image Signal Proces 147(3):288–294
21. Li Q, Yuan C, Zong YZ (2007) Adaptive DWT-SVD domain image watermarking using human visual model. In: Proc. of international conference on advanced communication technology, Phoenix Park, Gangwon-Do, Republic of Korea, pp 1947–1951
22. Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 4(1):121–128
23. Meerwald P, Uhl A (2001) A survey of wavelet-domain watermarking algorithms. In: Proc. of SPIE, electronic imaging, security and watermarking of multimedia contents III, San Jose, CA, USA, pp 4314
24. Nason GP, Silverman BW (1995) The stationary wavelet transform and some statistical applications. Notes Stat 108:281–289
25. Piva A, Barni M, Bartonlini F, Cappellini V (1997) DCT-based watermarking recovering without restoring to the uncompressed original image. In: Proc. of IEEE international conference on image processing, Washington, DC, USA, vol 1, pp 520–523
26. Pun CM (2006) A novel DFT-based digital watermarking system for images. In: Proc. of international conference of signal processing, Vienna, Austria, vol 2, pp 1–4
27. Schyndle RGV, Trikel AZ, Osbrone CF (1994) A digital watermark. In: Proc. of IEEE international conference on image processing, Austin, Texas, vol 2, pp 86–90
28. Shirani S, Gallant M, Kossentini F (2001) Multiple description image coding using pre- and post-processing. In: Proceedings of international conference on information technology: coding and computing, Las Vegas, Nevada, pp 35–39
29. Solachidis V, Pitas I (2004) Optimal detector for multiplicative watermarks embedded in the DFT domain of non-white signals. EURASIP J Appl Signal Process 2004:2522–2532
30. Strang G (1993) Introduction to linear algebra. Wellesley-Cambridge Press
31. Sverldov A, Dexter S, Eskicioglu AM (2005) Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies. In: Proc. of European signal processing conference, Antalya, Turkey. http://www.eurasip.org/Proceedings/Eusipco/Eusipco2005/defevent/abstract/a1023.pdf

32. Wang Y, Doherty JF, Van-dyck RE (2002) A wavelet based watermarking algorithm for ownership verification of digital images. IEEE Trans Image Process 11(2):77–88
33. Xia X, Boncelet CG, ARCE GR (1997) A multiresolution watermark for digital images. In: Proc. of IEEE international conference on image processing, Washington, DC, USA, vol 3, pp 548–551
34. Yavuz E, Telatar Z (2007) Improved SVD-DWT based digital image watermarking against watermark ambiguity. In: Proc. of ACM symposium on applied computing, Seoul, Korea, pp 1051–1055.
35. Zeng BLW, Lei S (1999) Extraction of multiresolution watermark images for resolving rightful ownership. In: Proc. of SPIE, security and watermarking of multimedia contents, San Jose, CA, vol 3657, pp 404–414
36. Zhang XP, Li K (2005) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 7(2):593–594

Gaurav Bhatnagar is the member of the Computer Vision and Sensing Systems Laboratory in the Department of Electrical and Computer Engineering at University of Windsor since 2009. He received his BSc from C.C.S. University in 2003 and MSc in Applied Mathematics from Indian Institute of Technology Roorkee in 2005. He has submitted his PhD from Indian Institute of Technology Roorkee, India in 2009. So far he has published one book chapter, eight international journals and 14 conference proceedings. His areas of research include digital watermarking, image analysis, image fusion, biometrics, wavelet analysis and cryptography.

Q. M. Jonathan Wu received the PhD degree in electrical engineering from the University of Wales, Cardiff, UK, in 1990. In 1995, he joined the National Research Council of Canada, Ottawa, ON, Canada, where he was a senior research officer and group leader. He is currently a full professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON. He is a holder of the Canada Research Chair in automotive sensors and sensing systems. He is the author of over 100 published scientific papers in the areas of computer vision, neural networks, fuzzy systems, robotics, micro sensors and actuators, and integrated Microsystems. Dr. Wu is an associate editor for the *IEEE Transactions on Systems Man and Cybernetics—Part A: Systems and Humans*. His current research interests include 3-D image analysis, active video object extraction, vision-guided robotics, sensor analysis and fusion, wireless sensor networks, multimedia security and integrated microsystems.

Balasubramanian Raman is an assistant professor in the Department of Mathematics at Indian Institute of Technology Roorkee since February 2006. He received his PhD in Mathematics from Indian Institute of Technology, Madras, India in 2001. He received his BSc and MSc in Mathematics from University of Madras in 1994 and 1996, respectively. So far he has published 26 international journals, 41 conference proceedings, four book chapter and a technical report. His areas of research include computer vision, graphics, satellite image analysis, scientific visualization, imaging geometry, reconstruction problems, biometrics and watermarking.