Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-019-03751-8

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Robust Invisible Digital Image Watermarking Using Hybrid Scheme

Dayanand G. Savakar[1] · Anand Ghuli[2,3]

Received: 19 July 2018 / Accepted: 2 February 2019

Abstract

Digital image watermarking is a technique to protect copyright of the image owner in the world of digital communication, and robustness is the major property to be addressed effectively. We propose an invisible hybrid watermarking scheme which is composed of blind and non-blind watermarking techniques. First, blind scheme is used as inner watermarking scheme and then non-blind watermarking scheme as outer watermarking scheme. A secret binary image is taken as a watermark and is embedded in an inner cover image using discrete wavelet transformation (DWT) with the help of the blind watermarking scheme in association with predefined binary digit sequence block and gain factor $\boldsymbol{\alpha}$ to get inner watermarked image. Then, this inner watermarked image is embedded into an outer cover image using DWT and singular value decomposition by non-blind watermarking technique to get hybrid watermarked image. On the contrary, to extract the secret binary image, first non-blind watermark extraction and then blind watermark extraction techniques are used. From the experimental results, it is shown that this hybrid watermarking approach is robust against—rotation, JPEG compression, salt and pepper noise, Gaussian noise, speckle noise and Poisson noise.

Keywords Secret binary image · Hybrid watermarking · Inner cover image · Outer cover image · Inner watermarked image · Blind · Type-II non-blind

1 Introduction

In the field of digital watermarking, many researchers are trying to reduce the gap between robustness, fidelity and capacity requirements. However, more emphasis is given for devising robust digital image watermarking scheme for copyright protection. The image with embedded watermark is called watermarked image. This watermarked image could be published, and the ownership of a suspected image can be claimed by retrieving the watermark from the watermarked image. A robust digital watermarking scheme should resist destruction from standard image processing and malicious attacks. Suppose the watermark (WM) of size $p \times q$ is to be sent to the receiver. This watermark is embedded into the cover image (CI) of size $M \times N$. This embedding process yields digital watermarked image (DWI), i.e., WM + CI = DWI of size $M \times N$. During the transmission through communication channel, this DWI is subjected to numerous types of attacks attempting to extract the trace of WM from DWI. Different set of frequency domain transformations were used by many watermark embedding and retrieval techniques to attain robustness. The digital watermarking process should be very much transparent, and this transparency can be measured by computing the level of distortion by suitable measures between CI and DWI. The technique and methodology of embedding WM into CI should be such that it should protect the WM from various types of attacks (i.e., robust) [33]. The digital watermarking schemes may be divided into two, namely blind scheme and non-blind scheme [33]. If the sender of a message is embedding the WM into CI using only suitable key and the same key is used during WM retrieval from DWI is known as a blind scheme. If the copy of original cover image (*note: This concept is used in our non-blind technique and the term copy of inner cover image is used) is needed at the receiving side to

✉ Anand Ghuli
anandghuli@gmail.com

Dayanand G. Savakar
dgsavakar@gmail.com

1 Department of Computer Science, P.G. Center, Rani Channamma University, Vijaypur, Karnataka 586108, India

2 Department of Computer Applications, B.L.D.E.A's V.P.Dr.P.G.Halakatti College of Engineering and Technology, Vijayapur, Karnataka 586103, India

3 Visvesvaraya Technological University, Belagavi, Karnataka, India

Published online: 14 February 2019

retrieve the watermark, then it is a non-blind scheme [33]. The literature reveals that spatial domain digital watermarking techniques are less secured and the frequency domain watermarking techniques are more robust [1–33].

We propose an image watermarking scheme with composition of blind and non-blind watermarking techniques along with DWT and SVD giving rise to a hybrid scheme. The proposed scheme uses both blind (only key is required to extract secret binary image) and Type-II non-blind (*Type-II non-blind* system requires the copy of embedded watermark and cover image for extraction) digital watermarking to attain robustness and fidelity [33]. The blind watermarking scheme here is referred to as inner watermarking scheme. The blind watermarking technique embeds the secret image (binary image) into a color image (inner cover image) as distributed noise using DWT with reference to predefined block structure sequence of binary digits giving rise to inner watermarked image. And in the outer watermarking scheme, non-blind technique is used; the usage of SVD in connection with DWT will help the inner watermarked image to be embedded in outer cover image of same size. When we subtract inner watermarked image (which is embedded with secret binary image) from hybrid watermarked image, we get inner watermarked image as it is, so blind watermark extraction will also give secret binary image exactly as it is. Hence, this hybrid watermarking with combination of blind and non-blind watermarking technique is more effective. The following discussion includes—Related Work, Methodology, Results and Discussion, Conclusion and References.

2 Related Work

The digital watermarking can be done in spatial domain and in frequency domain. The frequency domain schemes use different frequency domain transformations either as a single tool or hybrid tool [1–33]. In most of the cases, DWT is used to decompose the image in various energy subbands and SVD is used to embed the watermark into singular values of the obtained matrix [1,2,4,7,17,19,21,26] also block-by-block optimization on singular values [18] used to attain considerable robustness and capacity measures. The block-based DCT [5,7,26] technique is used to avoid redundancy by transforming real data into real spectrum [18,19,21]. The classified vector quantization [20] is used to improve robustness on gray-scale image watermarking. Artificial bee colony algorithm with DWT [22] and adaptive logo texturization [16] are used to insert gray-scale watermark into gray-scale image with robustness. Usage of real oriented wavelet transforms [23] and multiple watermarking were used to sustain regional attacks [7,24]. The lifting wavelet transform and firefly algorithm [8] is proposed to achieve robustness but no 100% correlation in case of watermark extraction. Local invariant features were used to propose a robust watermarking method to deal with de-synchronization attacks and also 70% of the watermark recovery is demonstrated under various noise attacks. Usage of Hermite transformation [11], optimal channel selection [9] and modulation by means of sign-altered DCT coefficients [15] has given good perceptual similarity between watermarked image and original cover image.

To improve the robustness of embedded information based on a discrete cosine transformation (DCT) domain is proposed [30]. The integration process consists of two main methods. First, the embedding intensity with vector support machines (SVMs) has been adjusted by training 1600 image blocks of different texture and luminance. Second, the embedding position has been selected using the optimized genetic algorithm (GA). In order to optimize GA, the best person in the first place of each generation directly entered the next generation and the best person in the second place took part in the crossover and the mutation process. When GA's generation number is 200, transparency reaches 40.5. A case study with the proposed method was carried out on the 256×256 Lena standard image. After several attacks such as cropping, JPEG compression, Gaussian low-pass filtering (3, 0.5), the histogram equalization and increasing contrast (0.5, 0.6) on the watermarked image were compared to the original watermark. The results show that the watermark can be recovered effectively after these attacks. Although the algorithm is weak against rotational attacks, it offers high-quality imperceptibility and robustness and is therefore a successful candidate for the implementation of a new watermarking system that meets real timescales [30].

The watermarking technique with a brightness model and a Hermite transform (HT) in digital images is proposed to achieve robustness and fidelity [31]. HT is an image representation model incorporating important human vision system (HVS) properties, such as the analysis of local orientation and the Gaussian model of early vision derivatives. The watermarking system proposed is based on a perceptive model that takes advantage of the HVS masking features, and this allows for the generation of a watermark which a human observer cannot detect. The mask is constructed using a luminosity model that takes advantage of the limited sensitivity of the human visual system to detect noise in areas of high or low light. The experimental results show that the watermark is imperceptible and that the algorithm proposed is robust for most common processing attacks. For geometric distortions, a phase of image normalization is performed before watermarking.

Plenoptic images are very demanding for large scenes in 3D representation [28]. Unlike images captured by conventional cameras, full-length images contain a considerable amount of angular information, which is very attractive for 3D reconstruction and scene display. Plenoptic images are becoming more important in areas such as medical imaging, control of manufacturing, metrology or even entertainment. Therefore, adapting and refining watermarking techniques to full-length images are a matter of increasing interest [28]. In this paper, a new method for watermarking plenoptic image is proposed. A secret key is used to specify the place of insertion of the logo. A robust feature is extracted for carrying the watermark using DCT and SVD. The peak signal-to-noise ratio (PSNR) of the watermarked image is always higher than 54.75 dB, which is far more than sufficient to discriminate against the watermarked image by the HVS. The proposed method is completely reversible and the embedded logo can be extracted in the absence of attacks and also in case of lowest watermark strength images. Even if there are enormous attacks, such as Gaussian noise, JPEG compression and median filtering, this method shows considerable robustness, as demonstrated by the promising bit error rate (BER) [28].

From the work done in the related field, it can be said that most of the articles shown more emphasis on hiding the single and/or multiple watermark image(s) into cover image to satisfy fidelity and robustness. Here, the attainment of robustness is not 100% in all cases with respect to attacks like Gaussian noise, salt and peppers, speckle noise, Poisson noise, rotation, JPEG and cropping is varying from 25 to 100% with variations in noise density [1–33]. So it is found that, there is a scope to reduce the gap from 25–100 to 90–100% by introducing the new techniques.

3 Methodology

The proposed hybrid watermarking can be clearly seen in the following presentation. The copy of inner watermarked image is the need of non-blind retrieval process, which has to be there at receiver side during communication.

3.1 Hybrid Scheme for Digital Watermark Embedding

As a first part of hybrid digital watermarking, the blind digital watermarking technique takes a secret binary image watermark which is to be embedded into inner cover image using transformation tool DWT to get inner watermarked image. And as a second part non-blind watermarking technique with DWT and SVD takes inner watermarked image as a watermark to be embedded into outer cover image.

Figure 1 demonstrates the hybrid watermarking scheme. In this scheme, generation of inner watermarked image is done by blind watermarking technique and in continuation, non-blind watermarking technique is used to generate hybrid watermarked image. Two-level discrete wavelet transformation (DWT—Haar wavelets) is applied on inner cover image to extract HL band, where horizontal edges are very clear and used for locating the suitable area to embed secret watermark image [22]. Figures 2 and 3 depict the computing of discrete wavelet transform (DWT) and can be done with a filtering cascade and a factor 2 subsampling. H and L are high- and low-pass filters, respectively, $\downarrow 2$ denotes subsampling. Outcomes of these filters are represented by Eqs. (1) and (2).

$$\boldsymbol{a}_{j+1}\left[\boldsymbol{p}\right] = \sum\nolimits_{\boldsymbol{n}=-\infty}^{+\infty} \boldsymbol{l}\left[\boldsymbol{n}-2\boldsymbol{p}\right]\boldsymbol{a}_j\left[\boldsymbol{n}\right] \tag{1}$$

$$\boldsymbol{d}_{j+1}\left[\boldsymbol{p}\right] = \sum\nolimits_{\boldsymbol{n}=-\infty}^{+\infty} \boldsymbol{h}\left[\boldsymbol{n}-2\boldsymbol{p}\right]\boldsymbol{a}_j\left[\boldsymbol{n}\right]. \tag{2}$$

Figure 2 shows that $\boldsymbol{a}_j$ elements are used for next step scaling of the transform and $\boldsymbol{d}_j$ elements taken as wavelet coefficients to determine output of the transform. $\boldsymbol{l}[\boldsymbol{n}]$ are coefficients of low-pass filters, and $\boldsymbol{h}[\boldsymbol{n}]$ are coefficients of high-pass filters. We can see that there is only half of number of $\boldsymbol{a}$ and $\boldsymbol{d}$ elements on scale $\boldsymbol{j}$ to scale $\boldsymbol{j}+\boldsymbol{1}$. So DWT can be done till two $\boldsymbol{a}_j$ elements remain in the analyzed sig-

Hybrid Watermark Embedding Process ($\otimes$ Indicates Watermark Embedding Process)
Secret Watermark *(Binary Image)* $\otimes$ Inner Cover Image *(Color Image)* = Inner Watermarked Image *(Color Image)* Inner Watermarked Image *(Color Image)* $\otimes$ Outer Cover Image *(Color Image)* = Hybrid Watermarked Image *(Color Image)*
Hybrid Watermark Extraction Process ($\circledast$ Indicates Watermark Extraction Process)
Hybrid Watermarked Image *(Color Image)* $\circledast$ Copy of Inner Watermarked Image *(Color Image)* = Inner Watermarked Image *(Color Image)* Inner Watermarked Image *(Color Image)* $\circledast$ Secret Key = Secret Watermark *(Binary Image)*

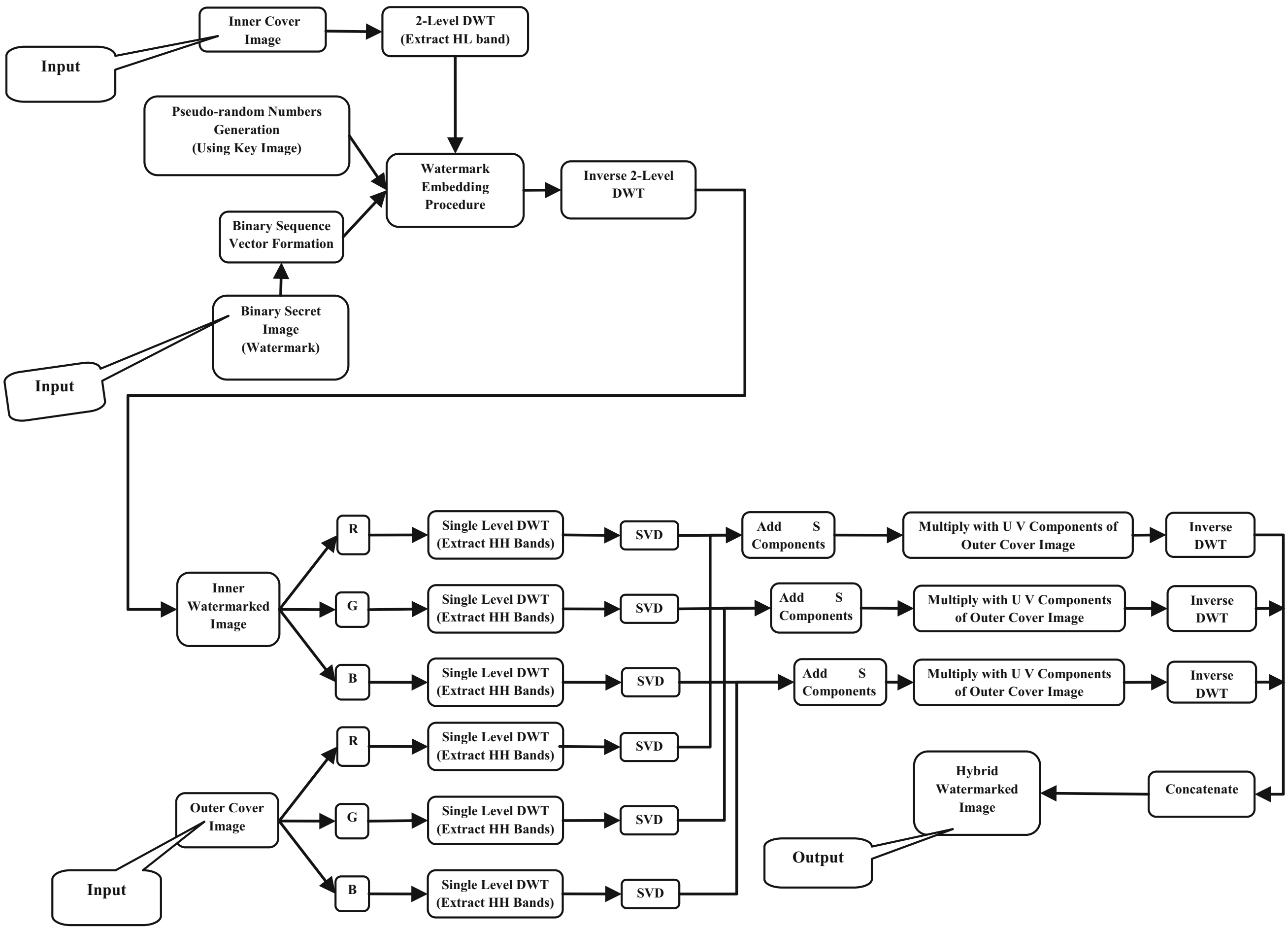


Fig. 1 Block diagram of hybrid scheme for digital watermarking process

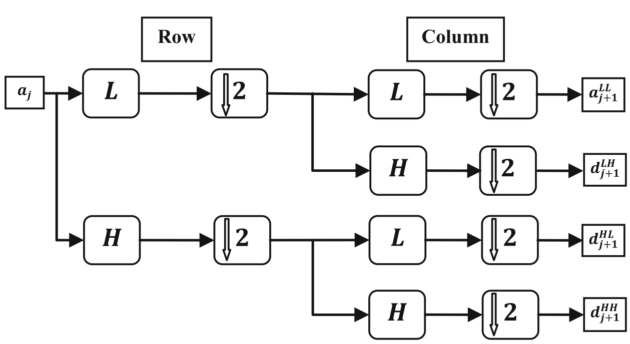


Fig. 2 Wavelet decomposition

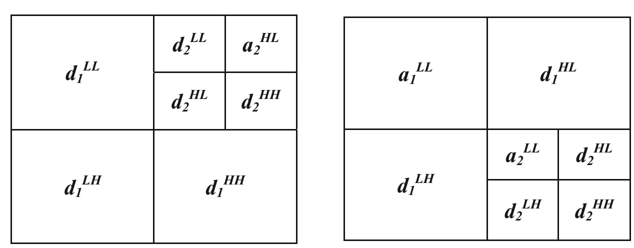


Fig. 3 Wavelet subband representation

nal and are called scaling function coefficients. As shown in Fig. 2, DWT is performed first for all image rows then for all image columns for two-dimensional pictures. The DWT is invertible and can be orthogonal. To achieve acceptable performance with respect to imperceptibility and robustness, it is always suitable to embed the watermark in the middle frequency subbands LHx and HLx [11]. Figure 3 demonstrates wavelet decomposition into LL LH HL HH subbands.

Then, secret binary image watermark is embedded using pseudorandom sequence generated with the help of key image and multiplied with a constant α into predefined binary sequence components of the block size 4×4 of inner cover image to get inner watermarked image. The predefined binary sequence may be framed in different combinations of 0's and 1's to achieve more robustness and security because as shown in Fig. 4; same binary sequence block is needed at the time of blind watermark embedding and watermark extraction. This 4×4 binary block is moved on HL band component row-wise and with respect to two uncorrelated pseudoran-

0	**1**	**0**	**1**
1	**0**	**1**	**0**
0	**1**	**0**	**1**
1	**0**	**1**	**0**

1	**1**	**1**	**1**
0	**0**	**0**	**0**
1	**1**	**1**	**1**
0	**0**	**0**	**0**

1	**1**	**0**	**0**
0	**0**	**1**	**1**
1	**1**	**0**	**0**
0	**0**	**1**	**1**

0	**0**	**0**	**0**
1	**1**	**1**	**1**
0	**0**	**0**	**0**
1	**1**	**1**	**1**

Fig. 4 Sample of 4×4 binary sequence used (for watermark embedding and extraction)

dom sequences (one for 0 and one for 1); thus created binary image vector sequence is inserted into inner cover image.

After getting the inner watermarked image (IWI), the non-blind watermarking technique is used to embed inner watermarked image into outer cover image. First decompose the outer cover image and inner watermarked image into R (Red), G (Green) and B (Blue) component panes to expand the space required to embed inner watermarked image into outer cover image. Then, DMeyer wavelet decomposition is applied on each of three R, G and B panes, respectively, to extract HH band where we can have high-frequency components of the image. The DMeyer wavelet is an approximation of the Meyer wavelet (dmey), and the usage of finite impulse response (FIR) approximations will facilitate for fast decomposition. Applying DMeyer wavelet to extract HH bands avoids staircase effect in the edges of objects of cover image after adding watermark compared with Haar wavelets.

Then, singular value decomposition (SVD) is applied on each pane to get computationally sustainable components in the form of diagonal singular values of the transformed images. Then, multiply each component matrix with U and V components of outer cover image and apply inverse DWT on each, and concatenate them to produce hybrid watermarked image. SVD is used in this to achieve robustness, because by using basis of eigenvectors, factorization of a rectangular real or complex matrix can be got by SVD, analogous to diagonalization of symmetric or Hermitian square matrices. To split the system into a set of linearly independent components, SVD is a stable and an effective method, each with own energy contribution. A given digital image of size $M \times N$, with $M \geq N$ can be represented by its SVD as Eq. (3);

$$\mathbf{A}_{M\times N} = \mathbf{U}_{M\times M}\,\mathbf{S}_{M\times N}\mathbf{V}^{\mathbf{T}}_{N\times N} \tag{3}$$

where

$$\mathbf{U}^{\mathrm{T}}\mathbf{U} = \mathbf{I}_{\mathrm{M}\times\mathrm{M}}$$
$$\mathbf{V}^{\mathrm{T}}\mathbf{V} = \mathbf{I}_{\mathrm{N}\times\mathrm{N}} \quad \text{(i.e., } U \text{ and } V \text{ are orthogonal)}$$

where the columns of U are the left singular vectors; S (dimensions as A) has diagonal singular values; and V^{T} has rows of right singular vectors. The SVD represents an expansion of the original data in a coordinate system where the covariance matrix is diagonal. Calculating the SVD consists of finding the eigenvalues and eigenvectors of AA^{T} and $A^{\mathrm{T}}A$. The eigenvectors of $A^{\mathrm{T}}A$ make up the columns of V, the eigenvectors of AA^{T} make up the columns of U. Also, the singular values in **S** are square roots of eigenvalues from AA^{T} or $A^{\mathrm{T}}A$. The singular values are the diagonal entries of the matrix S, arranged in descending order.

3.2 Hybrid Scheme for Watermark Extraction

The complete picture of secret binary image watermark extraction is shown in Fig. 5. First as an input for this process, copy of inner watermarked image and hybrid watermarked image is given to non-blind watermark extraction technique to get embedded inner watermarked image using transformation tools DWT and SVD. Then, blind watermark extraction technique uses DWT tool, binary digit sequence block, gain factor $\boldsymbol{\alpha}$ and a key to extract secret watermark image from inner watermarked image.

Now, the inputs for watermark extraction from hybrid watermarked image are—copy of inner watermarked image and hybrid watermarked image. First, decompose the hybrid watermarked image and inner watermarked image into R (Red), G (Green) and B (Blue) component panes. DMeyer single-level DWT is applied on each R, G and B component panes to extract HH band, respectively, where we have high-frequency components of the input image. The singular value decomposition (SVD) is applied on each pane to get watermark embedded components of inner watermarked image and hybrid watermarked image in the form of diagonal singular values of the transformed images of each pane. Subtract S components of each of HH band of copy of inner watermarked image from S components of each of HH band of hybrid watermarked image. Multiply each HH component matrix with U and V components of copy of inner watermarked image and apply inverse DWT on each, and by concatenating them we produce inner watermarked image. Now as a blind watermark extraction process, two-level discrete wavelet transformation (DWT—Haar wavelets)

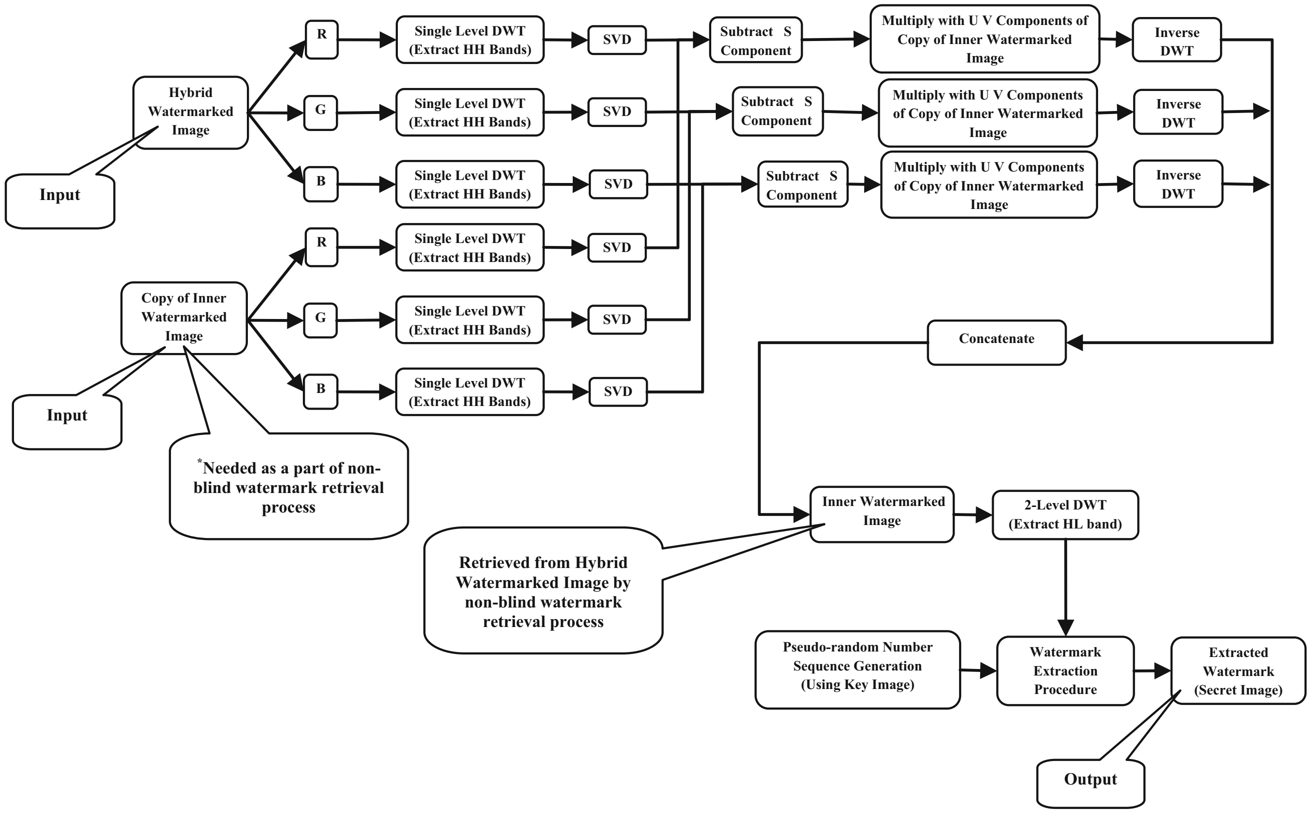


Fig. 5 Block diagram of hybrid scheme for watermark extraction

is applied on inner watermarked image to extract HL band, where horizontal edges are very clear and locate the place where we inserted secret watermark image. By moving 4×4 binary block on HL band component row-wise and with respect two correlated pseudorandom sequences (one for 0 and one for 1), the created binary image vector sequence is extracted using pseudorandom sequence generated with the help of key image, multiplied with gain factor into predefined binary sequence components of the block size 4×4 of inner watermarked image. The reconstruction of this sequence will give secret binary image watermark.

4 Algorithms

Abbreviations: *ICI* inner cover image, *OCI* outer cover image, *HWI* hybrid watermarked image, E_IWI extracted inner watermarked image.

Watermark embedding process:

$$\mathrm{IWI}^0 = \mathrm{ICI}_{\mathrm{HL}} + \alpha \times \mathrm{PN}_{0_{\mathrm{pbs}}}$$
$$\mathrm{IWI}^1 = \mathrm{ICI}_{\mathrm{HL}} + \alpha \times \mathrm{PN}_{1_{\mathrm{pbs}}}$$
$$\mathrm{IWI} = \mathrm{IWI}^0 + \mathrm{IWI}^1$$
$$\begin{aligned}\mathrm{HWI} = IWT\{&[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{R(HH)}})) + (\mathrm{SVD}(\mathrm{OCI}^{\mathrm{R(HH)}}))]\\ &+[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{G(HH)}})) + (\mathrm{SVD}(\mathrm{OCI}^{\mathrm{G(HH)}}))]\\ &+[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{B(HH)}})) + \mathrm{SVD}(\mathrm{OCI}^{\mathrm{R(HH)}}))]\}\end{aligned}$$

Watermark extraction process:

$$\begin{aligned}&\mathrm{Extracted\ (IWI)} = \{\mathrm{IDWT}[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{HH(R)}}))\\ &\quad - (\mathrm{SVD}(\mathrm{OCI}^{\mathrm{HH(R)}}))] + \mathrm{IDWT}[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{HH(G)}}))\\ &\quad - (\mathrm{SVD}(\mathrm{OCI}^{\mathrm{HH(G)}}))] + \mathrm{IDWT}[(\mathrm{SVD}(\mathrm{IWI}^{\mathrm{HH(B)}}))\\ &\quad - \mathrm{SVD}(\mathrm{OCI}^{\mathrm{HH(B)}}))]\}\\ &\mathrm{Extracted\ (WM)} = \{[\mathrm{Extracted\ (IWI)}]^{\mathrm{HL}}\\ &\quad - [(\alpha \times \mathrm{PN\_0_{pbs}}) + (\alpha \times \mathrm{PN\_1_{pbs}})]\}\end{aligned}$$

Algorithm 1: Watermark Embedding

Input : i. Inner cover image.
ii. Secret binary image (Watermark).
iii. Outer cover image

Output : Hybrid Watermarked image.

Start

Step.1: Decompose the inner cover image into four non-overlapping sub-bands using 2-level haar discrete wavelet transformation: $(ICI)^{LL}$, $(ICI)^{HL}$, $(ICI)^{LH}$, and $(ICI)^{HH}$.

Step.2: Divide the sub-band $(ICI)^{HL}$ into series of predefined binary digit sequence structure of 4×4 blocks.

Step.3: Re-formulate the secret binary image watermark into a vector of zeros and ones.

Step.4: Generate two uncorrelated pseudorandom sequences. One sequence is used to embed the watermark bit 0 and the other sequence is sued to embed the watermark bit 1.

Step.5: Embed the two pseudorandom sequences; sequence 0 and sequence 1, with a gain factor some k*,* 4×4 blocks of the selected $(ICI)^{HL}$ DWT sub-bands of the inner cover image.

If the secret binary image watermark bit is 0 then

$X' = X + k \times$ pseudorandom sequence for 0

otherwise,

$X' = X + k \times$ pseudorandom sequence for 1

[Where X ' represents the pseudorandom sequence embedded block. X denotes the matrix of the coefficients of block.]

Step.6: Apply the inverse DWT on the modified sub-band, to produce the inner watermarked image.

Step.7: Segregate the R, G and B component Panes from Inner watermarked image and Outer cover image as IWI^R, IWI^G, IWI^B and IWI^R, OCI^G, OCI^B respectively.

Step.8: Decompose the respective IWI^R, IWI^G, IWI^B and OCI^R, OCI^G, OCI^B in to sub-bands: LL, HL, LH, and HH and extract LL using 1-level DMeyer wavelet decomposition respectively.

$HH(IWI^R)$, $HH(IWI^G)$, $HH(IWI^B)$ and $HH(OCI^R)$, $HH(OCI^G)$, $HH(OCI^B)$.

Step.9: Apply SVD to each $HH(IWI^R)$, $HH(IWI^G)$, $HH(IWI^B)$ and $HH(OCI^R)$, $HH(OCI^G)$, $HH(OCI^B)$ to get U, S and V matrices as.

$U(HH(IWI^R))$, $S(HH(IWI^R))$, $V(HH(IWI^R))$

$U(HH(IWI^G))$, $S(HH(IWI^G))$, $V(HH(IWI^G))$

$U(HH(IWI^B))$, $S(HH(IWI^B))$, $V(HH(IWI^B))$

$U(HH(OCI^R))$, $S(HH(OCI^R))$, $V(HH(OCI^R))$

$U(HH(OCI^G))$, $S(HH(OCI^G))$, $V(HH(OCI^G))$

$U(HH(OCI^B))$, $S(HH(OCI^B))$, $V(HH(OCI^B))$

Step.10: $New\_S(HH(IWI^R)) = S(HH(IWI^R)) \times Constant\_1 + S(HH(OCI^R)) \times Constant\_2$

$New\_S(HH(IWI^G)) = S(HH(IWI^G)) \times Constant\_1 + S(HH(OCI^G)) \times Constant\_2$

$New\_S(HH(IWI^B)) = S(HH(IWI^B)) \times Constant\_1 + S(HH(OCI^B)) \times Constant\_2$

Step.11: $HWI\_R = U(HH(OCI^R)) \times New\_S(HH(IWI^R)) \times V(HH(OCI^R))$

$HWI\_G = U(HH(OCI^G)) \times New\_S(HH(IWI^G)) \times V(HH(OCI^G))$

$HWI\_B = U(HH(OCI^B)) \times New\_S(HH(IWI^B)) \times V(HH(OCI^B))$

And apply inverse DMeyer DWT on HWI_R, HWI_G, HWI_B.

Step.12: Now concatenate each matrix to produce Hybrid Watermarked Image (HWI)

Stop.

The Algorithm 1 uses blind watermarking technique first to embed secret binary image into inner cover image and Non-blind watermarking technique to embed inner watermarked image into outer cover image.

Algorithm 2: Watermark extraction

Input : Hybrid Watermarked image and Copy of inner watermarked image

(*Inner watermarked image is the image where the secret binary image is embedded with it, and the copy of this inner watermarked image is needed in case of non-blind technique)

Output : Secret binary image watermark

Start

Step.1: Segregate the R, G and B component Panes from Inner watermarked image and Hybrid Watermarked Image as IWI^R, IWI^G, IWI^B and HWI^R, HWI^G, HWI^B respectively.

Step.2: Decompose the respective IWI^R, IWI^G, IWI^B and HWI^R, HWI^G, HWI^B in to sub-bands: LL, HL, LH, and HH and extract LL using 1-level DMeyer wavelet decomposition respectively.
HH (IWI^R), HH (IWI^G), HH (IWI^B) and HH (HWI^R), HH (HWI^G), HH (HWI^B).

Step.3: Apply SVD to each HH (IWI^R), HH (IWI^G), HH (IWI^B) and HH (HWI^R), HH (HWI^G), HH (HWI^B) to get U, S and V matrices as.

U (HH (IWI^R)), S (HH (IWI^R)), V (HH (IWI^R))
U (HH (IWI^G)), S (HH (IWI^G)), V (HH (IWI^G))
U (HH (IWI^B)), S (HH (IWI^B)), V (HH (IWI^B))
U (HH (HWI^R)), S (HH (HWI^R)), V (HH (HWI^R))
U (HH (HWI^G)), S (HH (HWI^G)), V (HH (HWI^G))
U (HH (HWI^B)), S (HH (HWI^B)), V (HH (HWI^B))

Step.4: New_S (HH (IWI^R)) = (S (HH (HWI^R)) - S (HH (IWI^R)) × Constant_1)
New_S (HH (IWI^G)) = (S (HH (HWI^G)) - S (HH (IWI^G)) × Constant_1)
New_S (HH (IWI^B)) = (S (HH (HWI^B)) - S (HH (IWI^B)) × Constant_1)

Step.5: New_IWI_R = U (HH (IWI^R)) × New_S (HH (IWI^R)) × V (HH (IWI^R))
New_IWI_G = U (HH (IWI^G)) × New_S (HH (IWI^G)) × V (HH (IWI^G))
New_IWI_B = U (HH (IWI^B)) × New_S (HH (IWI^B)) × V (HH (IWI^B))
And apply inverse DMeyer DWT on New_IWI_R, NEW_IWI_G, New_IWI_B.

Step.6: Now concatenate each matrix to produce Extracted Inner watermarked image (E_IWI)

Step.7: Apply 2-level Haar DWT on extracted inner watermarked image to extract E_IWI^{HL} band.

Step.8: Divide the sub-band E_IWI^{HL} into series of predefined binary sequence structure of 4 × 4 blocks.

Step.9: Regenerate the two pseudorandom sequences for 0 and 1 using the same seed used in the blind watermark embedding procedure

Step.10: For each block in the sub-band E_IWI^{HL}, calculate the correlation between the elements coefficients and the two generated pseudorandom sequences for 0 and 1.
If the correlation with the pseudorandom sequence 0 was higher than the correlation with pseudorandom sequence 1, then the extracted watermark bit is considered 0
Otherwise the extracted watermark is considered 1.

Step.11: Reconstruct the watermark using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

Stop.

The Algorithm 2 uses Non-blind watermarking technique to extract inner watermarked image from hybrid watermarked image and Blind watermarking technique to extract secret binary image from extracted inner watermarked image.

5 Results and Discussion

The purpose of embedding secret binary image (Watermark) using proposed hybrid watermark embedding scheme is to provide more security to the secret binary image with high robustness. The combination of blind and non-blind techniques leads to minimization of false-negative error (the probability of failing to detect the embedded watermark) in the absence of attacks or signal distortions. This minimization of false-negative error is due to SVD [2] and the extraction process as depicted in Algorithm-2, where inner watermarked image is extracted from hybrid watermarked image. At the same time, this combination leads to false-positive error (probability to detect another watermark during the absence of watermark) [2,33].

The perceptual similarity between outer cover image and hybrid watermarked image can be verified by measuring—structural similarity (SSIM) [4–17,32] index [Eq. (4)] and peak signal-to-noise ratio PSNR [4–17,32] [Eq. (5)] in decibels (dB). The structural similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as a reference. SSIM considers image degradation as a perceived change in structural information. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The SSIM [32] metric is calculated on various windows of an image. The measure between two windows x and y of common size N×N is:

$$\mathbf{SSIM}\,(\mathbf{x},\mathbf{y}) = \frac{\left(2\mu_{\mathbf{x}}\mu_{\mathbf{y}} + \mathbf{c}_1\right)\left(2\sigma_{\mathbf{xy}} + \mathbf{c}_2\right)}{\left(\mu_x^2 + \mu_{\mathbf{y}}^2 + \mathbf{c}_1\right)\left(\sigma_{\mathbf{x}}^2 + \sigma_{\mathbf{y}}^2 + \mathbf{c}_2\right)}. \tag{4}$$

where

$\mu_{\mathbf{x}}$ is the average of x
$\mu_{\mathbf{y}}$ is the average of y
$\sigma_{\mathbf{x}}^2$ Variance of x
$\sigma_{\mathbf{y}}^2$ Variance of y
$\sigma_{\mathbf{xy}}$ Covariance of x and y

$\mathbf{c}_2 = (\mathbf{k}_2, \mathbf{L})^2$

$\mathbf{c}_1, \mathbf{c}_2$ The two variables stabilize the division with weak denominator.
L Dynamic range of pixels (255).
$\mathbf{k}_1 = 0.01$ and $\mathbf{k}_2 = 0.03$ By default.

Peak signal-to-noise ratio (PSNR) [32] (Eq. 5) in decibels (dB). For example, if an image with 8 bits per pixel contains integers from 0 to 255 (B), PSNR will be given as Eq. 5.

$$\mathbf{PSNR} = \mathbf{20log}_{10}\frac{\left(2^{\mathbf{B}} - 1\right)}{\sqrt{\mathbf{MSE}}} \tag{5}$$

The mean-square-error (MSE) is the squared norm of the difference between the data x and the approximation $\hat{x}$ divided by the number of elements.

where $\mathbf{MSE} = \dfrac{\mathbf{x} - \hat{\mathbf{x}}^2}{\mathbf{N}}$

To compare the correlation between original secret watermark image and extracted secret watermark image, we use the formula as depicted in Eq. 6.

$$\mathbf{r} = \frac{\sum_{\mathbf{i}}(\mathbf{x_i} - \mathbf{x_m})\,(\mathbf{y_i} - \mathbf{y_m})}{\sqrt{\sum_{\mathbf{i}}(\mathbf{x_i} - \mathbf{x_m})^2}\sqrt{\sum_{\mathbf{i}}(\mathbf{y_i} - \mathbf{y_m})^2}} \tag{6}$$

where x_i and y_i are intensity values of ith pixel of original secret watermark image and extracted secret watermark image, x_m and y_m are the mean intensity values of original secret watermark image and extracted secret watermark image. The correlation coefficient r is 1 if the images under comparison are completely identical, r is 0 if images under comparison are uncorrelated and r is -1 (negative) if the images under comparison are anti-correlated. Table 1 shows the correlation between original watermark and extracted watermark, PSNR and SSIM between outer cover image and hybrid watermarked image.

The results thus obtained in Table 1 are due to the embedding of secret binary image into the second level HL bands that is the secret binary image energy is embedded into horizontal edges and texture which represents most of the coefficients in the HL subbands. This will enhance invisibility of the watermarking process because the human eye is less sensitive to changes in edge and texture information, compared to changes in low-frequency components. Then, this inner watermarked image is embedded into outer cover image by extracting HH subbands of both the images by applying DMeyer wavelet to extract HH bands which avoids staircase effect in the edges of objects of cover image after adding watermark compared with Haar wavelets. Thus, HH subbands are having high-frequency image information into them. The SVD applied will provide the robustness [2,12,14,16,21]. So by embedding the inner watermarked image into

Table 1 Results of hybrid digital image watermarking

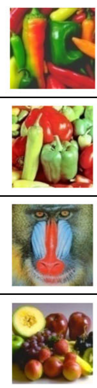
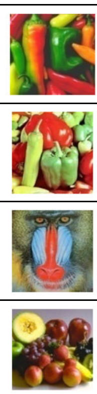
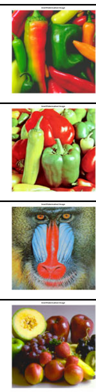
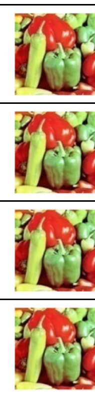
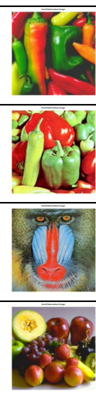
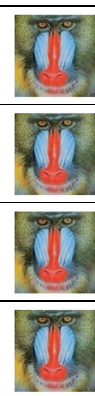
Secret Binary Image (Watermark) Size (50×20)	Different Inner cover Images Size (512×512)	Inner Watermarked Image Size (512×512)	Outer Cover Image Size (512×512)	Hybrid Watermarked Image Size (512×512)	PSNR in dB (Between Hybrid Watermarked Image and Outer Cover Image)	SSIM (Between Hybrid Watermarked Image and Outer Cover Image)	Correlation Between Secret Watermark and Extracted Secret Watermark
anand					61.7524	0.9999	1.0000
anand					54.6660	0.9990	1.0000
anand					51.7797	0.9978	1.0000
anand					61.3628	0.9999	1.0000
anand					55.4104	0.9993	1.0000
anand					64.5371	0.9999	1.0000
anand					60.0742	0.9998	1.0000
anand					56.7247	0.9995	1.0000
anand					52.4940	0.9996	1.0000
anand					63.0111	1.0000	1.0000
anand					64.1944	1.0000	1.0000
anand					53.3180	0.9997	1.0000
anand					59.8649	0.9999	1.0000
anand					54.8176	0.9995	1.0000
anand					51.6786	0.9989	1.0000
anand					59.6544	0.9999	1.0000

Table 2 Effects of various noise attacks on proposed hybrid scheme

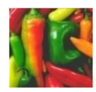
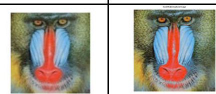
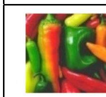
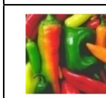
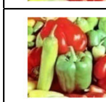
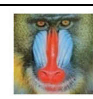
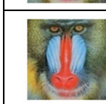
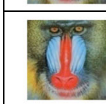
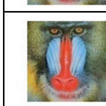
Secret Binary Image (Watermark) Size (50×20)	Different Inner cover Images Size (512×512)	Inner Watermarked Image Size (512×512)	Outer Cover Image Size (512×512)	Hybrid Watermarked Image Size (512×512)	Correlation between original watermark and extracted watermark				
					Gaussian Noise	Salt & Pepper Noise	Poisson Noise	Speckle Noise	Rotation
anand					0.9438	0.9139	1.0000	0.9346	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					0.9564	0.9464	0.9965	0.9464	1.0000
anand					0.9376	0.9139	0.9896	0.9081	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					0.9495	0.9432	0.9861	0.9401	1.0000
anand					0.9376	0.9168	0.9896	0.9197	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					0.9495	0.9464	0.9861	0.9495	1.0000
anand					0.9407	0.9139	1.0000	0.9226	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					1.0000	1.0000	1.0000	1.0000	1.0000
anand					0.9495	0.9464	0.9965	0.9464	1.0000

Table 3 Comparison between proposed hybrid scheme with other schemes of references for various attacks

Attack type on hybrid watermarked image	Correlation between secret watermark and extracted secret watermark (proposed scheme)	Method [8]	Method [10]	Method [16]	Method [29]	Method [31]
Gaussian noise	0.9376 – 1.0000	0.8552 – 1.0000	0.25 – 0.5	0.796 – 0.895	0.640	0.215 – 0.69
Speckle noise	0.9081 – 1.0000	0.9886 – 1.0000	–	–	0.840	–
Salt and pepper noise	0.9139 – 1.0000	0.8454 – 0.9609	–	–	0.840	0.13 – 0.69
Poisson noise	0.9861 – 1.0000	1.0000	–	–	–	–
Rotation (90°)	1.0000	0.1084	0.64	0.765	1.0000	0.13
Rotation (180°)		–	–	–		0.3
Rotation (270°)		0.1141	0.90	0.919		
JPEG compression	1.0000	1.0000	0.4500 – 1.0000	0.891 – 0.901	0.650	0.05 – 0.69

HH subbands of outer cover image in tune with SVD will preserve the content and will also improve the perceptual similarity between outer cover image and hybrid watermarked image.

Table 2 shows the results of secret binary image extraction with various attacks. The purpose of combining blind and non-blind scheme is—Type-II non-blind scheme here needs the copy of inner watermarked image and hybrid watermarked image to perform extraction of inner watermarked image from hybrid watermarked image. The usage of SVD here gives one level of robustness. And blind watermarking scheme needs specific key and same binary sequence block as stated above to extract secret binary image watermark from inner watermarked image, which gives another level of robustness. The effect of various types of attacks on extraction of secret binary image and the comparison with other methods shown in Table 2 are the results due to the combination of blind and non-blind watermarking schemes. Whenever the hybrid watermarked image is attacked by different noises or rotation, the non-blind watermark extraction process of the proposed technique takes inputs as attacked hybrid watermarked image and inner watermarked image for the extraction process. When inner watermarked image is extracted from attacked hybrid watermarked image, most of the inner watermarked content is extracted as it is because the secret binary image is in the horizontal edges and texture. This will safely preserve the secret binary image. Giving the false-positive error is the weak point of proposed method. That is it may detect another watermark during the absence of original secret binary image (watermark). Table 3 shows perceptual similarity comparison between different techniques and proposed techniques.

Table 4 shows the comparison between perceptual similarity obtained by proposed method and various results from the reference articles.

6 Conclusion

A hybrid watermarking scheme using blind and non-blind watermark embedding process has been proposed in this article. The proposed scheme is the combination of block processing, DWT in blind technique and DWT, SVD processing in non-blind technique. Four color images were used in combination with different outer cover images and inner cover images to get sixteen possible results. The DWT, SVD transformations are used and tested for better results. The perceptual similarity between same inner cover image and outer cover image is measured with PSNR value as 64.5371 dB to 51.6786 dB. In all cases, extracted secret watermark correlation measured as 1.0000. This scheme is robust against attacks like JPEG compression, rotation and addition of

Table 4 Perceptual similarity result comparison between proposed hybrid scheme with other schemes of references

Method	PSNR in dB For different samples of Color cover images	SSIM For different samples of color cover images
Method [10]	48.86–49.62	0.9891–0.9893
Method [13]	52.90–57.47	0.9774–0.9985
Method [14]	48.91–58.97	–
Method [15]	40.02–40.13	0.9720–0.9750
Method [29]	100.88	–
Method [31]	36.9731–43.0007	0.9816–0.9893
Proposed method	51.6786–64.5371	0.9989–1.0000

Gaussian, Poisson, salt and pepper and speckle noises. The proposed method leads to minimization of false-negative error and possesses false-positive error. The proposed scheme can be improved to avoid false-positive error and also to achieve more fidelity and 100% robustness in various active attacks.

References

1. Abuturab, M.R.: Multiple color-image fusion and watermarking based on optical interference and wavelet transform. Opt. Lasers Eng. **89**, 47–58 (2017)
2. Jeronymo, D.C.; Borges, Y.C.C.; dos Santos Coelho, L.: Image forgery detection by semi-automatic wavelet soft-thresholding with error level analysis. Expert Syst. Appl. **85**, 348–356 (2017)
3. Etemad, E.; Samavi, S.; Soroushmehr, S.M.R.; Karimi, N.; Etemad, M.; Shirani, S.; Najarian, K.: Robust image watermarking scheme using bit-plane of hadamard coefficients. Multimed. Tools Appl. **77**(2), 2033–2055 (2017)
4. Savakar, D.G.; Ghuli, A.: Non-blind digital watermarking with enhanced image embedding capacity using DMeyer wavelet decomposition, SVD and DFT. Pattern Recognit. Image Anal. **27**(3), 511–517 (2017)
5. Ananthaneni, V.; Nelakuditi, U.R.: Hybrid digital image watermarking using contourlet transform (CT), DCT and SVD. Int. J. Image Process. (IJIP) **11**(3), 85–93 (2017)
6. Bansal, N.; Deolia, V.K.; Bansal, A.; Pathak, P.: Comparative analysis of digital watermarking techniques. In: Proceedings of the International Congress on Information and Communication Technology, pp. 105–115. Springer, Singapore (2016)
7. Zear, A.; Singh, A.K.; Kumar, P.: A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed. Tools Appl. **77**(4), 4863–4882 (2016)
8. Kazemivash, B.; Moghaddam, M.E.: A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. Multimed. Tools Appl. **76**(20), 20499–20524 (2016)
9. Tang, Z.; Lao, H.; Zhang, X.; Liu, K.: Robust image hashing via DCT and LLE. Comput. Secur. **62**, 133–148 (2016)
10. Pan-Pan, N.; Xiang-Yang, W.; Yu-Nan, L.; Hong-Ying, Y.: A robust color image watermarking using local invariant significant bitplane histogram. Multimed. Tools Appl. **76**(3), 3403–3433 (2016)
11. Coronel, S.L.G.; Ramírez, B.E.; Mosqueda, M.A.A.: Robust watermark technique using masking and Hermite transform. SpringerPlus **5**(1), 1830 (2016)
12. Benrhouma, O.; Hermassi, H.; Belghith, S.: Security analysis and improvement of an active watermarking system for image tampering detection using a self-recovery scheme. Multimed. Tools Appl. **76**(20), 21133–21156 (2016)
13. Albalawi, U.; Mohanty, S.P.; Kougianos, E.: A new region aware invisible robust blind watermarking approach. Multimed. Tools Appl. **76**(20), 21303–21337 (2016)
14. Huynh-The, T.; Banos, O.; Lee, S.; Yoon, Y.; Le-Tien, T.: Improving digital image watermarking by means of optimal channel selection. Expert Syst. Appl. **62**, 177–189 (2016)
15. Hu, H.T.; Chang, J.R.; Hsu, L.Y.: Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception. AEU-Int. J. Electron. Commun. **70**(10), 1374–1381 (2016)
16. Andalibi, M.; Chandler, D.M.: Digital image watermarking via adaptive logo texturization. IEEE Trans. Image Process. **24**(12), 5060–5073 (2015)
17. Narula, N.; Sethi, D.; Bhattacharya, P.P.: Comparative analysis of DWT and DWT–SVD watermarking techniques in RGB images. Int. J. Signal Process. Image Process. Pattern Recognit. IJSIP **8**(4), 339–348 (2015)
18. Huang, H.; Chen, D.; Lin, C.; Chen, S.; Hsu, W.: Improving SVD-based image watermarking via block-by-block optimization on singular values. EURASIP J. Image Video Process. **2015**(1), 1–10 (2015)
19. Islam, M.S.; Chong, U.: Performance of a hybrid DCT SVD visually imperceptible digital watermarking against signal processing attacks. Comput. Sci. Appl. Lect. Notes Electr. Eng. **330**, 7–14 (2015)
20. Ding, X.; Lu, Z.; Yu, F.; Nie, T.; Sun, J.: A robust blind image watermarking scheme based on classified vector quantization. J. Inf. Hiding Multimed. Signal Process. **6**(1), 74–80 (2015)
21. Loukhaoukha, K.; Refaey, A.; Zebbiche, K.; Nabti, M.: On the security of robust image watermarking algorithm based on discrete wavelet transform, discrete cosine transform and singular value decomposition. Appl. Math. Inf. **9**(3), 1159–1166 (2015)
22. Sha, F.; Lo, F.; Chung, Y.Y.; Chen, X.; Yeh, W.: A novel optimized watermark embedding scheme for digital images. In: MultiMedia Modeling Lecture Notes in Computer Science, pp. 208–219 (2015)
23. Agarwal, H.; Atrey, P.K.; Raman, B.: Image watermarking in real oriented wavelet transform domain. Multimed. Tools Appl. **74**(23), 10883–10921 (2014)
24. Liu, Y.; Wang, Y.; Zhu, X.: Novel robust multiple watermarking against regional attacks of digital images. Multimed. Tools Appl. **74**(13), 4765–4787 (2014)
25. Singh, A.K.; Kumar, B.; Dave, M.; Mohan, A.: Robust and imperceptible dual watermarking for telemedicine applications. Wirel. Pers. Commun. **80**(4), 1415–1433 (2014)
26. Al-Haj, A.: Combined DWT–DCT digital image watermarking. J. Comput. Sci. **3**(9), 740–746 (2007)

27. Savakar, D.G.; Kannur, A.: A practical aspect of identification and classifying of Guns based on gunshot wound patterns using gene expression programming. Pattern Recognit. Image Anal. **26**(2), 442–449 (2016)
28. Ansari, A.; Hong, S.; Saavedra, G.; Javidi, B.; Martinez-Corral, M.: Ownership protection of plenoptic images by robust and reversible watermarking. Opt. Lasers Eng. **107**, 325–334 (2018)
29. Bal, S.N.; Nayak, M.R.; Sarkar, S.K.: On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. J. King Saudi Univ. Comput. Inf. Sci. (2018). https://doi.org/10.1016/j.jksuci.2018.04.006
30. Zhou, X.; Cao, C.; Ma, J.; Wang, L.: Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm. Math. Probl. Eng. **2018** (2018). https://doi.org/10.1155/2018/2685739
31. Escalante-Ramírez, B.; Gomez-Coronel, S.L.: A perceptive approach to digital image watermarking using a brightness model and the hermite transform. Math. Probl. Eng. **2018** (2018). https://doi.org/10.1155/2018/5463632
32. Hore, A.; Ziou, D.: Image quality metrics: PSNR vs. SSIM. In: 2010 20th International Conference on Pattern Recognition, Istanbul, pp. 2366–2369 (2010) https://doi.org/10.1109/ICPR.2010.579
33. Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J.; Kalker, T.: Digital Watermarking and Steganography, vol. 2. Morgan Kaufmann Publishers, Burlington (2008)