THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

A multi-scale image watermarking based on integer wavelet transform and singular value decomposition

A multi-scale image watermarking based on integer wavelet transform and singular value decomposition

Yuling Luo[1,2], Liangjia Li[1], Junxiu Liu[1,*], Shunbin Tang[1], Lvchen Cao[1],
Shunsheng Zhang[1], Senhui Qiu[1,3], Yi Cao[4]

[1] School of Electronic Engineering, Guangxi Normal University, Guilin, China

[2] Guangxi Key Lab of Multi-source Information Mining & Security,
Guangxi Normal University, Guilin, China

[3] Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing,
Guilin, China

[4] Management Science and Business Economics Group, Business School,
University of Edinburgh, Edinburgh, UK, EH8 9JS

Email: yuling0616@gxnu.edu.cn, 1131489877@qq.com, j.liu@ieee.org*,
13395972993@163.com, 18810775110@163.com, 1065355934@qq.com,
qiusenhui@gxnu.edu.cn, jason.caoyi@gmail.com

Abstract: Image watermarking technique is one of effective solutions to protect copyright, and it is applied to a variety of information security application domains. It needs to meet four requirements of imperceptibility, robustness, capacity and security. A multi-scale and secure image watermarking method is proposed in this work, which is based on the Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD). Four IWT sub-bands are firstly obtained after 1-level IWT on the host image, and the corresponding singular diagonal matrices of four sub-bands can be obtained using SVD. Then, each singular diagonal matrix is divided into four non-overlapping sections in terms of the size of embedding watermark. Particularly, the size of upper left part is same as the size of watermark. The watermark can be directly embedded into four upper left parts afterwards by multiplying different scaling factors to complete the final watermarking operation. Especially, a novel optimized authentication mechanism is designed to resolve the false positive problem, which exists in the SVD-based watermarking algorithms. In addition, three-dimensional optimal mapping algorithm is proposed to search the optimal scaling factors through a novel objective evaluation function, and it can significantly improve the imperceptibility and robustness. The experimental test and comparison analysis illustrate that the proposed watermark scheme demonstrates a high imperceptibility with peak signal to noise ratio values of 45dB and strong robustness with average normalized correlation values of 0.92.

Keywords: Multi-scale watermarking; IWT; SVD; Optimal mapping; Authentication mechanism

1. Introduction

It has been reported that the image copyright infringement issues are especially severe such as image tampering (Amerini et al., 2011), image forgery (Farid, 2009) and false ownership claims (Wong & Memon, 2001). Watermarking technique is considered as an effective method to protect the copyright (Ansari et al., 2016; Liu et al., 2019; Makbol et al., 2017a; Makbol & Khoo, 2014). The watermarking methods can be roughly classified into three categories of fragile, semi-fragile and robust watermarking (Makbol & Khoo, 2014). Robust watermarking technology does not significantly reduce the visual quality of watermarked images, and watermarks can be extracted from watermarked images whose quality has been destroyed (Malvar & Florêncio, 2002). The fragile watermark is used to ensure the integrity of the image, and its purpose is to analyze the changes of the extracted watermark in order to locate and track the damaged location and degree of influence on the watermarked image (Zhang & Wang, 2008). The characteristic of semi-fragile watermark is between the former two. It requires the embedded watermark can resistant against general processing, but it is very sensitive to malicious tampering or attacks (Qi & Xin, 2011). Among them, robust watermarking is widely considered for copyright protection and ownership verification in the image watermarking (Liu et al., 2019). For the robust watermarking schemes, there are two most common embedding methods: the space domain insertion and the transform domain insertion (Chan & Cheng, 2004; Guo et al., 2017; Nikolaidis & Pitas, 1998; Yadav et al., 2018). Specifically, the former is that the pixel values of host image are

changed directly to embed watermark, which has low computational complexity but the ability of resisting image processing attack and geometric attack is relatively weak (Makbol & Khoo, 2014). The latter is that the transform coefficients of the cover image are used to embed the watermark, and the transform coefficients can be obtained by performing different transform, e.g., Discrete Wavelet Transform (DWT) (Yadav et al., 2018), Integer Wavelet Transform (IWT) (Su et al., 2012), redundant discrete wavelet transform (H.-C. Ling et al., 2013), discrete cosine transform (Barni et al., 1998), and discrete Fourier transform (Pun, 2006) etc. Compared with space domain insertion, the robustness of transform domain insertion is better, while the computational complexity is higher. Consequently, the scheme based on transform domain can enhance robustness against malicious attacks (e.g., Noise and Cropping) and image processing attacks (e.g., JPEG compression and Sharpening) (Ansari et al., 2016). In addition, the watermarking methods utilizing wavelet transform have the superiorities in the energy compression, multi-resolution and visual quality (Hsieh et al., 2001; Y. Wang et al., 2002).

Researches show that the watermarking schemes only based on wavelet transform are hard to resist the geometric attacks (e.g., Scaling and Rotation) (Muhammad & Bibi, 2015). To address this limitation, the watermarking schemes based on wavelet transform by combining matrix decompositions such as Singular Value Decomposition (SVD) (Makbol & Khoo, 2014), Hessenberg decomposition (Liu et al., 2019) or QR decomposition (Guo et al., 2017) are proposed. The most commonly used matrix decomposition is SVD because the watermarking schemes by combining wavelet transform and SVD can resist image processing attacks and geometric attacks (Ali & Ahn, 2014a; Muhammad & Bibi, 2015). The expression of SVD is denoted by

$$A = USV^T, \tag{1}$$

where A represents a matrix or an image, U denotes left singular unitary matrix, S denotes singular diagonal matrix and V denotes right unitary singular matrix. The three matrices can be utilized to embed watermark. Matrix S is the most commonly used due to its good stability towards various attacks, and it can keep good visual quality of the image (Liu et al., 2019). However, those SVD-based watermarking methods face False Positive Problem (FPP) if watermark is embedded into matrix S (Makbol et al., 2018), i.e. attacker can extract non-embedded watermarks from the host images or watermarked images. Two embedding processes cause FPP. The first type of embedding scheme is calculated by

$$S_{HW} = S_H + \alpha S_W, \tag{2}$$

where S_{HW}, S_H and S_W are singular diagonal matrices of watermarked image, host image and watermark, respectively, α is scaling factor. In this embedding process, S_H and S_W are obtained by SVD. Furthermore, the host image is embedded with a watermark by adding αS_W (Ahmad et al., 2011; Rastegar et al., 2011). However, most of the image information are carried through matrix U and V (Tian et al., 2003). Therefore, wrong watermark can be extracted by an attacker who uses their matrix U

and V to declare the false ownership (Ali & Ahn, 2015; H. C. Ling et al., 2013). The second type of FPP is described by

$$S_H + \alpha W = U_{HW} S_{HW} V_{HW}^T, \qquad (3)$$

where W denotes watermark, U_{HW}, S_{HW} and V_{HW} are matrices with watermark information. In this embedding process, SVD is performed on the host image to obtain S_H. Then the watermark is embedded into S_H by adding αW. Next, three matrices U_{HW}, S_{HW} and V_{HW}^T are obtained by performing SVD again (Ansari et al., 2016; H.-C. Ling et al., 2013; Makbol & Khoo, 2014). Therefore, this embedding process also suffers from FPP as only S_H is used.

To resolve FPP, different solutions are proposed such as using hash value for authentication (Loukhaoukha et al., 2011), principle component insertion (Ali & Ahn, 2014a), digital signature insertion for authentication (Ansari et al., 2016; Makbol & Khoo, 2014) and image encryption schemes (Luo et al., 2016, 2018; Luo, Lin, et al., 2019; Luo, Ouyang, et al., 2019). Specifically, in (Loukhaoukha et al., 2011), two hashing values are obtained by performing one-way hash function on matrix U_W and V_W, and then two hashing values are stored privately and used for authentication before beginning the process of watermark extraction. In (Ali & Ahn, 2014a), four singular values of transformed image are embedded with the principle components (matrix U_W and S_W) of transformed watermark to avoid FPP, but this scheme has poor imperceptibility and robustness. Therefore, differential evolution optimization algorithm is proposed to improve imperceptibility and robustness. In addition, the signature for authentication is used to address FPP (Ansari et al., 2016; Makbol & Khoo, 2014; Singh & Singh, 2017). In their schemes, matrix U_W and V_W are used to generate digital signature. Then the digital signature is inserted into the transformed image or watermarked image to verify the authenticity, which can avoid FPP. However, according to the results in (Makbol & Khoo, 2014), recovered signature bits are poor under some attacks. In (Liu et al., 2019), the matrix U_W and V_W are encrypted by chaotic systems to resolve FPP and the original watermark can be extracted only using the correct keys.

In addition, the trade-off between invisibility and robustness has also been investigated. Nature inspired optimization techniques such as firefly algorithm (Ali & Ahn, 2014b; Guo et al., 2017), particle swarm optimization (Aslantas et al., 2008), artificial bee colony (Ansari et al., 2016, 2017) and firefly optimization algorithm (Liu et al., 2019) are used to solve this problem. All of these bio-inspired algorithms are utilized to search the most suitable scaling factor for improving the imperceptibility and robustness. Inspired by the aforementioned approaches, a multi-scale and secure watermarking scheme is proposed in this work by combining IWT with SVD. The main contributions of this work are as follows. (1) An Optimized Authentication Mechanism (OAM) is designed to address the FPP, which can improve the security of the watermarking algorithm. (2) A novel Objective Evaluation Function (OEF) and Three-dimension Optimal Mapping (TDOM) algorithm are proposed to facilitate searching the optimal scaling factors, which achieves a trade-off between invisibility and

robustness. (3) The limitation of fixed watermark size is eliminated in this scheme. Besides, the proposed algorithm is tested against various attacks and the results show that it has high robustness and good imperceptibility.

The rest of this paper is arranged as follows. The descriptions of IWT and SVD are provided in Section 2. In Section 3, the watermarking method based on IWT-SVD, OAM and TDOM is proposed. Section 4 gives the experimental results and performance analysis. Section 5 presents the conclusion.

2. Preliminaries

2.1. Integer wavelet transform

IWT can be perfectly constructed by using lifting schemes (Sweldens, 1998). Lifting scheme can be utilized for realizing the reconstruction of integer onto integer wavelet transform (Su et al., 2012). IWT is used in the mapped process, because IWT has some advantages in the data decomposition, such as no rounding error and reversibility property. Moreover, compared with classical wavelet transform, IWT is more efficient and faster (Pan et al., 2010). Similar to lifting scheme, IWT is consisted of three basic steps, including split, prediction and update (Jia et al., 2010). The detailed steps are illustrated in Figure 1.
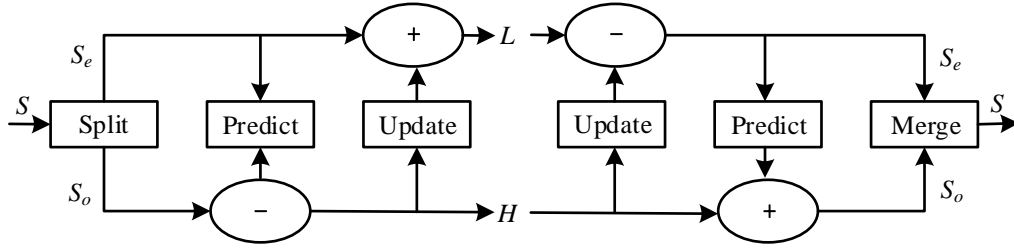

Figure 1. The steps of lifting and the inverse lifting.

For the split operation, the original signal (S) is divided into even samples set (S_e) and odd sample set (S_o). Then S_o is predicted from the S_e based on the predictor. By integrating the predicted S_o and original S_e, a new S_e is generated based on an updater. The new sample and original sample have the same feature. The inverse lifting steps are finished by reversing lifting steps, and the split is substituted for the merge.

2.2. Singular value decomposition

SVD is widely used in watermarking (Ali et al., 2015; Ali & Ahn, 2014a; Ansari et al., 2016; Vali et al., 2018), since it is a useful linear algebra matrix decomposition technology. For example, an image A performs SVD, and left singular unitary matrix U, singular diagonal matrix S and right singular unitary matrix V are obtained. Matrix U and V follow the properties $UU^T = I_n$ and $VV^T = I_n$, where I_n is unit matrix. Matrix S contains singular values which are ordered in descend. If $r(r \leq n)$ represents the rank of A, the diagonal values are decided by

$$d_1 \geq d_2 \geq \cdots \geq d_r > d_{r+1} > d_{r+2} \ldots > d_{n=0}, \tag{4}$$

where d_i is the ith singular value. A is computed by

$$A = \sum_{i=1}^{r} d_i \mu_i v_i^T,$$ (5)

where μ_i and v_i represent the ith column vector of U and V, respectively.

3. Proposed watermarking method

In this section, the proposed watermarking scheme is introduced. The watermarking embedding algorithm and extraction algorithm are described in Section 3.1 and 3.2, respectively. OAM is introduced in Section 3.3 and TDOM algorithm is detailed in Section 3.4.

3.1. Watermarking embedding algorithm

Firstly, the $M \times M$ host image H is decomposed by 1-level IWT to obtain four sub-bands: LL, LH, HL and HH, where LL represents approximate details. LH emphasizes vertical details. HL gives the horizontal details and HH provides the diagonal details. The size of each sub-band is $M/2 \times M/2$. All sub-bands are embedded watermark by multiplying different scaling factors in this work. Besides, the singular diagonal matrices of all sub-bands are obtained by SVD. Furthermore, according to the size of watermark, the singular diagonal matrices are divided into four non-overlapping matrices which are labelled as S_{i_11}, S_{i_12}, S_{i_21} and S_{i_22} ($i= LL$, LH, HL or HH). The size of S_{i_11} is same as the size of watermark. Meanwhile, watermark is embedded into S_{i_11}. Hence, the watermark W with the size of less than or equal to $M/2 \times M/2$ can be embedded into the host image by the proposed algorithm. The embedding procedure is shown in Figure 2 and the embedding algorithm is described as the following steps.

Step 1. The host image H is decomposed with 1-level IWT to obtain four sub-bands which are recorded as i.

Step 2. Sub-band i is decomposed by SVD, which is detailed by

$$U_i S_i V_i^T = SVD(i).$$ (6)

Step 3. Depending on the size of watermark, the matrix S_i is divided into four non-overlapping matrices labelled as S_{i_11}, S_{i_12}, S_{i_21} and S_{i_22}, respectively. The detailed process is introduced by

$$S_i = \begin{bmatrix} S_{i\_11} & S_{i\_12} \\ S_{i\_21} & S_{i\_22} \end{bmatrix}.$$ (7)

Step 4. The watermark is embedded into S_{i_11} by adding $\alpha_n W$ (where $n=[1, 2]$, α_1 is used for LL sub-band, and α_2 is used for other sub-bands). The detailed process is given by

$$S_i^w = \begin{bmatrix} S_{i\_11} + \alpha_n W & S_{i\_12} \\ S_{i\_21} & S_{i\_22} \end{bmatrix}.$$ (8)

6

Step 5. S_i^w is decomposed by SVD again by

$$U_{Wi}S_{Wi}V_{Wi}^T = SVD(S_i^w). \tag{9}$$

Step 6. The new modified IWT sub-band i^w is obtained by inverse SVD, which is defined by

$$i^w = U_i S_{Wi} V_i^T. \tag{10}$$

Step 7. The watermarked image H^w is obtained by

$$H^w = IWT^{-1}(i^w). \tag{11}$$

Step 8. The unique signature information is embedded into the watermarked image H^w using signature embedding process (Its generation process is detailed in Section 3.3(a)). Later, the watermarked image with signature is obtained and labelled as H_s^w.

Figure 2. Watermarking embedding procedure.

3.2. Watermarking extraction algorithm

In the extraction algorithm, the input is watermarked image with signature H_s^w that may be attacked, and the output is watermark W^E. Before extracting watermark, OAM is applied to decide if watermarking extraction process is performed to avoid FPP (OAM is detailed in Section 3.3). The extraction procedure is shown in Figure 3. Non-blind watermarking algorithm is used in this work, thus three matrices S_{i_11}, U_{Wi} and V_{Wi} are required in extraction process. The extraction process is detailed as follows. Firstly, H_s^w is decomposed by performing 1-level IWT to get four sub-bands which are labelled as i^w. Then, i^w is decomposed into three matrices by $U_i^w S_i^w V_i^{wT} = SVD(i^w)$. U_{Wi}, S_i^w and V_{Wi} are used to perform inverse SVD to obtain matrix m_i^w which contains watermark information, i.e. $m_i^w = U_{Wi}S_i^w V_{Wi}^T$. Matrix m_i^w is divided into four non-overlapping matrices of $m_{i\_11}^w$, m_{i_12}, m_{i_21} and m_{i_22}. Finally, the embedded watermark is extracted by $W_i^E = (m_{i\_11}^w - S_{i\_11})/\alpha_n$.
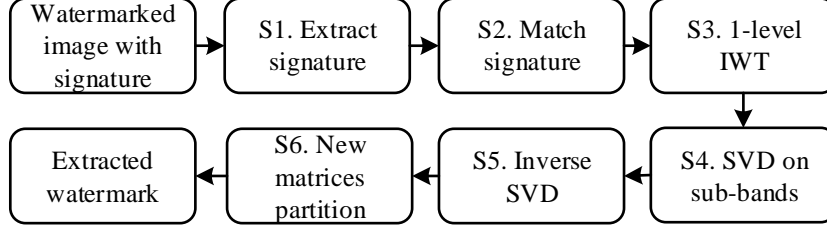
Figure 3. Watermarking extraction procedure.

3.3. The optimized authentication mechanism

OAM is applied in this work to resolve FPP. The digital signature is generated by using U_{Wi}, V_{Wi} and B (a binary array). Then, the generated signature is embedded into the watermarked image. Before the watermark is extracted, the digital signature is extracted to verify whether the extracted digital signature is equal to the embedded one. If they are identical, watermarking extraction process is performed. Otherwise, the watermarking extraction process is terminated. OAM includes signature generation, embedding and extraction processes.

(a). Signature generation process. Hash function is named as digest functions with the purpose of extracting a string with a fix bit length into a message, and it plays a major role in the file of information security (Araghi et al., 2018). Due to the irreversibility of hash function, a unique digital signature can be generated by using hash function. As a traditional hash function, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and generates a 160-bit (20-byte) hash value and it always regarded as a hexadecimal number (40 digits long) (X. Wang et al., 2018). Therefore, SHA-1 function is applied to this work to get a hash value of 160 bits. Specifically, as S_i is used to embed watermark, U_{Wi} and V_{Wi} are generated in this procedure. The signature is generated by using U_{Wi}, V_{Wi} and B. The signature generation process is provided as follows. Firstly, matrix U_{Wi} and V_{Wi} with the size of $M/2 \times M/2$ are reshaped into one-dimensional sequence with the size of $1 \times M/2 \times M/2$. Afterwards, two hashing values Sig_{Ui} and Sig_{Vi} are calculated by

$$Sig_{Ui} = Hash(U_{Wi}, SHA\text{-}1), \qquad (12)$$

and

$$Sig_{Vi} = Hash(V_{Wi}, SHA\text{-}1). \qquad (13)$$

Besides, Sig_{Ui} and Sig_{Vi} are mapped into their corresponding binary values, and $R_i = Sig_{Ui} \oplus Sig_{Vi}$ is performed to gain R_i, where $\oplus$ is XOR operation. Further, XOR operation is performed again between R_i by $R = R_{LL} \oplus R_{LH} \oplus R_{HL} \oplus R_{HH}$. A binary matrix B is selected whose dimension is same as R. Finally, the first 8 bits of R_{final} is used as the digital signature, and R_{final} is obtained by performing XOR operation between R and B via $R_{final} = R \oplus B$.

(b). Signature embedding process. Based on the analyses in previous subsections, the watermarking scheme by combining wavelet transformation and matrix

8

decomposition has a very strong robustness against different attacks. Therefore, the robustness and visual quality of watermarked image are not affected significantly after embedding the digital signature, and the algorithm based on DWT-SVD is a good choice to embed the signature (Araghi et al., 2018; Khoo et al., 2016; Thakkar & Srivastava, 2017). The signature embedding process is as follows. Initially, the watermarked image H^w is decomposed by 2-level DWT to gain LL sub-band, and LL is divided into 4×4 non-overlapping blocks. Besides, standard deviations of each block is calculated and sorted in descending order, and first eight blocks are selected to embed signature, which results in high imperceptibility (Kazemivash & Moghaddam, 2017). Finally, selected blocks are decomposed by SVD. Signature bits are embedded into the watermarked image by modifying the values in matrix U (Fan et al., 2008). When the signature bit is 1 and the absolute values of $(U_{2,1} - U_{3,1})$ are less than threshold T, $U_{2,1}$ and $U_{3,1}$ are modified by

$$\begin{cases} U'_{2,1} = sign(U_{2,1}) \times (U_{ave} + T/2) \\ U'_{3,1} = sign(U_{3,1}) \times (U_{ave} - T/2) \end{cases} \tag{14}$$

where $U_{ave} = (|U_{2,1}| + |U_{3,1}|)/2$. When the signature bit is 0 and the absolute value of $(U_{2,1} - U_{3,1})$ is greater than threshold T, $U_{2,1}$ and $U_{3,1}$ are modified by

$$\begin{cases} U'_{2,1} = sign(U_{2,1}) \times (U_{ave} - T/2) \\ U'_{3,1} = sign(U_{3,1}) \times (U_{ave} + T/2) \end{cases} \tag{15}$$

After these steps, $U_{2,1}$ and $U_{3,1}$ of each selected block are modified. Therefore, new LL sub-band is obtained when selected blocks are performed by inverse SVD. Finally, the watermarked image with signature H_s^w is obtained by inverse 2-level DWT.

(c). Signature extraction process. The signature embedding procedure is a blind solution. Hence, the embedded signature is easy to extract without depending on other information. Firstly, the watermarked image with signature H_s^w is decomposed by 2-level DWT to get LL sub-band. Then, LL sub-band is divided into 4×4 non-overlapping blocks, and eight blocks containing signature bits are selected. Selected blocks are executed via SVD and the signature bits are extracted by

$$signature(z) = \begin{cases} 0, & if \ U_{2,1} > U_{3,1} \\ 1, & if \ U_{2,1} \le U_{3,1} \end{cases} \tag{16}$$

where $z = 1,2 \dots,8$ is the signature bit.

3.4. Three-dimensional optimal mapping

As mentioned in section 1, α_n is related to the balance of imperceptibility and robustness. The greater α_n, the stronger robustness and the lower invisibility. TDOM is proposed to search the optimal α_n faster. The details of TDOM is summarized as follows. Firstly, two evaluation indicators of invisibility and robustness are used to

construct OEF. Peak Signal Noise Ratio (*PSNR*) and Structural Similarity Index Measure (*SSIM*) are used to measure the invisibility. The definition of *PSNR* is expressed by

$$PSNR(H, H^w) = 10\lg\frac{H_{max}^2}{MES}, \tag{17}$$

where H_{max} is maximum pixel value of H, and MES is mean square error between H and H^w. MES is defined by

$$MES = \frac{1}{M^2}\sum_{i=1}^{M}\sum_{j=1}^{M}[H(i,j) - H^w(i,j)]^2, \tag{18}$$

where M is the side length of H and H^w. Moreover, $SSIM$ is defined by

$$SSIM(H, H^w) = \frac{(\mu_H\mu_{H^w} + c_1)(\sigma_{HH^w} + c_2)}{(\mu_H^2 + \mu_{H^w}^2 + c_1)(\sigma_H^2 + \sigma_{H^w}^2 + c_2)}, \tag{19}$$

where μ_H and μ_{H^w} are the averages of H and H^w, σ_H^2 and $\sigma_{H^w}^2$ are variances of H and H^w, σ_{HH^w} is the covariance between H and H^w, c_1 and c_2 are two variables. The robustness is evaluated using Normalized Correlation (*NC*), and it is defined by

$$NC(W, W_i^E) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}W(i,j) \cdot W_i^E(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}[W(i,j)]^2} \cdot \sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}[W_i^E(i,j)]^2}}, \tag{20}$$

where N denotes the side length of W, (i,j) represents the coordinates of the watermark. Therefore, a new OEF is constructed using $PSNR$, $SSIM$ and NC, which is given by

$$F(\beta_x, \gamma_y) = \frac{1}{PSNR(H, H_s^w)} + \frac{1}{SSIM(H, H_s^w)} + [1 - \frac{\sum_{t=1}^{k}NC_{ave}(W, W_i^{Ek})}{K}], \tag{21}$$

where $\beta_x(x = 1,2,..,s)$ and $\gamma_y(y = 1,2,..,t)$ are the scaling factor arrays, W_i^{Ek} is the extracted watermark from K^{th} attacks, K is the amount of attacks applied to the H_s^w, NC_{ave} represents the average *NC* of four extracted watermarks and it is calculated by $NC_{ave}(W, W_i^E) = \sum NC(W, W_i^E)/4$.

According to the equation (21), the $PSNR$, $SSIM$ and NC_{ave} are inversely proportional with F, and F decrease as the $PSNR$, $SSIM$ and NC_{ave} increase. The

great $PSNR$, $SSIM$ and NC_{ave} mean that the excellent outperformance can be obtained. Moreover, each F is calculated based on β_x and γ_y, e.g., $F_1 = F(\beta_1, \gamma_1)$ or $F_2 = F(\beta_1, \gamma_2)$ and $F = [F_1, F_2, F_3, ..., F_{s \times t}]$. If F_{min} (the minimum value) is found in F, two corresponding values in arrays β_x and γ_y are obtained according to F_{min}. This process is named as TDOM algorithm. According to the equation (21), the specific initial ranges of arrays β_x and γ_y, and various attacks should be determined. In (Makbol & Khoo, 2014), the scaling factors α_1=0.05 and α_2=0.005 are selected directly. Therefore, based on these previous works, the range of 0.03~0.06 with a step of 0.01 is set for β_x, and the range of 0.002~0.008 with a step of 0.001 is set for γ_y. α_1 is found in β_x and used in LL sub-band, while α_2 is found in γ_y and used in other sub-bands. Furthermore, various attacks include No Attack (NA), Gaussian Noise (GN), Speckle Noise (SN), Salt & Peppers Noise (SPN), Average Filter (AF), Wiener Filter (WF), Gaussian Low-Pass Filter (GLPF), Median Filters (MF), JPEG compression (JPEG), JPEG2000 compression (JPEG2000), Rescaling (RE), Cropping (CR), Motion Blur (MB), Sharping (SH), Rotation (RO), Histogram Equalization (HE), Gamma Correction (GC) and Contrast Adjustment (CA). The flow chart of TDOM is shown in Figure 4. Firstly, the specific initial ranges of β_x and γ_y are set 0.03~0.06 and 0.002~0.008, respectively. For a pair of values in β_x and γ_y, the $PSNR$, $SSIM$ and NCs are calculated after the H_s^w is under aforementioned attacks. Then, a F is calculated using equation (21). Repeat these steps until the last β_x and γ_y are used, and an array F is obtained. Then the F_{min} is found in array F, and two corresponding values in β_x and γ_y are obtained, which are assigned to α_1 and α_2. The previous α_1 and α_2 are used as optimal scaling factors in this algorithm.

Figure 4. The scaling factors optimization.

4. Experiment results and analysis

In this section, the performance about invisibility and robustness of the proposed scheme is evaluated. Before testing, the specific optimal scaling factors are found by using TDOM. Then, the best values of $PSNR$, $SSIM$ and NC are calculated with the help of optimal scaling factors. In addition, the robustness and the security of this scheme are further verified by using different attack types. Finally, the performance of proposed method is compared with related works. More than ten gray-scale images are

tested. In this paper, only three commonly host images ("Man", "Lena" and "Pepper" with size of 512×512) and two gray-scale watermarks (labelled by "W_1" and "W_2" with sizes of 256×256, 128×128 and 64×64) are selected. All test images are illustrated in Figure 5.

Figure 5. Host images. (a) Man; (b) Lena; (c) Pepper; Watermark images. (d-f) W_1; (g-i) W_2.

4.1. Security test

In some SVD-based watermarking schemes, FPP is a main problem because the information (matrix U_W and V_W) is required by the watermarking extraction process. However, many SVD-based schemes cannot resolve the FPP (Lagzian et al., 2011; H.-C. Ling et al., 2013). Therefore, to enhance security of the proposed watermarking scheme, OAM is proposed to address it. In OAM, the signature including 8 bits are embedded into the watermarked image. If the recovered signature bits are not changed, it proves that the algorithm is highly secure. Table I shows the recovered signature bits comparison under different attacks. From the results, the signature bits cannot be completely recovered under CR (20 pixels each side) and RO (45 degree), but the signature bits can be completely recovered under other attacks. Compared with (Makbol & Khoo, 2014; Vali et al., 2018), the recovered results by OAM is the same as their works under different attacks. However, in some attacks, the recovered digital signature is more effective than the comparison schemes. For example, under RE (0.5) and JPEG (QF = 50), only 5-bit and 7-bit or 8-bit can be recovered in (Makbol & Khoo, 2014), while it can be completely recovered using OAM. Moreover, only 6-bit can be recovered under CR (10 pixels one side) in (Vali et al., 2018), while it can be completely recovered utilizing OAM. Specifically, different from the scheme of (Makbol & Khoo, 2014) in which only $U_{2,1}$ of U matrix of 1-level wavelet sub-band LL is used, the signature bits are embedded by slightly modifying the value of the $U_{2,1}$ and $U_{3,1}$ of U matrix of 2-level wavelet sub-band LL in this work. Besides, some related works have proved that there exists a strong correlation between the $U_{2,1}$ and $U_{3,1}$ of U matrix when SVD is used in the watermarking and it makes suitable for embedding binary data (Su et al., 2013). Moreover, the blind extraction scheme by combining 2-level DWT and SVD can resist against most types of attacks (Vali et al., 2018). Therefore, the method with OAM in this work can recover bits efficiently, and it demonstrates the security of this work can be significantly improved.

Table I. Recovered signature bits compared with (Makbol & Khoo, 2014; Vali et al., 2018).

Attack	Number of recovered bits		
	(Makbol &	(Vali et al.,	In this

12

	Khoo, 2014)	2018)	work
NA	8	8	8
GN (0.005)	-	8	8
GN (0.01)	8	8	8
SN (0.01)	8	8	8
SPN (0.01)	8	8	8
AF (3 × 3)	-	-	8
WF (3 × 3)	8	-	8
WF (5 × 5)	-	8	8
GLPF (3 × 3)	-	-	8
GLPF (5× 5)	-	8	8
MF (3 × 3)	8	-	8
MF (5 × 5)	-	8	8
JPEG (QF = 10)	-	8	8
JPEG (QF = 50)	7 or 8	-	8
JPEG2000 (CR = 12)	-	-	8
RE (0.5)	5	8	8
CR (20 pixels each side)	7	-	7
CR (10 pixels one side)	-	6	8
MB (Theta=4, Len=7)	-	-	8
SH (0.8)	-	8	8
RO (45 degree)	5	5	5
HE	-	8	8
GC (0.8)	8	-	8
CA (20%)	-	-	8

4.2. Invisibility analysis

Imperceptibility represents that the embedded information, including the watermark and digital signature, is imperceptible via the human visual system. Imperceptibility is measured by *PSNR* and *SSIM*. Generally, a minimum *PSNR* with 37dB proves that the embedded watermark is not seen through the human visual system. Moreover, when the minimum *SSIM* is 0.93, the watermarked image is slightly different with the host image (Ansari et al., 2017). The *PSNR* and *SSIM* are calculated after two watermarks "W_1" and "W_2" are embedded into three host images, respectively. Table II lists the *PSNRs* and *SSIMs* before and after embedding the digital signature when the watermark image is no attacked. According to the results of Table II, the *PSNRs* of many test images are above 45dB, and some of them even reach 48dB. Moreover, the *SSIMs* are greater than 0.99, which shows that both of the *PSNRs* and *SSIMs* are greater than the acceptable values in this paper. Moreover, the average change of *PSNR* before and after the digital signature is embedded into the watermarked image is 0.4266, and *SSIM* is 0.0008. Therefore, the distortion of host image is small and the embedded watermark cannot be seen by the human visual system, i.e. the proposed scheme has an excellent imperceptibility.

Table II. The *PSNRs* and *SSIMs* before and after embedding the digital signature when the watermark image is not attacked.

Host image	Watermark	PSNR (dB)		SSIM	
		Before	After	Before	After
Man	$W_1(d)$	47.7781	47.6514	0.9963	0.9962
	$W_1(e)$	48.4169	48.3186	0.9964	0.9962
	$W_1(f)$	48.4526	48.3887	0.9963	0.9961
	$W_2(g)$	46.1845	46.0774	0.9957	0.9956
	$W_2(h)$	47.5738	47.4375	0.9960	0.9958
	$W_2(i)$	48.1556	48.0316	0.9961	0.9959
Lena	$W_1(d)$	47.6219	46.9649	0.9954	0.9942
	$W_1(e)$	48.4969	47.7091	0.9956	0.9943
	$W_1(f)$	48.6838	47.8895	0.9955	0.9943
	$W_2(g)$	45.9090	45.4373	0.9947	0.9935
	$W_2(h)$	47.4999	46.8647	0.9950	0.9938
	$W_2(i)$	48.2443	47.3191	0.9951	0.9936
Pepper	$W_1(d)$	47.5385	46.9811	0.9951	0.9942
	$W_1(e)$	48.3323	47.7700	0.9953	0.9945
	$W_1(f)$	48.5297	48.0192	0.9954	0.9946
	$W_2(g)$	45.9330	45.6259	0.9945	0.9938
	$W_2(h)$	47.3868	46.8825	0.9948	0.9940
	$W_2(i)$	48.1055	47.7961	0.9949	0.9940
	Average	47.7135	47.2869	0.9955	0.9947

4.3. Robustness analysis

With being intentionally or unintentionally modified, robustness refers to the ability of a watermarked image to retain watermark information. Generally, the range of *NC* is from 0 to 1. When *NC* is equal to 1, it means that the extracted watermark is identical with the original watermark. In this work, two watermarks "W_1" and "W_2" are embedded into three host images, and the *NCs* of the extracted watermark are 1.0000 when the watermarked images are not attacked, i.e. watermark synchronization (Liu et al., 2019). The robustness is further analysed by using different attacks which are given in section 3.4. Specifically, Table III shows the extracted watermark "$W_1(d)$" from the watermarked image "Lena" after suffering from several different attacks including GN (0.01), SN (0.01), SPN (0.01), WF (3 × 3), MF (3 × 3), JPEG (QF = 50), RE (2), CR (20 pixels each side), RO (45 degree), HE, GC (0.8) and GA (20%). In addition, the average *NCs* of four sub-bands under various attacks for host images "Man ", "Lena " and "Pepper" are shown in Figure 6, Figure 7 and Figure 8, respectively. As shown in Table III, the extracted watermarks "$W_1(d)$" from each sub-band of watermarked image "Lena" are clearly visible, and their corresponding *NCs* are larger than 0.94. The results indicate the proposed scheme has strong robustness under different attacks. In Figure 6, almost all the average *NCs* are greater than 0.95 for host image "Man". Similar results are obtained in other images and the corresponding average *NCs* are shown in Figure 7

and Figure 8, and their average *NCs* are larger than 0.92. Thus, the aforementioned results certify the proposed scheme has high robustness.

Table III. Watermarked image with signature and the extracted watermarks under different attacks.

Attack	GN (0.01)	SN (0.01)	SPN (0.01)	WF (3×3)
Attacked watermarked image with signature				
Extracted watermarks	$NC_{LL}=0.9749$ $NC_{HL}=0.9585$ $NC_{LH}=0.9789$ $NC_{HH}=0.9775$	$NC_{LL}=0.9906$ $NC_{HL}=0.9482$ $NC_{LH}=0.9730$ $NC_{HH}=0.9785$	$NC_{LL}=0.9903$ $NC_{HL}=0.9521$ $NC_{LH}=0.9754$ $NC_{HH}=0.9794$	$NC_{LL}=0.9972$ $NC_{HL}=0.9941$ $NC_{LH}=0.9937$ $NC_{HH}=0.9933$
Attack	**MF (3×3)**	**JPEG (QF=50)**	**RE (2)**	**CR (20 pixels each side)**
Attacked watermarked image with signature				
Extracted watermarks	$NC_{LL}=0.9968$ $NC_{HL}=0.9935$ $NC_{LH}=0.9929$ $NC_{HH}=0.9943$	$NC_{LL}=0.9996$ $NC_{HL}=0.9948$ $NC_{LH}=0.9955$ $NC_{HH}=0.9962$	$NC_{LL}=0.9991$ $NC_{HL}=0.9960$ $NC_{LH}=0.9963$ $NC_{HH}=0.9951$	$NC_{LL}=0.9957$ $NC_{HL}=0.9934$ $NC_{LH}=0.9816$ $NC_{HH}=0.9967$
Attack	**RO (45)**	**HE**	**GC (0.8)**	**CA (20%)**
Attacked watermarked image with signature				
Extracted watermarks	$NC_{LL}=0.9932$ $NC_{HL}=0.9705$ $NC_{LH}=0.9926$ $NC_{HH}=0.9892$	$NC_{LL}=0.9968$ $NC_{HL}=0.9965$ $NC_{LH}=0.9962$ $NC_{HH}=0.9952$	$NC_{LL}=0.9928$ $NC_{HL}=0.9928$ $NC_{LH}=0.9928$ $NC_{HH}=0.9928$	$NC_{LL}=0.9923$ $NC_{HL}=0.9896$ $NC_{LH}=0.9896$ $NC_{HH}=0.9867$

Figure 6. Average *NCs* of four sub-band under various attacks for host image "Man" and watermarks "W_1" and "W_2", and a~r represent GN (0.01), SN (0.01), SPN (0.01), AF (3 × 3), WF (3 × 3), GLPF (3 × 3), MF (3 × 3), JPEG (QF = 50), JPEG2000 (CR = 12), RE (0.5), RE (2), CR (20 pixels each side), MB (Theta=4, Len=7), SH (0.8), RO (45 degree), HE, GC (0.8), CA (20%), respectively.

Figure 7. Average *NCs* of four sub-band under various attacks for host image "Lena" and watermarks "W_1" and "W_2", and a~r represent GN (0.01), SN (0.01), SPN (0.01), AF (3 × 3), WF (3 × 3), GLPF (3 × 3), MF (3 × 3), JPEG (QF = 50), JPEG2000 (CR = 12), RE (0.5), RE (2), CR (20 pixels each side), MB (Theta=4, Len=7), SH (0.8), RO (45 degree), HE, GC (0.8), CA (20%), respectively.

Figure 8. Average *NCs* of four sub-band under various attacks for host image "Pepper" and watermarks "W_1" and "W_2", and a~r represent GN (0.01), SN (0.01), SPN (0.01), AF (3 × 3), WF (3 × 3), GLPF (3 × 3), MF (3 × 3), JPEG (QF = 50), JPEG2000 (CR = 12), RE (0.5), RE (2), CR (20 pixels each side), MB (Theta=4, Len=7), SH (0.8), RO (45 degree), HE, GC (0.8), CA (20%), respectively.

The robustness should be further evaluated by using various attacks with dynamic parameters. Figure 9 shows the average *NCs* of four sub-bands under various attacks with different parameters. Figure 9(a), (b) and (c) are GN, SN and SPN, and their noise variances are in the range of 0.1 to 0.5 with step of 0.05. For Figure 9 (a), (b) and (c), as the noise parameter increases, the average *NCs* of the extracted watermark gradually decrease. But the reduction is not great. In addition, under same intensity attack, since different watermarks are embedded, the average *NCs* of the extracted watermarks will be slightly different. But, in general, the average *NCs* of all test images are above 0.93. Figure 9(d), (e) and (f) are WF, GLPF and MF, and their filter size is set from 2× 2 to 10× 10 with a step 1× 1. In Figure 9 (d), as the WF's filter window parameters increase, the average *NCs* of the extracted watermark are not changed much. Moreover, the average *NCs* of different filter window parameters are close to 1. For Figure 9 (e), as the GLPF's filter window parameters increase, the average *NCs* of the extracted watermark are not changed much. However, when the GLPF's filter window is odd parameter, the average *NCs* are slightly higher than the even filter window parameter. Besides, the average *NCs* are close to 1 under odd filter window parameter. In Figure 9 (f), as the MF's filter window parameter increases, the average *NCs* of the extracted watermark gradually decrease. But the reduction is not obvious. Even the MF's filter window parameter is set to 10× 10, almost all the average *NCs* of the extracted watermark are greater than 0.95. Figure 9(g) is JPEG compression with the quality factor varied from 10 to 90 with step of 10. As the quality factor increases, the average *NCs* of the extracted watermark are closer to 1. Moreover, even QF = 10, the average *NCs* of all test images are also greater than 0.96. Figure 9(g) is RO whose rotation angle varied from 5 degree to 50 degree with step of 5 degree. The average *NCs* of the extracted watermark are hardly affected by the rotation angle and the average *NCs* are larger than 0.97. Therefore, the results certify that the proposed scheme achieves a satisfactory performance.

Figure 9. Average *NCs* of each sub-band under various attacks with different parameters. (a) GN; (b) SN; (c) SPN; (d) WF; (e) GLPF; (f) MF; (g) JPEG; (h) RO.

4.4. Performance comparison

In this section, the performance of this paper is compared with related works, and Table IV shows the general comparison of this work with four state-of-the-art schemes (Ansari et al., 2016; Liu et al., 2019; Makbol et al., 2017b; Makbol & Khoo, 2014). From the Table IV, the types of watermarking algorithms designed in this work and

other comparative works are non-blind algorithms, which are designed based on wavelet transform and SVD. Similar to (Makbol & Khoo, 2014), four sub-bands obtained by conducting wavelet transformation are utilized to embed the watermark in this work. In (Ansari et al., 2016), LL, LH and HH are used, while only LL is used in (Liu et al., 2019; Makbol et al., 2017b). Moreover, the singular matrix is used to embed watermark in all schemes. Besides, the FPP is resolved in those schemes. It is worth noting that the proposed scheme can be used for watermarks with a size equal to or less than 256×256, while only three fixed-size watermarks including 256×256, 128×128 and 64×64 can be applied in (Liu et al., 2019). The remaining three schemes are only suitable for watermarks with size of 256×256. Therefore, the applicability of the proposed watermarking scheme is more flexible. The performance of proposed watermarking algorithm and other approaches is compared as follows.

In order to obtain reasonable comparison results for invisibility, 512×512 host images and 256×256 watermarks are utilized to test. Table V presents the comparisons results of *PSNR* with other watermarking techniques (Ansari et al., 2016; Liu et al., 2019; Makbol et al., 2017b; Makbol & Khoo, 2014). *PSNRs of this work are noticeably higher than other approaches for three host images. Especially, the average PSNR of (Liu et al., 2019) is only 38.1458dB, and the average PSNR is 47.1991dB in this work. When only the LL sub-band is used to embed the watermark, the PSNR of watermarked image with signature even reach 50.1099dB. Thus, the transparency of this algorithm is better than other approaches.* Furthermore, Table VI, Table VII, Table VIII and Table IX show the robustness comparisons with other works, respectively. Specifically, Table VI shows the *NC* comparisons with (Makbol & Khoo, 2014) for host "Lena" and watermark "$W_1(d)$". The *NCs* of the watermarks extracted from four sub-bands are greater than (Makbol & Khoo, 2014). Especially under SN (0.01) and SPN (0.01), the *NCs* of the extracted watermarks from four sub-bands are above 0.94 using the proposed scheme, and the minimum *NC* of (Makbol & Khoo, 2014) is 0.8067. Table VII shows the *NC* comparisons with (Liu et al., 2019) for host "Lena" and watermark "$W_2(g)$". *When only the LL sub-band is used to embed watermark, the NC values of extracted watermark are greater than (Liu et al., 2019) under different attacks. Moreover, when all sub-bands are used to embed watermark, the average NC values from all the sub-bands are still higher than (Liu et al., 2019), and the watermark capacity is four times than that of (Liu et al., 2019).* Table VIII shows *NC* comparisons with (Ansari et al., 2016) for host "Man" and watermark "$W_1(d)$". The *NCs* of the extracted watermarks from the three sub-bands using the proposed scheme are higher than (Ansari et al., 2016). Especially under GN (0.005), the minimum *NC* is 0.9660 in this work, and the minimum *NC* is 0.8054 in (Ansari et al., 2016). *Table IX shows NC comparisons with (Makbol et al., 2017a) for host "Pepper" and watermark "$W_1(d)$". From the comparisons results, whether only LL sub-band or four sub-bands are used to embed watermark, the NCs of this work are greater than (Makbol et al., 2017a) under various attacks. Moreover, the watermark capacity of this work is four times than that of (Makbol et al., 2017a) when four sub-bands are embedded with watermark. According the above comparison results, it proves that the proposed watermarking scheme outperforms other approaches in both invisibility and robustness, which are*

mainly because of the use of TDOM. Specifically, when the TDOM is used to search the optimal scaling factors, a variety of different attacks would be applied to use in OEF to conduct experiments. Then a good robustness of the extracted watermark can be completed even under different attacks. That is, the optimal scaling factors searched by TDOM can be different for different sizes of watermark. For example, as for a smaller size watermark, the optimal scaling factors searched by TDOM will increase, which can improve the robustness of extracted watermark without affecting the imperceptibility to some extent. Therefore, the robustness of this scheme is relatively high.

Table IV. Comparison of this work and other schemes.

Description	(Makbol & Khoo, 2014)	(Liu et al., 2019)	(Ansari et al., 2016)	(Makbol et al., 2017a)	This work
Scheme type	Non-blind	Non-blind	Non-blind	Non-blind	Non-blind
Main scheme	IWT+SVD	DWT+HD +SVD	IWT+SVD	IWT+SVD	IWT+SVD
Sub-bands used	All	LL	LL+LH+HL	LL	All / LL
Insertion in	S matrix	S matrix	S matrix	S matrix	S matrix
Host image size	512× 512	512× 512	512× 512	512× 512	512× 512
Watermark size	256× 256	256× 256, 128× 128, 64× 64	256× 256	256× 256	Any size
FPP	No	No	No	No	No

Table V. *PSNRs of this work and other schemes [unit: dB].*

Image	(Makbol & Khoo, 2014)	(Liu et al., 2019)	(Ansari et al., 2016)	(Makbol et al., 2017a)	In this work	
					All sub-bands	LL sub-band
Man	42.3562	-	44.4263	-	47.6514	50.4833
Lena	43.6769	38.1621	45.0326	42.9245	46.9649	50.2342
Pepper	43.4763	38.1295	44.8923	42.9477	46.9811	49.6123
Average	43.1698	38.1458	44.7837	42.9361	47.1991	50.1099

Table VI. *NCs of (Makbol & Khoo, 2014) and this work for host "Lena" and watermark "$W_1(d)$".*

Attack	(Makbol & Khoo, 2014)				In this work			
	LL	LH	HL	HH	LL	LH	HL	HH

GN (0.01)	0.9360	0.8998	0.8207	0.8959	**0.9749**	**0.9789**	**0.9585**	**0.9775**
SN (0.01)	0.9720	0.8656	0.8067	0.8995	**0.9906**	**0.9730**	**0.9481**	**0.9785**
SPN (0.01)	0.9710	0.8820	0.8234	0.9084	**0.9903**	**0.9754**	**0.9521**	**0.9794**
MF (3× 3)	0.9890	0.9758	0.9725	0.9704	**0.9968**	**0.9928**	**0.9935**	**0.9943**
WF (3× 3)	0.9890	0.9772	0.9737	0.9495	**0.9972**	**0.9937**	**0.9941**	**0.9933**
GLPF (3× 3)	0.9910	0.9324	0.9735	0.9770	**0.9977**	**0.9886**	**0.9944**	**0.9956**
JPEG (QF=30)	0.9980	0.9701	0.9773	0.8967	**0.9993**	**0.9938**	**0.9942**	**0.9873**
RE (0.5)	0.9840	0.8995	0.8753	0.9043	**0.9954**	**0.9733**	**0.9690**	**0.9811**
RE (2)	0.9980	0.9854	0.9834	0.9664	**0.9991**	**0.9963**	**0.9960**	**0.9951**
CR (30 columns)	0.9840	0.9868	0.9705	0.9870	**0.9977**	**0.9977**	**0.9981**	**0.9987**
RO (45 degree)	0.9770	0.9773	0.8983	0.9660	**0.9932**	**0.9927**	**0.9705**	**0.9892**
GC (0.6)	0.9840	0.9880	0.9847	0.9859	**0.9928**	**0.9902**	**0.9903**	**0.9871**

Table VII. *NCs* of (Liu et al., 2019) and this work for host "Lena" and watermark "$W_2(g)$".

Attacks	(Liu et al., 2019)	In this work	
		NC_{ave}	NC_{LL}
GN (0.001)	0.9864	**0.9958**	**0.9982**
MF (3× 3)	0.9685	**0.9946**	**0.9964**
WF (3× 3)	0.9682	**0.9938**	**0.9968**
GLPF (3× 3)	0.9749	**0.9952**	**0.9973**
AF (3× 3)	0.9294	**0.9684**	**0.9920**
RE (0.25)	0.9269	**0.9304**	**0.9991**
CR (2%)	0.9823	**0.9988**	**0.9996**
HE	0.9924	**0.9965**	**0.9966**
MB (Theta=4, Len=7)	0.8322	**0.9825**	**0.9910**
RO (2 degree)	0.9496	**0.9907**	**0.9996**

Table VIII. *NCs* of (Ansari et al., 2016) and this work for host "Man" and watermark "$W_1(d)$".

Attack	(Ansari et al., 2016)			In this work		
	LL	LH	HL	LL	LH	HL
GN (0.01)	0.9452	0.9035	0.8353	**0.9853**	**0.9742**	**0.9679**
GN (0.005)	0.9684	0.8859	0.8054	**0.9915**	**0.9706**	**0.9660**
MF (3× 3)	0.9898	0.9812	0.9784	**0.9958**	**0.9909**	**0.9901**
WF (2× 2)	0.9971	0.9859	0.9832	**0.9980**	**0.9953**	**0.9950**
GLPF (3× 3)	0.9914	0.9368	0.9792	**0.9974**	**0.9928**	**0.9934**

JPEG (QF=40)	0.9994	0.9745	0.9811	**0.9997**	**0.9947**	**0.9947**
RE (0.5)	0.9859	0.9078	0.8946	**0.9949**	**0.9677**	**0.9606**
RE (2)	0.9989	0.9878	0.9842	0.9986	**0.9958**	**0.9952**
CR (20 pixels each side)	0.9879	0.9881	0.9889	**0.9959**	**0.9934**	**0.9950**
SH (0.8)	0.9396	0.9483	0.9308	**0.9999**	**0.9965**	**0.9976**
RO (20 degree)	0.9869	0.9084	0.9598	**0.9927**	**0.9927**	**0.9914**
CA (20%)	0.9808	0.9791	0.9724	**0.9898**	**0.9886**	**0.9882**

Table IX. *NCs* of (Makbol et al., 2017a) and this work for host "Man" and watermark "$W_1(d)$".

Attacks	(Makbol et al., 2017a)	In this work	
		NC_{ave}	NC_{LL}
GN (0.001)	0.9810	**0.9877**	**0.9965**
GN (0.01)	0.9712	**0.9764**	**0.9853**
SN (0.1)	0.9578	**0.9733**	**0.9916**
SPN (0.05)	0.9736	**0.9756**	**0.9769**
SPN (0.01)	0.9841	**0.9819**	**0.9941**
SPN (0.1)	0.9220	**0.9696**	**0.9550**
MF (2× 2)	0.9802	**0.9929**	**0.9975**
MF (3× 3)	0.9800	**0.9930**	**0.9958**
JPEG (QF=50)	0.9811	**0.9914**	**0.9997**
JPEG (QF=75)	0.9819	**0.9961**	**0.9998**
RO (45 degree)	0.9779	**0.9930**	**0.9937**
RO (270 degree)	0.9884	**0.9954**	**0.9999**

5. Conclusion

By combining IWT with SVD, a multi-scale watermarking is proposed in this study. The SVD-based solutions may suffer from the FPP, and this problem is addressed effectively by the proposed OAM. Specifically, a novel OEF is constructed and TDOM is designed to search the optimal scaling factors, which significantly improve the invisibility and robustness of the proposed watermarked algorithm. In addition, the proposed scheme can use various sizes of watermarks. Results show that the proposed watermark scheme has good robustness against different attacks such as image compression, noise adding, cropping, scaling and sharpening. Future work will investigate the algorithm optimization and digital video watermarking.

Acknowledgements

References

Ahmad, G., Ohsawa, Y., & Nishihara, Y. (2011). Optimal design of LQR weighting matrices based on intelligent optimization methods. *International Journal of Intelligent Information Processing*, *2*(1), 1–8. https://doi.org/10.4156/ijiip.vol2

Ali, M., & Ahn, C. W. (2014a). An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Processing*, *94*(1), 545–556. https://doi.org/10.1016/j.sigpro.2013.07.024

Ali, M., & Ahn, C. W. (2014b). Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Systems with Applications*, *41*(17), 7858–7867. https://doi.org/10.1016/j.eswa.2014.10.045

Ali, M., & Ahn, C. W. (2015). Comments on optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Systems with Applications*, *42*(5), 2392–2394. https://doi.org/10.1016/j.eswa.2014.10.045

Ali, M., Ahn, C. W., Pant, M., & Siarry, P. (2015). An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Information Sciences*, *301*(11), 44–60. https://doi.org/10.1016/j.ins.2014.12.042

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security*, *6*(3), 1099–1110. https://doi.org/10.1109/TIFS.2011.2129512

Ansari, I. A., Pant, M., & Ahn, C. W. (2016). Robust and false positive free watermarking in IWT domain using SVD and ABC. *Engineering Applications of Artificial Intelligence*, *49*(1), 114–125. https://doi.org/10.1016/j.engappai.2015.12.004

Ansari, I. A., Pant, M., & Ahn, C. W. (2017). Artificial bee colony optimized robust-reversible image watermarking. *Multimedia Tools and Applications*, *76*(17), 18001–18025. https://doi.org/10.1007/s11042-016-3680-z

Araghi, T. K., Manaf, A. A., & Araghi, S. K. (2018). A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Systems with Applications*, *112*(1), 208–228. https://doi.org/10.1016/j.eswa.2018.06.024

Aslantas, V., Latif Dogan, A., & Ozturk, S. (2008). DWT-SVD based image watermarking using particle swarm optimizer. *2008 IEEE International Conference on Multimedia and Expo*, 241–244. https://doi.org/10.1109/ICME.2008.4607416

Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998). A DCT-domain system for robust image watermarking. *Signal Processing*, *66*(3), 357–372. https://doi.org/10.1016/S0165-1684(98)00015-2

Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3), 469–474. https://doi.org/10.1016/j.patcog.2003.08.007

Fan, M.-Q., Wang, H.-X., & Li, S.-K. (2008). Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, *203*(2), 926–930. https://doi.org/10.1016/j.amc.2008.05.003

Farid, H. (2009). A survry of image forgery detection. *IEEE Signal Processing Magazine*, *26*(2), 16–25. https://doi.org/10.1109/MSP.2008.931079

Guo, Y., Li, B.-Z., & Goel, N. (2017). Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. *IET Image Processing*, *11*(6), 406–415. https://doi.org/10.1049/iet-ipr.2016.0515

Hsieh, M. S., Tseng, D. C., & Huang, Y. H. (2001). Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transactions on Industrial Electronics*, *48*(5), 875–882. https://doi.org/10.1109/41.954550

Jia, Z., Zhu, H., & Cheng, W. (2010). A blind watermarking algorithm based on lifting wavelet transform and scrambling technology. *2010 International Conference on Electrical and Control Engineering*, 4576–4579. https://doi.org/10.1109/iCECE.2010.1105

Kazemivash, B., & Moghaddam, M. E. (2017). A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. *Multimedia Tools and Applications*, *76*(20), 20499–20524. https://doi.org/10.1007/s11042-016-3962-5

Khoo, B. E., Makbol, N. M., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, *10*(1), 34–52. https://doi.org/10.1049/iet-ipr.2014.0965

Lagzian, S., Soryani, M., & Fathy, M. (2011). Robust watermarking scheme based on RDWT-SVD: embedding data in all subbands. *2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, 48–52. https://doi.org/10.1109/AISP.2011.5960985

Ling, H.-C., Phan, R. C.-W., & Heng, S.-H. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU - International Journal of Electronics and Communications*, *67*(10), 894–897. https://doi.org/10.1016/j.aeue.2013.04.013

Ling, H. C., Phan, R. C. W., & Heng, S. H. (2013). Comment on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU - International Journal of Electronics and Communications*, *67*(10), 894–897. https://doi.org/10.1016/j.aeue.2013.04.013

Liu, J., Huang, J., Luo, Y., Cao, L., & Yang, S. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. *IEEE Access*, *7*(1), 80849–80860. https://doi.org/10.1109/ACCESS.2019.2915596

Loukhaoukha, K., Chouinard, J.-Y., & Taieb, M. H. (2011). Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization. *Journal of Information Hiding and Multimedia Signal Processing*,

2(4), 303–319. https://doi.org/https://doi.org/10.1016/j.eswa.2014.06.011

Luo, Y., Cao, L., Qiu, S., Lin, H., Harkin, J., & Liu, J. (2016). A chaotic map-control-based and the plain image-related cryptosystem. *Nonlinear Dynamics*, *83*(4), 2293–2310. https://doi.org/10.1007/s11071-015-2481-7

Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., & Zhou, R. (2019). A robust image encryption algorithm based on chua's circuit and compressive sensing. *Signal Processing*, *161*(1), 227–247. https://doi.org/10.1016/j.sigpro.2019.03.022

Luo, Y., Ouyang, X., Liu, J., & Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, *7*(1), 38507–38522. https://doi.org/10.1109/ACCESS.2019.2906052

Luo, Y., Zhou, R., Liu, J., Cao, Y., & Ding, X. (2018). A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. *Nonlinear Dynamics*, *93*(3), 1165–1181. https://doi.org/10.1007/s11071-018-4251-9

Makbol, N. M., & Khoo, B. E. (2014). A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing*, *33*(1), 134–147. https://doi.org/10.1016/j.dsp.2014.06.012

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2018). Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. *Multimedia Tools and Applications*, *77*(20), 26845–26879. https://doi.org/10.1007/s11042-018-5891-y

Makbol, N. M., Khoo, B. E., Rassem, T. H., & Loukhaoukha, K. (2017a). A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. *Information Sciences*, *417*(1), 381–400. https://doi.org/10.1016/j.ins.2017.07.026

Makbol, N. M., Khoo, B. E., Rassem, T. H., & Loukhaoukha, K. (2017b). A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. *Information Sciences*, *417*(1), 381–400. https://doi.org/10.1016/j.ins.2017.07.026

Malvar, H. S., & Florêncio, D. A. (2002). Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing*, *4*(4), 898–905. https://doi.org/10.1109/icassp.2002.5745359

Muhammad, N., & Bibi, N. (2015). Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. *IET Image Processing*, *9*(9), 795–803. https://doi.org/10.1049/iet-ipr.2014.0395

Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. *Signal Processing*, *66*(3), 385–403. https://doi.org/https://doi.org/10.1016/S0165-1684(98)00017-6

Pan, J., Bisht, J., Kapoor, R., & Bhattacharyya, A. (2010). Digital image watermarking in integer wavelet domain using hybrid technique. *2010 International Conference on Advances in Computer Engineering*, 163–167. https://doi.org/10.1109/ACE.2010.41

Pun, C. (2006). A novel DFT-based digital watermarking system for images. *2006 8th*

International Conference on Signal Processing, 3–6. https://doi.org/10.1109/ICOSP.2006.345581

Qi, X., & Xin, X. (2011). A quantization-based semi-fragile watermarking scheme for image content authentication. *Journal of Visual Communication and Image Representation*, *22*(2), 187–200. https://doi.org/10.1016/j.jvcir.2010.12.005

Rastegar, S., Namazi, F., Yaghmaie, K., & Aliabadian, A. (2011). Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEU - International Journal of Electronics and Communications*, *65*(7), 658–663. https://doi.org/10.1016/j.aeue.2010.09.008

Singh, D., & Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, *76*(11), 13001–13024. https://doi.org/10.1007/s11042-016-3706-6

Su, Q., Niu, Y., Liu, X., & Zhu, Y. (2012). A blind dual color images watermarking based on IWT and state coding. *Optics Communications*, *285*(7), 1717–1724. https://doi.org/10.1016/j.optcom.2011.11.117

Su, Q., Niu, Y., Zou, H., & Liu, X. (2013). A blind dual color images watermarking based on singular value decomposition. *Applied Mathematics and Computation*, *219*(16), 8455–8466. https://doi.org/10.1016/j.amc.2013.03.013

Sweldens, W. (1998). The lifting scheme: a construction of second generation wavelets. *SIAM Journal on Mathematical Analysis*, *29*(2), 511–546. https://doi.org/10.1137/S0036141095289051

Thakkar, F. N., & Srivastava, V. K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, *76*(3), 3669–3697. https://doi.org/10.1007/s11042-016-3928-7

Tian, Y., Tan, T., Wang, Y., & Fang, Y. (2003). Do singular values contain adequate information for face recognition? *Pattern Recognition*, *36*(3), 649–655. https://doi.org/10.1016/S0031-3203(02)00105-X

Vali, M. H., Aghagolzadeh, A., & Baleghi, Y. (2018). Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. *Expert Systems with Applications*, *114*(1), 296–312. https://doi.org/10.1016/j.eswa.2018.07.004

Wang, X., Zhu, X., Wu, X., & Zhang, Y. (2018). Image encryption algorithm based on multiple mixed hash functions and cyclic shift. *Optics and Lasers in Engineering*, *107*(1), 370–379. https://doi.org/10.1016/j.optlaseng.2017.06.015

Wang, Y., Doherty, J. F., & Van Dyck, R. E. (2002). A wavelet-based watermarking algorithm for ownership verification of digital images. *IEEE Transactions on Image Processing*, *11*(2), 77–88. https://doi.org/10.1109/83.982816

Wong, P. W., & Memon, N. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, *10*(10), 1593–1601. https://doi.org/10.1109/83.951543

Yadav, B., Kumar, A., & Kumar, Y. (2018). A robust digital image watermarking algorithm using DWT and SVD. *Advances in Intelligent Systems and Computing*, *583*(1), 25–36. https://doi.org/10.1007/978-981-10-5687-1_3

Zhang, X., & Wang, S. (2008). Fragile watermarking with error-free restoration capability. *IEEE Transactions on Multimedia*, *10*(8), 1490–1499. https://doi.org/10.1109/TMM.2008.2007334