Journal of Computers Vol. 28, No. 1, 2017, pp. 167-179
doi:10.3966/199115592017022801013

A Novel Approach to Image Authentication with Tamper Localization and Self-Recovery

Zhen Liu, Yue-Sheng Zhu, Yi Fan, and Xiao-Mei Xing

Lab of Communication and Information Security, Institute of Big Data Technologies,
Shenzhen Graduate School, Peking University, Shenzhen, 518055, China
{l.zhen, zhuys, fanyi, xingxiaomei}@sz.pku.edu.cn

Received 21 September 2015; Revised 10 December 2015; Accepted 13 April 2016

Abstract. In this paper, a novel dual watermarking scheme for image authentication is proposed with the ability of tamper localization and self-recovery based on compressive sensing (CS) and DWT-SVD (singular value decomposition). The original image is first divided into sub-blocks, and for each block two different watermarks can be generated: One is obtained from CS which can be further used for self-recovery; the other is acquired based on DWT-SVD which is extremely robust to non-malicious processing operations. The two watermarks are both embedded in the singular values of the host image with a novel method to guarantee the invisibility of the proposed watermarking scheme. During the authentication procedure, a novel approach for adaptive threshold selection is proposed. Our analysis and experimental results demonstrate that the proposed scheme can precisely distinguish malicious and non-malicious attacks. In addition, the maliciously tampered regions can be accurately localized and further recovered with high quality as well.

Keywords: compressive sensing, dual watermarking, image authentication, singular value decomposition, tamper localization and self-recovery

1 Introduction

Along with the speeding up of the process of digitalization and the increasing popularity of multimedia applications, multimedia processing technologies and specific software are more and more powerful. Consequently, the editing and processing of digital works is becoming exceedingly easy. Hence, verifying the authenticity and integrity of multimedia contents has become an urgent issue. Watermarking scheme has been proven to be an efficient technique for content-based authentication [1-2]. In a typical watermarking scheme, a watermark is first embedded into the multimedia content, and later extracted for authentication purposes. However, traditional watermarking schemes can hardly balance the tradeoff between imperceptibility, security, robustness and recovery capability.

In recent years, a new theory which is known as compressive sensing has brought about fresh inspiration for content-based authentication. The basic principle of CS is that a sparse signal can be perfectly recovered from a small set of linear, incoherent, non-adaptive measurements [3]. The CS-based watermarking schemes for content-based multimedia authentication mainly include the following several advantages: First, the measurements obtained in the observation process not only contain all the information of the original signal, but the amount of the data is much smaller. Meanwhile the tampering of the original signal can be amplified in the observation process so that similar signals will produce quite different measurements, and the accuracy of tamper detection and localization can be guaranteed accordingly. Additionally, the random observation can be regarded as a process of encryption, where the random seed of the observation matrix can be considered as the secret key which is only known to the sender and authorized receivers. Without the prior knowledge of the key, it is impossible for the attackers to proceed the observation process with the received image.

Several CS-based watermarking schemes for content-based authentication have been explored in the literature [4-6]. Veena et al. [4] combined Arnold scrambling with compressive sensing to propose a scheme with high security. However, compressive sensing is only applied here to encryption, and the tampered regions cannot be localized and recovered. In [5] a robust watermarking scheme was proposed based on CS and distributed source coding. This method can be used for tampering identification and localization to some extent. However, this scheme is only applicable in cases where the attack is sparse, which is not always flexible in practical applications. In order to recover the tampered regions, T. Emmanuel et al. [6] proposed a robust watermarking scheme by embedding the CS measurements into LSB of the host image for multiple times to ensure the accuracy of the reconstruction. However, the authors make no discussion about how to deal with the conflict between the imperceptibility and robustness of the watermarking scheme. I. Orovic et al. [7] analyzed the performance of watermark detection under the attack of compressive sensing. The watermark is embedded into the DCT coefficients of the host image. Before the watermark extraction procedure, the watermarked image is processed with compressed sensing. The paper demonstrated that the watermark cannot be reliably detected and retrieved even though the reconstructed image has a high visual quality. I. Orovic et al. [8] proposed an image watermarking scheme based on compressive sampling. The watermark is embedded into some randomly chosen measurements form image blocks. At the received end, the image is reconstructed from the watermarked measurements with the total variation minimization algorithm to ensure the quality of the recovered image. And the embedded watermark can be detected and retrieved from the recovered image afterwards. The choosing mechanism not only enhances the transparency of the proposed watermarking scheme, but the security can also be guaranteed. Y. W. Jiang et al. [9] proposed a watermarking scheme based on DWT and block compressed sensing (BCS). The original image is divided into server non-overlapping blocks, and for each block the watermark in LL sub-band of the host image in DWT domain. The use of BCS improved the performance of the watermarking scheme in terms of robustness and Computational Complexity. In the algorithms proposed in [8-9], watermark is directly embedded into the compressive sampling measurements, as a result, the robustness of these watermarking scheme is degraded. In order to enhance the robustness, X. F. Chi et al. [10] presented a watermarking scheme based on SVD and compressed sensing. The watermark is embedded into the singular values of the host image in CS transform domain. And the transparency of this method is favorable as well. M. Yamac et al. [11] proposed a new watermarking encoding-decoding algorithm that exploits the sparsity of the signal to achieve dense watermarking scheme. The proposed algorithm is robust under white Gaussianoise and impulsive noise, and the embedding capacity outperforms both classical l_1 and l_2 methods. H. M. Zhao et al. [12] presented a secure semi-fragile compressed sensing based watermarking scheme for video authentication in cloud environment. The watermark is generated by CS measurements which can express all features of the original video frame. The measurements values possess an encryption property from random elements of sensing matrix, consequently, the security pf the proposed authentication scheme is guaranteed. However, a common drawback of these CS-based watermarking schemes is that the performance of robustness gets worse as the growing of the strength of the non-malicious attacks.

On the other hand, SVD-based watermarking schemes are always robust against incidental attacks [13], such as noise, loss compression, filtering etc. and consequently are widely explored for content-based authentication. X. H. Ma et al. [14] proposed a grayscale blind watermarking scheme based on SVD. Each bit of the watermark is embedded into the corresponding host image block by the quantification of largest singular value. And Arnold chaos is utilized to ensure the security. The proposed method is blind and quite robust to signal processing operations and some geometric distortions. X. L. Jia et al. [15] proposed an anti-geometric attack SVD digital watermark algorithm based on geometric center and image mass centroid. The principle of geometric invariance is based on the invariance of geometric center and image centroid. This method can not only resist signal processing attacks such as noise, loss compression, filtering etc., but also has favorable robustness against geometric attacks such as rotation, scaling and translation. M. A. Kayum Hawlader et al. [16] presented a robust and secure dual watermarking scheme for copyright protection in SVD domain. The primary watermark is embedded into secondary watermark, and the secondary watermark is embedded into the host image by modifying corresponding singular values (SVs). In order to provide high security, Logistic map is used to encrypt the primary watermark and Arnold is utilized to scramble the cover image. The proposed scheme offers superior robustness against various attacks. Moreover, in order to improve the performance of watermarking schemes in terms of robustness, transparency etc., more and more researchers devote themselves to hybrid (SVD related) watermarking algorithms. W. Wang et al. [17] combined DWT and SVD to construct a zero watermarking scheme. However, an intellectual property rights (IPR) database is needed to register the zero-watermark, as a result, the capacity of the database is a limitation of the proposed system. Y. Pathak et al. [18] provided a secure transmission way for medical images by using DWT-SVD based watermarking technique. The watermark is embedded into the host image in DWT-SVD domain to ensure the robustness of this scheme. P. Mitra et al. [19] presented an image watermarking scheme based on Contourlet Transform (CT) and SVD. The singular values of watermark after the QR and SVD decomposition is embedded into the singular values of the original image after the CT and SVD decomposition technique. The proposed method is quite robust against attacks such as JEPG compression, Gaussian noise, scaling, low-pass filtering etc. However, the common drawback SVD-related watermarking schemes is that the tampered regions cannot be efficiently recovered.

The attractive properties and existing drawbacks of CS-based and SVD-based watermarking schemes motivate us to propose a novel dual watermarking scheme for image content-based authentication, in which a new DWT-SVD based watermark is presented, and a modification is made to the algorithm in [6] to generate our CS-based watermark. The dual watermark is embedded into the singular values (SVs) of the host image in a smart way. Due to the fact that slight modifications of the SVs do not affect the visual perception of the host image, the transparency of our dual watermarking scheme can be guaranteed. The novel SVD-based watermark has strong robustness against common image processing operations and consequently can be extracted for tamper detection and localization, while the CS-based watermark is responsible for self-recovery of the tampered region. During the watermark embedding and extracting processes, the chaotic mapping is applied to enhance the security of the proposed system. The theory analyses and experimental results demonstrate that the proposed dual watermarking scheme has favorable ability of tamper localization and self-recovery with good imperceptibility and strong robustness ensured.

The rest of this paper is organized as follows: Section 2 provides a general introduction of compressed sensing and singular value decomposition. Section 3 elaborates our proposed authentication system. Next, the experimental results and corresponding analyses are discussed in section 4. Finally, several concluding remarks are given in section 5.

2 Background

2.1 Basic Principle of Compressive Sensing

For a one-dimensional discrete real signal $f \in R^N$, f can be represented in an orthogonal basis Ψ as:

$$f = \sum_{i=1}^{N} \psi_i x_i \qquad or \qquad f = \Psi x \tag{1}$$

Where x=[x_1, x_2,…, x_N] is the corresponding coefficient vector. If only K(K<N) out of N coefficients of X are nonzero, X is called a K-sparse vector, in other word, the original signal f can be called a K-sparse signal under the basic Ψ . And then M(M<N) linear, non-adaptive random measurements can be obtained in the observation process, namely,

$$y = \Phi f = \Phi \Psi x = \Theta x \tag{2}$$

Where $\Phi \in R^{M \times N}$ is the measurement matrix which is uncorrelated to Ψ . And Θ is called the information operator. It is proven [22][24] that if the matrix Θ satisfies the restricted isometry property (RIP) principle [22], x can be reconstructed precisely with proper reconstruction algorithm. For a K-sparse signal $f \in R^N$, if there exists a $\delta_K \in (0,1)$ such that

$$(1-\delta_K)\|x\|_2^2 \le \|\Theta x\|_2^2 \le (1+\delta_K)\|x\|_2^2 \tag{3}$$

it can be considered that Θ satisfies the RIP. And x can be reconstructed from M (where $M \ge O(Klog(N/K))$) measurements with high probability by solving a l_0 norm problem as follows:

$$\begin{aligned} &\hat{x} = \arg\min_{x} \ \|x\|_0 \\ &\text{s.t. } \Theta x = y \end{aligned} \tag{4}$$

However, (4) is a NP-hard problem which is difficult to be solved in practice. An alternative approach to address this problem is to convert the l_0-norm into its convex approximation, i.e. the l_1-norm optimization problem which is depicted as:

$$\begin{aligned} &\hat{x} = \arg\min_x \ \|x\|_1 \\ &\text{s.t. } \Theta x = y \end{aligned} \quad \textbf{(5)}$$

Furthermore, in most practical situations, the measurement vector is probably affected by noise (e.g. quantization noise). Hence the observation process can be amended as $y = \Theta x + n$, where n is a norm-bound noise. Assume that $\|n\|_2 < \sigma$, and then (5) can be modified as follows:

$$\begin{aligned} &\hat{x} = \arg\min_x \ \|x\|_1 \\ &\text{s.t. } \|y - \Theta x\|_2 \le \sigma \end{aligned} \quad \textbf{(6)}$$

Typical reconstruction algorithms include pursuit reconstruction algorithms and greedy iterative algorithms. After x is reconstructed, f can be eventually recovered by simply employing the corresponding inverse transformation.

2.2 Singular Value Decomposition

Singular Value Decomposition (SVD) is an effective tool for matrix analysis which is widely utilized for image processing [25]. For a given grayscale image $A = R^{m\times n}$. It can be decomposed into a product of three matrices in the following form:

$$A = USV^T = \sum_{i=1}^{r} \lambda_i U_i V_i \quad \textbf{(7)}$$

Where r is the rank of A, and the orthogonal matrices $U = R^{m\times m}$ and $V = R^{n\times n}$ are the left singular matrix and right singular matrix of A, respectively. S is a diagonal matrix which can be expressed as follows:

$$S = diag(\lambda_1, \lambda_2, ..., \lambda_r) \quad \textbf{(8)}$$

where $\lambda_1 > \lambda_2 > \cdots > \lambda_r$ are the singular values of A, respectively. SVD mainly has the following several attractive properties: (a) Singular values (SVs) specify the luminance of the image layers and represent the intrinsic property rather than visual perception of the image; (b) Slight variations of the SVs do not affect the visual perception of the image too much; (c) SVs are extremely stable when facing with common image processing operations.

These properties are explored and expanded in this paper. To be specific, (a) and (b) motivate us to extract the biggest SV of each image block to form a robust watermark while (c) give us inspiration to embed the proposed dual watermark by slightly modifying the SVs of the host image to guarantee the invisibility of the proposed scheme.

3 Proposed Authentication System

The proposed scheme for tamper localization and self-recovery is depicted in Fig. 1. In this section, the watermark generating and embedding procedures are first introduced, and the watermark extracting procedure is introduced afterwards, at last, the judgment method, which contains tamper localization and self-recovery, is detailed.

3.1 Watermark Generation

In this part, the CS-based watermark and the DWT-SVD based watermark are respectively generated from the original image. The original image $F = R^{N\times N}$ is first divided into sub-blocks, whose size ($B \times B$) can be adjusted according to the expected accuracy of tamper localization. The number of the blocks is assumed to n, i.e. $n = N^2 / B^2$. Generally, the smaller the block size is, the higher localization accuracy

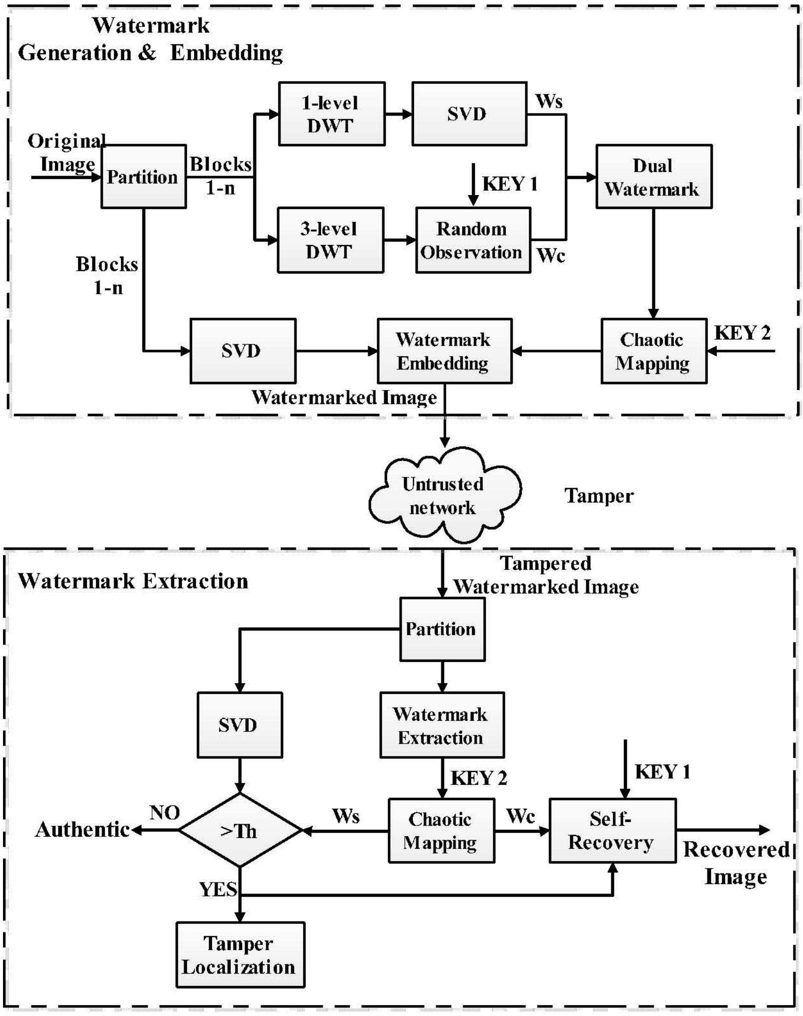


Fig. 1. Block diagram of the proposed image authentication scheme

can be provided. The following watermark generation and embedding procedures are executed to all the blocks, sequentially.

Generation of the DWT-SVD based watermark WS. The DWT-SVD based watermark is generated in this procedure which can be further utilized to distinguish malicious and non-malicious attacks. This process is performed as follows:

Step.1 1-level DWT: Take the block *i* for example, 1-level DWT is applied to decompose block *i* into four sub-bands, i.e. *LL, LH, HL, HH*. The majority of the information of block *i* is focused in *LL*.

Step.2 Singular value decomposition: SVD is performed on *LL* of each block, this process can be described as follows:

$$LL_i = USV^T = \sum_{j=1}^{r} \lambda_{ij} U_{ij} V_{ij} \tag{9}$$

The biggest singular value of each block is extracted to form the robust watermark *WS* which can be expressed as:

$$WS = [\lambda_{11}, \cdots, \lambda_{i1}, \cdots, \lambda_{n1}] \tag{10}$$

Generation of the CS-based watermark WC. In this procedure, the recovery watermark is generated based on CS. The specific steps are described as follows:

Step.1 Sparse Representation: Take the block *i* for example again, f_i is the 1-D representation of block *i*. The first step of CS is to find a sparse representation of each block. However, most signals are not sparse in spatial domain, but fortunately natural signals are approximatively sparse in some transform domain. In this paper, *3*-level DWT is applied to each block where the bi-orthogonal *9/7* wavelet basis

[26] is chosen as the sparse basis, and the transform coefficients $x_i(x_i = \Psi^T f_i)$ are the approximatively sparse representation of the block *i*.

Step.2 Random Observation: Designing a stable observation matrix Φ which is unrelated with the transform matrix Ψ is extremely important for the self-recovery procedure. Here the Gaussian random matrix is used as the observation matrix as it is uncorrelated to almost all the orthogonal matrices. Moreover, this process can be considered as an encryption operation where the seed of the Gaussian random matrix can be regarded as the secret ***key*** for the system. This process can be expressed as: $Y_i = \Phi f_i = \Phi \Psi x_i = \Theta x_i$. And WC can be represented as:

$$\begin{aligned} &WC = [WC_1, \cdots, WC_i, \cdots WC_n] \\ &s.t.\ WC_i = Y_i = [y_{i1}, y_{i2}, \cdots, y_{iM}]. \end{aligned} \tag{11}$$

3.2 Watermark Embedding

The dual watermark is required to embed into the singular values of the host image. In order to enhance the accuracy of tamper localization and self-recovery, the watermark generated form each block is respectively embedded into two different blocks: one is into the block itself, the other block is obtained by means of a chaotic mapping sequence. The specific steps of this procedure are show as follows:

Step 1. Generate the Logistic Chaotic mapping sequence by means of Logistic Chaotic Mapping.

$$S_{i+1} = \mu S_i(1 - \mathrm{S}_i) \tag{12}$$

Where $\mu \in (3.5699456, 4]$, $S_i \in (0,1)$ and $S = [s_1, s_2, \cdots, s_n]$ is a chaotic sequence. And then a stable sorting algorithm is performed to *S*, and an ordered sequence $S_a = [S_{a_1}, S_{a_2}, \cdots, S_{a_n}]$ can be obtained afterwards. And the mapping function can be expressed as $y = f(i) = a_i$, i.e. the watermark generated from block *i* is required to embed into block *i* and a_i. In this procedure, the chaotic sequence will change enormously according to the initial value s_1, which can be regarded as the secret ***key*** of the chaotic system.

Step 2. Perform SVD on the blocks of the host image. (block a_i for example, the following step 3, 4, 5 are the same**)**

$$f_{a_i} = U_{a_i} S_{a_i} V_{a_i}{}^T = \sum_{j=1}^{r} \lambda_{a_i j} U_{a_i j} V_{a_i j} \tag{13}$$

Step 3. Embed the dual watermark into the corresponding singular value matrix.

$$D_{a_i} = S_{a_i} + b_2 * (WS_i + WS_{a_i}) + b_1 * (WC_i + WC_{a_i}) \tag{14}$$

Where b_1 and b_2 is strength factor of WC and WS, respectively, here b_1 and b_2 can be adjusted according to the tradeoff between the imperceptibility of the watermarked image and the accuracy of the extracted watermark.

In order to illustrate more clearly, we use the following Fig. 2 to show the mechanism of this step (assume that the block size is $8*8$). The compression rate in compressive sensing is 0.4, thus $\lfloor 8 \wedge 2 * 0.4 \rfloor = 25$ measurements can be obtained from each block. The proposed embedding method is quite balanced which is beneficial for the accuracy of the extracted watermark.

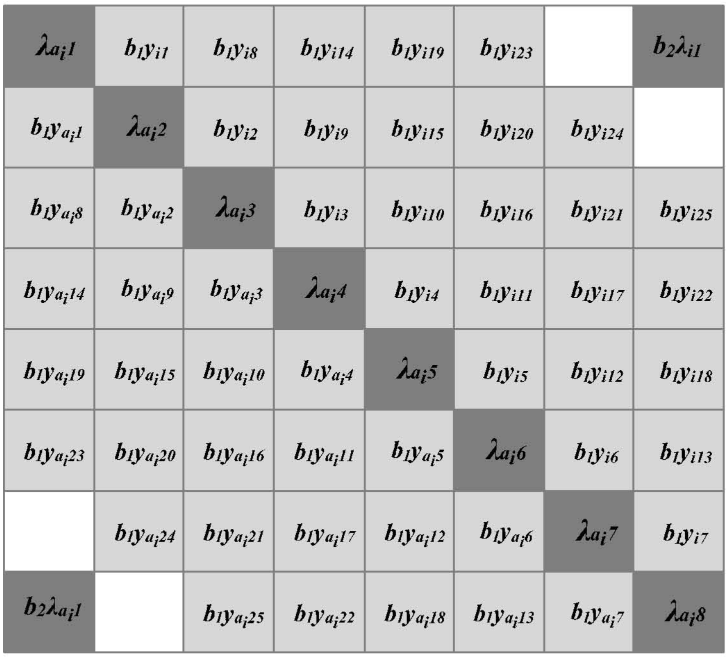
Step 4. Perform SVD on the new singular value matrix D_{a_i}

$$D_{a_i} = U_{a_i w} S_{a_i w} V_{a_i w}{}^T \tag{15}$$

Step 5. Obtain the watermarked image by applying:

$$f_{a_i w} = U_{a_i} S_{a_i w} V_{a_i}{}^T \tag{16}$$

Where $f_{a_i w}$ is the watermarked block, the watermarked image can be obtained after all the blocks are embedded with the proposed dual watermark.



λ_{a_i1}	b_1y_{i1}	b_1y_{i8}	b_1y_{i14}	b_1y_{i19}	b_1y_{i23}		$b_2\lambda_{i1}$
$b_1y_{a_i1}$	λ_{a_i2}	b_1y_{i2}	b_1y_{i9}	b_1y_{i15}	b_1y_{i20}	b_1y_{i24}	
$b_1y_{a_i8}$	$b_1y_{a_i2}$	λ_{a_i3}	b_1y_{i3}	b_1y_{i10}	b_1y_{i16}	b_1y_{i21}	b_1y_{i25}
$b_1y_{a_i14}$	$b_1y_{a_i9}$	$b_1y_{a_i3}$	λ_{a_i4}	b_1y_{i4}	b_1y_{i11}	b_1y_{i17}	b_1y_{i22}
$b_1y_{a_i19}$	$b_1y_{a_i15}$	$b_1y_{a_i10}$	$b_1y_{a_i4}$	λ_{a_i5}	b_1y_{i5}	b_1y_{i12}	b_1y_{i18}
$b_1y_{a_i23}$	$b_1y_{a_i20}$	$b_1y_{a_i16}$	$b_1y_{a_i11}$	$b_1y_{a_i5}$	λ_{a_i6}	b_1y_{i6}	b_1y_{i13}
	$b_1y_{a_i24}$	$b_1y_{a_i21}$	$b_1y_{a_i17}$	$b_1y_{a_i12}$	$b_1y_{a_i6}$	λ_{a_i7}	b_1y_{i7}
$b_2\lambda_{a_i1}$		$b_1y_{a_i25}$	$b_1y_{a_i22}$	$b_1y_{a_i18}$	$b_1y_{a_i13}$	$b_1y_{a_i7}$	λ_{a_i8}

Fig. 2. The proposed mechanism of the watermark embedding

3.3 Watermark Extraction

Step 1. Employ the same Logistic Chaotic Mapping to generate the mapping sequence by means of the same secret key as is described in 3.2.

Step 2. Perform SVD on each block of the received image **(**block a_i for example, the following step 3, 4, 5 are the same**)**

$$f^*_{a_iw} = U^*_{a_i} S^*_{a_iw} V^{*T}_{a_i} \tag{17}$$

Step 3. Obtain the predicted singular value matrix $D^*_{a_i}$ which contains the dual watermark by applying:

$$D^*_{a_i} = U_{a_iw} S^*_{a_iw} V_{a_iw}{}^T \tag{18}$$

Step 4. Extract the dual watermark from $D^*_{a_i}$ as follows:

$$b_2 * (WS^*_i + WS^*_{a_i}) + b_1 * (WC^*_i + WC^*_{a_i}) = D^*_{a_i} - S_{a_i} \tag{19}$$

Both the dual watermarks W_i and W_{ai} can be extracted from block a_i in this step. Consequently, if block *i* is tampered and the information embedded in block *i* is lost, block *i* can still be recovered with the information extracted from block a_i. However, if W_i is failed to be extracted from block i and block a_i, there would not be enough information to recover the tampered block *i*. In this situation, we first localize the block where the recovered information is lost, and then employ bilinear interpolation to get the approximate pixels of the block.

3.4 Tamper Localization and Self-recovery

In this step, the dual watermark extracted in the above steps is utilized here for content-based image authentication where the tampered regions can be localized and further recovered. *WS* is first utilized here verifying the authenticity of each block, and *WC* is employed for self-recovery of the tampered regions afterwards.

Authentication with tamper localization. The watermark *WS* is singularly robust to non-malicious processing operations. Thus *WS* can be applied here for content-based authentication by calculating the distance between WS^* and S_{max} of the received image as follows:

$$d(WS_i^*, S_{\max i}) = \left|\lambda_{i1}^* - \overline{\lambda}_{i1}\right| \quad s.t. \begin{cases} WS^* = [\lambda_{11}^*, \lambda_{21}^*, \cdots, \lambda_{i1}^*, \cdots, \lambda_{n1}^*] \\ S_{max} = [\overline{\lambda}_{11}, \overline{\lambda}_{21}, \cdots, \overline{\lambda}_{i1}, \cdots, \overline{\lambda}_{n1}] \end{cases} \tag{20}$$

Where i=1,2,…, n is the id of each block, and S_{max} is a matrix about the biggest singular value of each block of the received image. And an appropriate threshold *TH* is utilized here to distinguish whether block *i* has been malicious tampered according to the following rules:

(i) $if\ \ d(WS_i, S_{\max i}) > TH\ \ then\ block\ i\ is\ tampered,$

(ii) $if\ \ d(WS_i, S_{\max i}) < TH\ \ then\ block\ i\ is\ authentic.$

The threshold *TH* is related to strength of non-malicious attacks and malicious attacks, thus it can be defined as follows:

$$TH = t_1 + \alpha t_2 \tag{21}$$

Where t_1 is average distortion caused by non-malicious processing operations, while t_2 is the smallest distortion of the biggest singular value of all the blocks caused by malicious attacks. And α is a strength factor which is correlated with t_1. Obviously, α satisfy the following roles:

(i) $if\ \ t_1$=0, $then\ \alpha$=0,

(ii) $\alpha\ and\ t_1\ are\ positively\ correlated.$

Thus the correlative parameters can be defined as follows:

$$\begin{aligned} t_1 &= C_1 \\ t_2 &= min(d(WS^*, WS)) \\ \alpha &= C_2 log(\frac{t_1}{C_3} + 1) \end{aligned} \tag{22}$$

Where C_2 and C_3 are correction factors. And C_1, C_2, C_3 are empirical constants, which are experimentally set as 200.0, 50.0 and 2.5 in this paper.

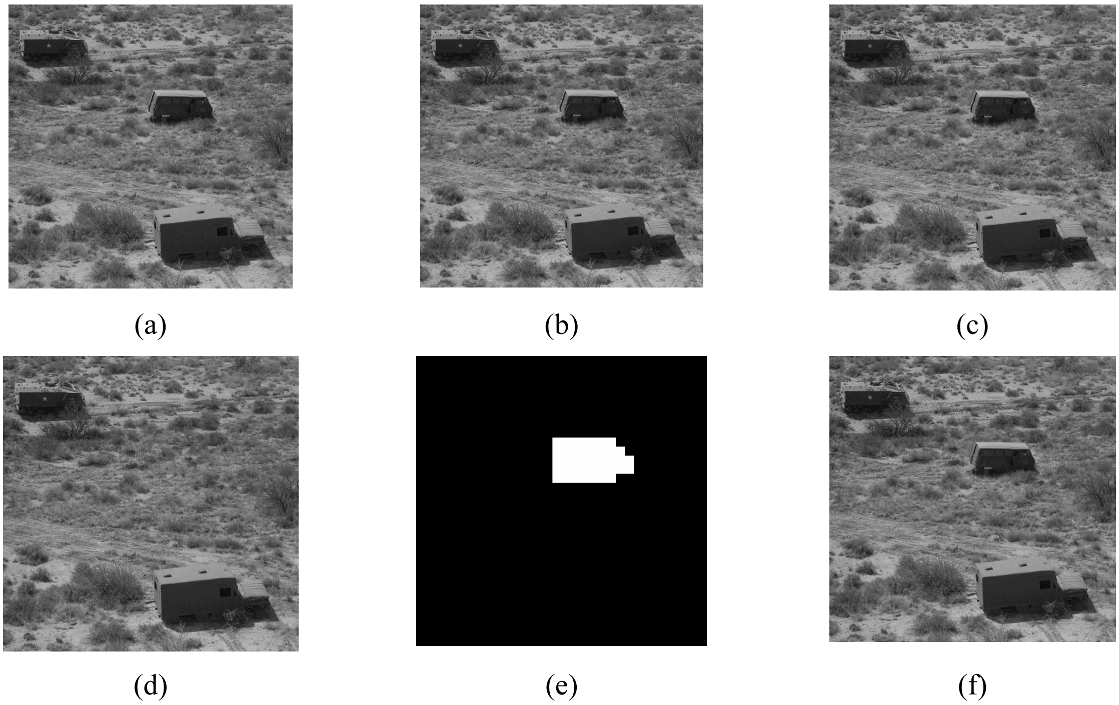
Self-recovery of the tampered regions. After the tampered regions are localized, the corresponding compressed data (*WC*) can be utilized for self-recovery of the tampered blocks. In order to enhance the accuracy of the reconstruction, Basis Pursuit (BP) algorithm which is detailed described in the literature [24] is chosen as the reconstruction method. And the tampered regions can be precisely recovered through inverse DWT afterwards. The whole image is obtained after all the tampered blocks are recovered.

4 Experimental Results and Analysis

In this part, the proposed scheme has been extensively simulated. And experiments were conducted to evaluate the performance of the proposed dual watermarking scheme in terms of the imperceptibility, robustness, accuracy of tamper localization and recovery capacity. Our experimental results were obtained from 20 different grayscale images of size 512x512, The block size is set as 16x16. The strength factor of *WS* and *WC* is set as 0.01 and 0.005, respectively. For recovery watermark *WC*, the compressed rate is set as 0.4 in compressive sensing. The proposed approach was carried out in MATLAB-7.6 environment on an AMD Athlon x4, 3.8GHz processor with 8GB of memory.

Fig. 3 provides an overview of the proposed scheme. Fig. 3 (b) shows that the visual quality of the watermarked image is extremely good, and the localization map in Fig. 3 (e) clearly reveals that the malicious attacks and non-malicious processing operations can be accurately distinguished, and the tampered regions can be precisely localized. Due to the attractive reconstruction ability of compressive sensing, the tampered regions can be further recovered with high quality as is show in Fig. 3 (f).

As is described in 2.2, the attractive properties of SVD guarantee us to enhance the imperceptibility of the watermarked image by embedding the dual watermark in the singular values of the cover image. The schemes in the literatures [6, 20-21] are also implemented to make comparisons with the proposed method in Table.1 in terms of invisibility of the watermarked image. The peak signal to noise ratio (PSNR) is employed to evaluate the transparency of these watermarking schemes. Suppose that the host image is $F = R^{M \times N}$ and the watermarked image is $F' = R^{M \times N}$, PSNR is defined as follows:



(a) (b) (c)

(d) (e) (f)

Fig. 3. Example of tamper localization and self-recovery: (a) original image (b)watermarked image with PSNR=45.1342dB (c)image tampered with JPEG compression with QF=50 (d) image tampered with malicious attack and JPEG compression with QF=50 (e) tamper localization (f) recovered image with PSNR=30.66dB

Table 1. Comparisons of PSNR (dB) of the watermarked images with different schemes

Images	[6]	[20]	[21]	Proposed
Lena	33.47	29.30	37.21	37.78
Cameraman	35.87	26.37	36.24	38.40
Moon surface	36.10	27.85	34.80	42.32
Aerial	31.82	26.54	37.52	37.42
Chemical plant	34.80	30.62	36.35	43.87

$$PSNR = 10log_{10} \frac{(2^k - 1)^2}{\frac{1}{MN} \sum_{m,n} (F_{m,n} - F'_{m,n})^2} \tag{23}$$

where m=(1, 2, …, M), n=(1, 2, …, N), and k is the bit rate of the image F and F’, in this paper 8-bit images are used, thus k is set as 8. The results clearly show that the proposed scheme performs better than the other methods when dealing with images with different textures.

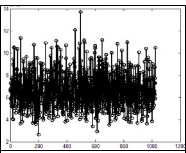
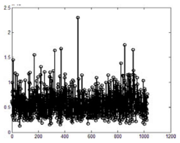
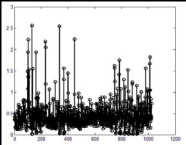
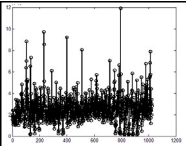
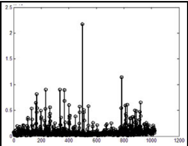
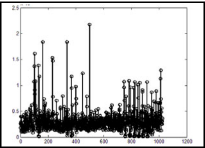
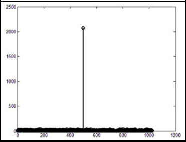
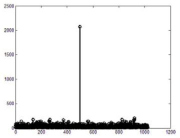
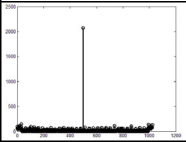
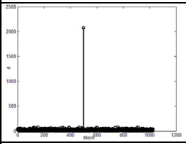
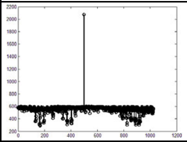
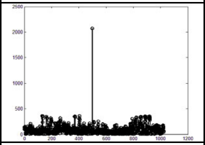
Moreover, in order to evaluate the robustness of the proposed scheme, several common non-malicious processing operations and combined non-malicious and malicious attacks are separately employed to the watermarked image, and the performance in terms of authentication and self-recovery are represented in Table. 2 and Table. 3.

Table 2. Performances under non-malicious attacks and combined attacks

Non-malicious attack only				Non-malicious and 5% malicious attacks	
Non-malicious attacks	Parameters	t_1	Authentication	TH	PSNR of the recovered images (dB)
Gaussian White Noise (Power)	5	8.33	Yes	13.35	32.08
	10	16.54	Yes	24.67	31.47
	15	26.89	Yes	36.74	29.82
	20	41.47	Yes	52.94	26.77
Salt & Pepper Noise (Density)	0.001	41.76	Yes	53.25	30.66
	0.005	64.31	Yes	78.65	26.95
	0.01	80.06	Yes	94.49	24.63
	0.05	224.1	Yes	242.2	18.51
Low-pass Filtering (Hsize, Sigma)	[3,3] 0.5	36.40	Yes	47.38	33.64
	[3,3] 1.0	81.76	Yes	95.83	29.50
	[3,3] 3.0	92.62	Yes	107.2	28.49
	[5,5] 0.5	36.54	Yes	47.53	33.63
	[5,5] 1.0	102.7	Yes	117.6	28.70
	[5,5] 3.0	151.9	Yes	168.5	26.28
JPEG (QF)	90	8.82	Yes	14.86	31.16
	70	21.67	Yes	30.73	30.86
	50	27.44	Yes	37.38	30.63
	30	34.67	Yes	45.47	29.81
	15	53.91	Yes	66.37	27.91
	5	147.8	Yes	164.2	24.71
Luminance Change (Strength)	+10%	144.1	Yes	160.4	26.97
	+20%	271.5	Yes	290.3	23.04
	-10%	160.1	Yes	176.8	27.03
	-20%	334.9	Yes	354.5	21.97
Contrast Change (Strength)	+10%	169.6	Yes	186.6	28.77
	20%	363.6	Yes	383.6	25.56
	-10%	156.7	Yes	173.3	30.20
	-20%	315.9	Yes	335.3	27.78

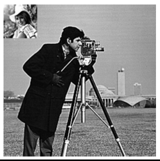
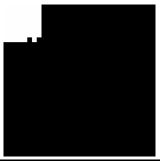
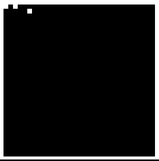
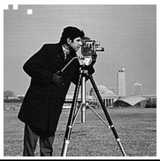
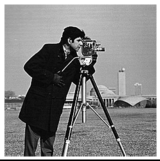
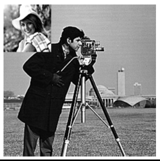
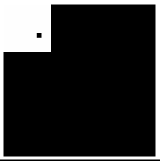
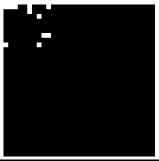
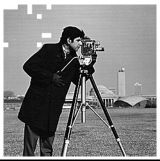
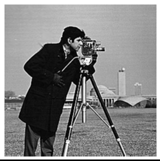
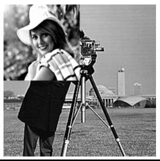
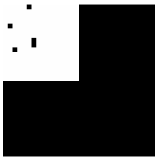
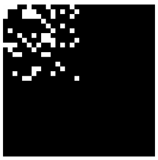
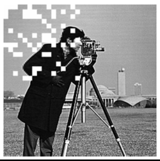
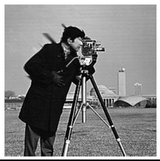
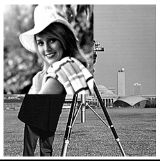
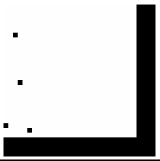
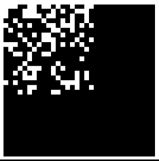
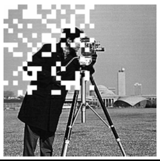
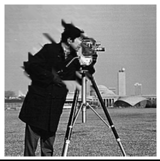
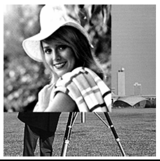
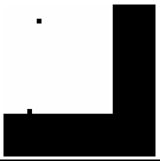
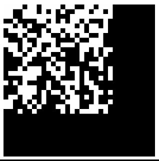
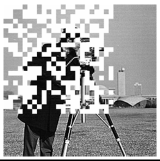
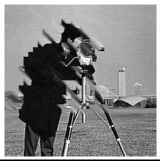
It can be concluded from Table. 2 that the proposed scheme is quite robust against different kinds of non-malicious attacks. Moreover, the malicious attacks and non-malicious attacks can be accurately distinguished by means of an adaptive threshold selection method which is proposed in this paper. In order to represent the robustness of the proposed scheme more clearly, the scheme in the literature [6] is implemented in the same way to make a comparison with our method. Results are shown in Table. 3. Here the watermarked image is tampered with malicious attack (block 500 is malicious attack) and non-malicious attacks. The experimental results demonstrate that the performance in terms of robustness of the proposed scheme is much better than that of in [6] especially when the strength of the non-malicious attacks is high.

Table 3. Comparision of the robustness against combined attacks

Scheme [6]						
Pro-posed Scheme						
	(a)Gaussian White Noise (Power =20dbW)	(b)Salt & Pepper Noise (Density=0.05)	(c)Low-pass Filtering (Sigma =3.0 Hsize =[5,5])	(d) JPEG (QF=10)	(e) Luminance Change (Strength =+50%)	(f)Contrast Change (strength =+20%)

Furthermore, the recovery capacity of the proposed scheme is evaluated and represented in Table.4. The experiments are carried out on images with JPEG compression (with QF=50%) together with different percent of “Copy and Paste” attacks. Table. 4 (b) demonstrates that the localization accuracy rate is approximately 100% and the performance will not get worse with the increase of the tampered percent. Furthermore, it can be observed from Table. 4 (c) and Table. 4 (d) that the lost recovery information shows a rising trend with the increase of the tampered percentage, and the corresponding PSNR of the recovered image declines with the increase of the lost recovery information accordingly. In addition, bilinear interpolation technique is employed here to fill up the pixels of the lost blocks. The experimental results in Table. 4 (e) demonstrate that the tampered image can still be recovered with an acceptable quality even though the tampered percentage is up to 35%.

Table 4. Performances of the recovery capacity under different tampered percent (a) tampered image (b) tamper localization (ER=error rate, black means authentic blocks while white means tampered regions) (c) Localization of the lost recovery information (LR=loss rate, black means acquired while white means lost) (d) recovered image (e) recovered image with bilinear interpolation

Percent=5% 	ER=0.20% 	LR=0.29% 	PSNR=31.56 	PSNR=34.68 
Percent=10% 	ER=0.10% 	LR=1.07% 	PSNR=28.28 	PSNR=34.01 
Percent=25% 	ER=0.49% 	LR=5.76% 	PSNR=18.13 	PSNR=26.89 
Percent=35% 	ER=0.39% 	LR=11.23% 	PSNR=14.08 	PSNR=21.24 
Percent=50% 	ER=0.20% 	LR=25.49% 	PSNR=10.35 	PSNR=17.76 
(a)	(b)	(c)	(d)	(e)

5 Conclusions

Content-based image authentication is definitely significant for the current digital and network era. In this paper, a novel dual watermarking scheme is proposed for content-based authentication where the tampered regions can be precisely localized and further recovered. Compressive sensing, DWT-SVD and Chaotic Mapping are all applied here to guarantee the performance of the proposed watermarking scheme in terms of the invisibility, security, robustness and recovery capability. Our experimental results have demonstrated that the proposed approach can precisely distinguish non-malicious processing operations and malicious attacks, besides the tampered regions can be accurately localized and further recovered with high quality. With the increasing need of content-based authentication nowadays, the combination of compressive sensing theory and SVD algorithm to promote the performance of the watermarking scheme is worth further investigating. In addition, future work will focus on employing efficient human visual system model to improve the transparency performance, and tamper localization and self-recovery will be deeply researched as well.

Acknowledgments

This work was supported by Shenzhen Engineering Laboratory of Broadband Wireless Network Security, and the Science and Technology Development Fund of Macao SARFDCT056/2012/A2 and UM Multi-year Research Grant: MYRG144(Y1-L2)-FST11-ZLM.

References

[1] J.C. Patra, J.E. Phua, D. Rajan, DCT domain watermarking scheme using Chinese Remainder Theorem for image authentication, in: Proc. of IEEE ICME-2010, 2010.

[2] L. Weng, G. Braeckman, A. Dooms, B. Preneel, P. Schelkens, Robust image content authentication with tamper location, in: Proc. of IEEE ICME-2012, 2012.

[3] D.L. Donoho, Compressed sensing, IEEE Trans. on Information Theory 52(4)(2006) 1289-1306.

[4] V.K. Veena, G. Jyothish Lal, S. Vishnu Prabhu, S. Sachin Kumar, K.P. Soman, A robust watermarking method based on compressed Sensing and Arnold scrambling, in: Proc. of IEEE MVIP-2012, 2012.

[5] G. Valenzise, M. Tagliasacchi, S. Tubaro, A compressive sensing based watermarking scheme for sparse image tampering identification, in: Proc. of IEEE ICIP-2008, 2009.

[6] T. Emmanuel, B. Premanand, Watermarking for self-recovery of tampered images using compressed sensing, in: Proc. of IEEE ICCC-2013, 2013.

[7] I. Orovic, S. Stankovic, Combined compressive sampling and image watermarking, in: Proc. of IEEE International Symposium on ELMAR, 2013.

[8] I. Orovic, A. Draganic, S. Stankovic, Compressive sensing as a watermarking attack, in: Proc. of IEEE TELFOR, 2013.

[9] Y.W. Jiang, X. M. Yu, On the robustness of image watermarking VIA compressed sensing, in: Proc. of IEEE ISEEE, 2014.

[10] X.F. Chi, G. Feng, A robust digital watermarking algorithm based on SVD of compressive sampling measurements, in: Proc. of IEEE CISP, 2014.

[11] M. Yamac, C. Dikici, B. Sankur, Robust watermarking of compressive sensed measurements under impulsive and Gaussian attacks, in: Proc. of IEEE EUSIPCO, 2013.

[12] H. Zhao, F. Lei, A novel video authentication scheme with secure CS-watermark in cloud, in: Proc. of IEEE BigMM, 2015.

[13] R.Z. Liu, T.N. Tan, SVD based digital watermarking method, Chinese Journal of Electronics 2(2001) 168-171.

[14] X.H. Ma, X.F. Shen, A novel blind grayscale watermark algorithm based on SVD, in: Proc. of IEEE ICALIP, 2008.

[15] X.L. Jia, Y.L. Qi, L.P. Shao, X.B. Jia, A watermark algorithm based on SVD and image geometric correction, in: Proc. of IEEE ICSAI, 2012.

[16] M.A. Kayum Hawlader, M. Moniruzzaman, M.F. Hossain, SVD based robust and secure dual stages watermarking scheme for copyright protection, in: Proc. of IEEE IFOST, 2014.

[17] W. Wang, A.D. Lai, Y. Bo, X.B. Chen, A novel robust zero watermarking scheme based on DWT and SVD, in: Proc. of

IEEE CISP-2011, 2011.

[18] Y. Pathak, S. Dehariya, A more secure transmission of medical images by two label DWT and SVD based watermarking technique, in: Proc. of IEEE ICAETR, 2014.

[19] P. Mitra, R. Gunjan, M.S. Gaur, A multi-resolution watermarking based on contourlet transform using SVD and QR decomposition, in: Proc. of IEEE RACSS, 2012.

[20] Q.L. Gu, T.G. Gao, A new image authentication based on reversible watermarking algorithm, in: Proc. of IEEE WCICA - 2008, 2008.

[21] F. Liu, H. Wang, L. Cheng, A.T.S Ho, Enhanced perceptual image authentication with tamper localization and self-restoration, in: Proc. of IEEE ICME-2014, 2014.

[22] E. Candès, J. Romberg, T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, IEEE Trans. on Information Theory 52(2006) 489-509.

[23] M. Tagliasacchi, G. Valenzise, S. Tubaro, Localization of sparse image tampering via random projections, in: Proc. of IEEE ICIP-2008, 2008.

[24] E.J. Candès, J. Romberg, T. Tao, Stable signal recovery from incomplete and inaccurate measurements, Communications on Pure and Applied Mathematics 59(8)(2006) 1207-1223.

[25] R.Z. Liu, T.N. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. On Multimedia 4 (1)(2002) 121-128.

[26] A. Cohen, I. Daubechies, J. Feauveau, BiorthogonaI bases of compactIy supported waveIets, Communications on Pure and Applied Mathematics 45(5)(1992) 485-560.