The ISC Int'l Journal of Information Security
ISeCure

July 2021, Volume 13, Number 2 (pp. 145–156)
http://www.isecure-journal.org

Blind Multipurpose Image Watermarking with Perfect Security

Sorour Sheidani [1] and Ziba Eslami [1,*]
[1] *Department of Data and Computer Science, Shahid Beheshti University, Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: March 17, 2020
Revised: September 23, 2020
Accepted: April 10, 2021
Published Online: May 29, 2021

Keywords:
Blind Watermarking, Copyright Protection, Image Authentication, Perfect Secrecy, Multipurpose Watermarking, Verifiable Threshold Secret Sharing Scheme

Type: Research Article

doi: 10.22042/isecure.2021.223025.527

dor: 20.1001.1.20082045.2021.13.2.5.0

Abstract

Nowadays, from one hand multimedia authentication techniques are widely used to achieve trustworthiness, on the other hand, due to the rapid growth of image processing software technologies, having a secure method to protect the copyright of these data seems fairly essential. Multipurpose watermarking emerged in order to simultaneously accomplish multimedia authentication and copyright protection. In this paper, we propose a multipurpose watermarking method which achieves perfect security, the ability to detect tampered areas of the watermarked image as well as a lower BER rate, at the cost of reducing capacity by half compared with previous works. This watermarking scheme is blind in the sense that on the receiver side, neither the original host image nor the embedded watermark is needed for ownership watermark extraction or tamper detection. Experimental results show that our method is able to reconstruct extracted tampered watermarks even after various attacks such as JPEG compression, average filtering, gamma correction, median filtering, speckle noise, sharpening, and Wiener filtering. Comparisons are provided with other multipurpose watermarking methods which primarily aim at simultaneous goals of copyright protection and authentication. We also show the superiority of our proposed method to three watermarking methods attaining these objectives on a one-goal-at-a-time basis.

1 Introduction

Nowadays image security has attracted extensive attentions as technology advancements allow images to be copied or manipulated easily. Therefore, ownership protection and image authentication are two active areas in the field of image security [1]. Watermarking realizes these goals by embedding some information to the images. Different goals demand different watermarking schemes. Based on its objectives, image watermarking can be classified into three main categories [2]: robust, fragile and semi-fragile watermarks. Robust watermarks are intended to withstand any intentional or unintentional manipulation or deletion of information [3]. In fragile watermarking, the watermark which is embedded in the host document is destroyed after any manipulation [4]. Semi-fragile watermarking is placed between robust and fragile types and can be designed to tolerate legitimate changes while highlighting intentional distortions. These watermarks are used for the purpose of authentication. Multipurpose [1] image watermarking is used to provide features of both robust and fragile watermark in

[*] Corresponding author.
Email addresses: s_sheidani@sbu.ac.ir, z_eslami@sbu.ac.ir
ISSN: 2008-2045 © 2020 ISC. All rights reserved.

[1] The terms *mutipurpose* as well as *hybrid/multiple/dual/double watermarking* are also used by some authors to indicate other objectives (see for example [5–11]).

one scheme. The advantage of using such a scheme is to figure out different types of false claim in a single check [12]. To the best of our knowledge, there does not exist many methods for multipurpose watermarking with simultaneous objectives of copyright protection and authentication in the literature. In the light of the fact that the existing multipurpose watermarking methods serve two different watermarks to authenticate the images and protect their copyright, multipurpose watermarking methods are categorized into three groups in the literature based on the order and position of the embedded watermarks relative to each other. The first category is the class of the approaches in which the fragile watermark is added to image after embedding the robust watermark. Some of the proposed methods of this category need the original watermark or host image for authentication and therefore they are informed methods [13–16]. Some of the schemes of this category also use spatial domain for image authentication [13, 14, 17–21]. This domain is too sensitive and an image which is processed even with innocent image processing operations may be detected as non-authentic [22]. In the second category of multipurpose watermarking, robust and fragile watermarks are embedded into two non-overlapping parts of the host image. The methods of [23, 24] are from this category. Although, they are not applicable to a wide range of the images. The method of [24] is specialized for geographic information system (GIS) applications and the method of [23] uses the color features of the host images.

The methods of the third category combine robust and fragile watermarks and embed it into the host image. By the extraction, the two combined watermarks are recovered separately. The methods of [25, 26], which are from this category, use spatial domain and least significant bit (LSB) method to embed authentication information. This approach makes them too sensitive to manipulations. Also, the method of [27] which combines two watermarks is not blind. Table 1 shows the summary of the relevant literature on multipurpose watermarking models compared to our method.

Table 1. Summary of the comparison of the models in relevant studies

Paper	Approach	Blind scheme	Not using SD* and LSB	applicable on a wide range of images	Using a single watermark	Perfectly secret
[19]	Using robust visual hash codes and hash functions	✓	✗	✓	✗	✗
[28]	Using multistage quantizer structure	✓	✓	✗	✗	✗
[15]	Using DWT decomposition	✗	✓	✓	✗	✗
[21]	Using square deviation modulation, MD5 hash function, and LSB	✓	✗	✓	✗	✗
[27]	Using 3-Level wavelet decomposition	✗	✓	✓	✗	✗
[16]	Using DCT coefficients	✗	✓	✓	✗	✗
[23]	Using different channels of YCbCr color space	✓	✓	✗	✗	✗
[20]	Using DCT and hash codes	✓	✗	✓	✗	✗
[17]	Using SVD and Chaotic sequence	✗	✓	✓	✗	✗
[14]	Using DCT and spatial domains	✓	✗	✓	✗	✗
[25]	Using 3-level integer wavelet transform and LSB	✓	✗	✓	✗	✗
[18]	Using DWT domain based on SVD and ABC intelligent method	✓	✗	✓	✗	✗
[13]	Using DWT, chaotic map, and Artificial Bee Colony (ABC) intelligent method	✗	✓	✓	✗	✗
[29]	Using a multiscale curvelet transform	✓	✓	✓	✗	✗
[26]	Using DCT based quantization and LSB	✓	✗	✓	✗	✗
[24]	Using feature and non-feature points of the objects in the map	✓	✓	✗	✗	✗
[30]	Using ROI and Lempel—Ziv—Welch algorithm	✗	✓	✓	✗	✗
Our previous approach	Using Feldman's VTSS	✓	✓	✓	✓	✗
Our proposed approach	Using Pedersen's VTSS	✓	✓	✓	✓	✓

*SD: Spatial Domain

Our contribution: In this paper, we propose a multipurpose watermarking technique with perfect security based on $(2,3)$-Pedersen's scheme to achieve both copyright protection and image authentication simultaneously with one watermark. (t,n)-Pedersen's verifiable secret sharing scheme is a well-known cryptographic protocol to share a secret amongst n persons such that any coalition of t people who possess correct shares is able to reconstruct the secret. It is also able to verify the validity of the shares without any need to access the original secret. Our key idea is that using Pederson's verifiable secret sharing as the underlying machinery, we find the tampered areas of the image blindly which is one of our key findings in this paper. Also, In our proposed scheme, we consider the watermark as a secret and distribute it among three shares. Due to this strategy and the perfect secrecy of Pedersen's verifiable threshold secret sharing, our scheme also gains the advantage of perfect secrecy over our previous work [31]. This is an important achievement regarding the fact that the concept of perfect secrecy implies no information leaks to the attackers even if they have unlimited time and computational resources. Going one step further, we will embed the computed shares to the host image in frequency domain. In this way, our scheme is able to verify the authenticity of the host image. The structure of the paper is as follows: In section 1 we focus on outline of the paper, multipurpose watermarking and its application. section 2 is provided to explain state-of-the-art literature of multipurpose watermarkings which have the same goals as us. In section 3 we briefly review the preliminaries and required background which encompasses verifiable threshold secret sharing and Pedersen's secret sharing scheme. section 4 is the description of our proposed method. In section 5 experimental results and the performance of the proposed scheme is tested and compared. Conclusions are finally provided in section 6.

2 Related Works

In this section, we explain some of the state-of-the-art literatures in the context of multipurpose watermarking. Here, we focus on the studies in which their goals are the same as us, i.e., copyright protection, authentication.

In 2017, [13] proposed a multipurpose watermarking with IDWT based algorithms for embedding and extraction. A logo for copyright protection is embedded in the subbands with low frequency, and in order to achieve authentication ability, another logo is embedded in in high frequency subbands. Because of the trade-off between capacity, fidelity and robustness, they have served artificial bee colony (ABC) algorithm.

[24] presented a digital image watermarking scheme for the goals of copyright protection and tamper localization of vector maps. Feature points of a vector map are used to embed copyright watermark and and non-feature points of objects were used to embed fragile watermark. In this method, the watermarks can be extracted separately. This method is proposed exclusively for geographic information system (GIS) applications.

[32] proposed a novel method for multipurpose digital image watermarking by the method of substitution of multiple LSBs. In order to achieve better performance of tamper detection, they select the place of embedding randomly. Despite all good merits of this method, it needs two separate watermarks for its different goals.

The paper proposed in 2020, [30], focuses on medical image watermarking. The security of ownership is provided by the embeddings based on the principal components (PC). And, LZW (Lempel-Ziv-Welch) based fragile watermarking is used to hide compressed image's region of interest (ROI). Complete reversibility of the ROI in this paper is provided by generating the watermarks based on the ROI. This paper again, serves different watermarks for its different goals.

3 Preliminaries

In this section, we briefly explain the basic background of our proposed multipurpose watermarking scheme. It is consists of a review of the concept of verifiable secret sharing and the means of providing perfect secrecy in related context. Secret sharing scheme, introduced by Blakley and Shamir (1979) independently, is a basic tool for protecting cryptographic keys [33–35]. A threshold SS involves a dealer who has a secret S, a set of n participants called shareholders, and a collection of subsets of shareholders, called the access structure, who can work together to recover the secret. In Shamir's (t, n) secret sharing, the dealer divides the secret S into n shares and distributes shares among n shareholders such that:

(1) Any t or more than t shares can reconstruct the secret,
(2) Fewer than t shares cannot obtain any information about the secret S [35–37].

However, a (t, n) secret sharing cannot detect whether there exists any deception between the dealer and shareholders. In 1985, Chor, Goldwasser *et al.* extended the notion of SS and proposed the first verifiable secret sharing [37]. Verifiability is the property of a verifiable secret sharing which ensures that each shareholder has received a valid share [38]. Later, Pedersen proposed a non-interactive verifiable secret sharing scheme with perfect security, in the sense that no information about the secret is revealed to the attackers[39]. Here, we touch on an introduction on Pedersen's verifiable threshold secret sharing scheme.

3.1 Pedersen's Verifiable Secret Sharing Scheme with Perfect Security

Verifiable threshold secret sharing (VTSS) provides the ability of validating correctness of the received shares. In the literature there exists a variety of VTSS [40–43], however the one proposed by Pedersen has the advantage of non-interactively achieving to perfect secrecy.

Definition. A perfect secret sharing scheme is a method of sharing a secret S among a set of n participants, in such a way that the following two properties are satisfied:

(1) If an authorized subset of participants pool their shares, then they can determine the value of S.
(2) If an unauthorized subset of participants pool their shares, then they can determine nothing

about the value of S [44].

Since this level of security can enhances the security of watermarks, in this paper, we are only concerned with Pedersen's VTSS. This choice obtains us perfect secrecy, simplicity and adequacy. In Pedersen's VTSS scheme, the dealer chooses two large prime numbers p and q such that $p|q-1$. Then, the generator $g \in \mathcal{Z}_p^*$ is chosen with order q. Also, let $h \in \mathcal{Z}_p^* - 1$ be a random element such that $log_g h$ is unknown to all parties. After that, the dealer chooses random polynomials $f(x)$ and $g(x)$ as below

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \mod q, \quad (1)$$

$$g(x) = b_0 + b_1 x + \cdots + b_{t-1} x^{t-1} \mod q. \quad (2)$$

Where a_j and $b_j \in \mathcal{Z}_q$ for $0 \leq j < t$, and $f(0) = a_0 = S$. The dealer sends shares $s_i = (f(i), g(i))$ to participant i using a private channel. Then, the dealer computes commitments according to Equation 3.

$$B_j = g^{a_j} h^{b_j} \mod p. \quad (3)$$

Participant i can verify the correctness of its share, s_i, by checking Equation 4,

$$g^{s_{i1}} h^{s_{i2}} \overset{?}{=} \prod B_j^{i^j} \mod q. \quad (4)$$

In the reconstruction phase, t or more correct pairs are collected from participants and S is retrieved using Lagrange interpolation formula

$$S = \sum_{i=1}^{t} f(i) \prod_{i=1, j \neq i}^{t} (-j/i - j) \mod p. \quad (5)$$

In subsequent sections, we will use Pedersen's scheme to share the watermark logo securely and then embed these shares to the host image.

4 The Proposed Scheme

We propose our scheme in this section to achieve simultaneously image copyright protection and its authentication. In this scheme we use $(2,3)$-Pedersen's verifiable threshold secret sharing scheme. Our reasons to choose this scheme are as follows:

- The reason of serving a **verifiable threshold secret sharing** as underlying machinery is that these schemes are able to distinguish tampered shares and non tampered ones by themselves. And their output shares are uncorrelated. So, we can recognize intact areas correctly.
- The reason of serving **Pedersen's** verifiable threshold secret sharing is its perfect secrecy. Hence, its security level is higher than other VTSS schemes like Feldman's.
- The reason of serving a **(2,3)**-Pedersen's VTSS is that in order to protect the copyright of the images, we want to be able to reconstruct tampered areas of the watermark. Hence, we need at least one more share in case of tampers to substitute. Note that this extra share *never* leaks information about the original watermark regarding the inherent information theoric security of Pedersen's VTSS.

Since our method is inherently a semi-fragile watermarking, it destroys upon the insertion of a second watermark (although by using a VTSS as underlying machinery it has the ability of reconstruction when needed), the destroyed areas show the manipulated regions by the insertion of any new watermark. So, it is secure against double watermarking attack. The security of our scheme is also provided by using private keys. This scheme includes four phases:

(1) **Encoding** in which the watermark is shared among three shares,
(2) **Embedding** where the generated shares are embedded into the host image using discrete wavelet transform,
(3) **Extraction** to extract the shares from the watermarked image,
(4) **Decoding** where the watermark is reconstructed to prove ownership and the authenticity of the image simultaneously. We list the notations used throughout the paper in Table 2.

Table 2. Notations

Symbol	Meaning
p	a prime number
q	s prime number having the property of $p\|q-1$
g	a generator in $\mathcal{Z}_p^*$ with the order q
h	a random element in $\mathcal{Z}_p^* - 1$
H	host image
OW	original watermark
OW'	recovered original watermark
w	decimal watermark in vector form
w'	recovered decimal watermark in vector form
S_j	j-th share from w $(j = 1, 2, 3)$ totally
S'_j	extracted j-th share from w' $(j = 1, 2, 3)$ totally
$S_j l$	l^{th} cell of the j-th share from w $(j = 1, 2, 3$ and $l = 1, 2)$
$S'_j l$	l^{th} cell of the extracted j-th share from w' $(j = 1, 2, 3$ and $l = 1, 2)$
BS_j	binary representation of j-th share of w $(j = 1, 2, 3)$ totally
BS'_j	binary representation of j-th extracted share of w' $(j = 1, 2, 3)$totally
BS_{jl}	binary representation of l^{th} cell of the j-th share of w $(j = 1, 2, 3$ and $l = 1, 2)$
BS'_{jl}	binary representation of l^{th} cell of the j-th extracted share of w' $(j = 1, 2, 3$ and $l = 1, 2)$
E_j	Embedding vector obtained from BS_j $(j = 1, 2, 3)$
E'_{jl}	Extracted vector from the watermarked image $(j = 1, 2, 3)$
WI	sent watermarked image
WI'	received watermarked image
v_j	vector form of DWT sub-bands coefficients in embedding phase $(j = 1, 2, 3)$
v'_j	vector form of DWT sub-bands coefficients in extraction phase $(j = 1, 2, 3)$
K_j	private keys $(j = 1, 2, 3)$
A_j	j-th authentication matrix $(j = 1, 2, 3)$
N	transformation levels
d	group size for embedding one bit of BS_j (capacity controller)
Q	quantization step
DWT	discrete wavelet transform
IDWT	inverse discrete wavelet transform
VTSS	verifiable threshold secret sharing
B_j	commitments to secret sharing coefficients

4.1 Encoding Phase

Input: The watermark OW, **Output:** Three shares made from watermark in binary form $[BS_{11}||BS_{12}], [BS_{21}||BS_{22}]$, and $[BS_{31}||BS_{32}]$

In this phase, the watermark is read from the input and processed to get prepared for using in Pedersen's scheme. Each pixel of the processed watermark is considered as a secret and is distributed into three shares using a (t, n)-Pedersen's verifiable threshold secret sharing scheme. Figure 1 shows the encoding and embedding phases of the watermark. The steps of this phase are described below in detail:

Step 1 First, a watermark OW is read from the input (or generated randomly).

Step 2 The watermark is turned into its decimal vector form. This vector is considered as w. (Henceforth, this is considered as watermark for using in secret sharing scheme.)

Step 3 Using Pedersen's verifiable secret sharing scheme, three pair of shares $S_1 = (S_{11}, S_{12}), S_2 = (S_{21}, S_{22}), S_3 = (S_{31}, S_{32})$ are made from w.

Step 4 Each cell of S_1, S_2, and S_3 is converted to its binary form $[BS_{11}||BS_{12}], [BS_{21}||BS_{22}]$, and $[BS_{31}||BS_{32}]$, respectively. Where '$||$' shows concatenation operation.

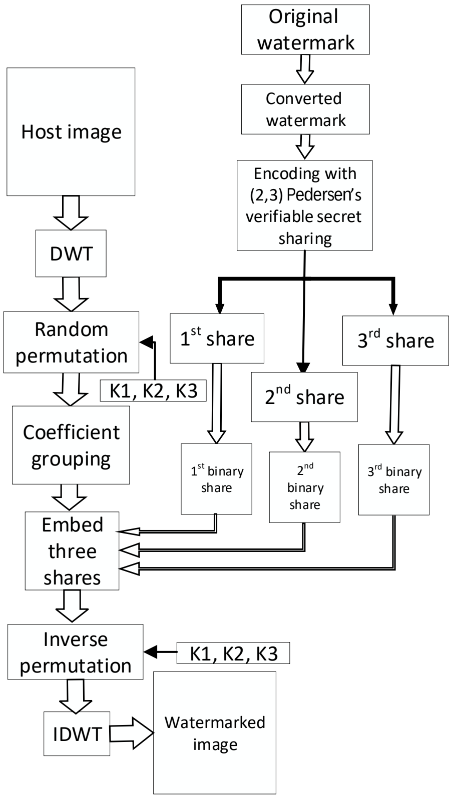


Figure 1. Encoding and embedding phases

4.2 Embedding Phase

The embedding phase is started by decomposing the host image using N level 2-dimensional DWT. Afterwards, the detailed coefficients of level N are chosen and permuted using private keys K_j for $j = 1, 2, 3$. Each $[BS_{j1}||BS_{j2}]$ is embedded in one sub-band. The steps are as follows:

Step 1 The gray scale host image H is decomposed using an N level 2D-DWT to have the sub-bands LL_n, LH_n, HL_n, HH_n.

Step 2 Sub-bands of LL_n, LH_n, HL_n are chosen. The coefficients of these sub-bands are saved in three vectors v_1, v_2, v_3, respectively.

Step 3 v_1, v_2, v_3 are permuted using the private keys K_1, K_2, K_3, respectively.

Step 4 In order to embed one bit into a group of d coefficients, the vectors obtained in the step are divided to the groups of size d without any overlap. The groups obtained from LL_n are saved in M_1, and the groups obtained from LH_n and HL_n are saved in M_2 and M_3, respectively, such that each matrix has d columns. This d controls the capacity of our scheme since we will embed 1 watermark bit per d columns.

Step 5 Vectors of E_j are made by assigning the bits of BS_{j1} to their odd indices, and assigning the bits of BS_{j2} to their even indices for $j = 1, 2, 3$.

Step 6 E_j $(j = 1, 2, 3)$ is embedded into M_j with the method explained in the following. Here, we get help from Preda's algorithm [45] in which the usage of DWT makes it more sensitive to detect tampers with smaller block sizes and causes its good performance against non-malicious attacks, although it is possible to benefit from any other semi-fragile algorithm at this step. The details are as follows:

(1) The average of each group is computed using Equation 6 in which $c_i(z)$ denotes z-th coefficient of the i-th group.

$$m_i = \sum_{z=1}^{d} (-1)^z |c_i(z)|. \tag{6}$$

(2) For each i, m_i^w is computed using Equation 7.

$$m_i^E = \begin{cases} \lfloor m_i/Q \rfloor \cdot Q & \text{if} \quad \bmod 2\lfloor m_i/Q \rfloor = E_{ij} \\ \lfloor m_i/Q \rfloor \cdot Q + Q & \text{if} \quad \bmod 2\lfloor m_i/Q \rfloor \neq E_{ij} \end{cases}. \tag{7}$$

(3) Modifying the greatest absolute value of each group, m_i is converted to m_i^E. Equation 8 shows the method of this modification.

$$c_{i,max}^E(z) = c_{i,max}(z) + (-1)^z \cdot sign(c_{i,max}) \cdot (m_i^E - m_i). \tag{8}$$

Step 7 The inverse permutation of the modified vectors are computed using K_1, K_2, K_3.

Step 8 Obtained vectors are converted into matrix form.

Step 9 The inverse of 2-dimensional DWT is computed.

4.3 Extraction Phase

The receiver of the watermarked image who has the private keys K_1, K_2, K_3 is able to extract the embedded shares. The steps of this phase are as follows:

Step 1 Received watermarked image is transformed into N levels using 2-dimensional DWT. The results are $LL'_n, LH'_n, HL'_n, HH'_n$.

Step 2 Sub-bands coefficients of LL'_n, LH'_n, HL'_n are saved in v'_1, v'_2, v'_3 in vector form.

Step 3 v'_1, v'_2, v'_3 are permuted independently using the keys K_1, K_2, K_3, respectively.

Step 4 The vectors of permuted coefficients are divided to the groups of size d.

Step 5 The bits of E'_1 $(j = 1, 2, 3)$ are extracted from three vectors resulted from Step 4 using Equation 9.

$$E'_{ij} = \mod 2(\lfloor m'_{ij}/Q \rfloor), \tag{9}$$

where $j = 1, 2, 3$, and i denotes the group number.

Step 6 BS'_{1j} is formed by the odd indices of E'_{ij}, and BS'_{2j} is formed by the even indices of E'_{ij}. Then, we put $BS'_j = [BS'_{1j} || BS'_{2j}]$ (for $j = 1, 2, 3$).

4.4 Decoding Phase

In this phase, binary shares are converted into their decimal forms. Moreover, authentication matrices are made which are used to authenticate the host image. The Boolean authentication matrices indicate the validity of each extracted share. The details of the steps are provided below.

Step 1 Each binary share is converted into its decimal form. The results are $S'_{11}, S'_{12}, S'_{21}, S'_{22}, S'_{31}, S'_{32}$.

Step 2 All the pair values of $[S'_{11}, S'_{12}], [S'_{21}, S'_{22}], [S'_{31}, S'_{32}]$. are verified using Equation 4.

Step 3 Whenever the shares $[S'_{11}, S'_{12}], [S'_{21}, S'_{22}]$ were not correct, the third pair S'_{31}, S'_{32} would be used instead. Using $(2, 3)$-Pedersen's verifiable threshold secret sharing scheme, two correct shares are enough to be set into the Equation 5 and consequently reconstruct each pixel of the watermark. W' is made by utilizing this equation and setting two correct shares in it.

Step 4 To achieve the original watermark on the receiver side (e.g. OW') the output of Step 3 (e.g. w') is converted to its binary form. The result of this step is the ownership watermark which was intended to protect copyright of the watermarked image.

4.5 Image Authentication Phase

The image authentication phase aims at finding the authentic and inauthentic regions of the image. This process is done as below:

Step 1 Three boolean authentication vectors $AV_j, j = 1, 2, 3$ are made with the same size as binary forms of S'_1, S'_2, S'_3. The default values of these matrices are "True".

Step 2 All the values of S'_1, S'_2, S'_3 are verified using Equation 4.

Step 3 Whenever S'_i verification returned "False" We put a "False" flag in all corresponding AV_is, for both S'_{i1} and S'_{i2}.

Step 4 $AV_1, AV_2, andAV_3$ are permuted using private keys K_1, K_2, and K_3.

Step 5 The vectors obtained in Step 4 are reshaped to their matrix form.

Step 6 The logical operator *and* of the cells of the three matrices which are at the same location is computed.

Step 7 Each "True" or "False" result from Step 6 is mapped to a square shape region of the size $N * N$ at the same position in the watermarked image.

In this way, all tampered regions of the watermarked image are illustrated by "False" positions in the watermarked image.

5 Experimental Results

To test the performance of the proposed multipurpose watermarking method, first, we show the performance of our method by reporting the results of the experiments on 3035 BOSS images [46]. Then to be comparable with [31, 45, 47, 48], a collection of 100 watermarked images of different sizes and formats are evaluated. In order to be comparable with [12, 45] and with our previous work [31], another set of the images were gathered from [49–53]. Since our previous work and Preda's semifragile watermarking results have been computed for 100 images against cropping and JPEG compression attack, we have presented the results of these attacks for 100 images. Then, in order to test the ability of our watermark to protect the copyright of the images, we have evaluated our method against image processing operations such as median filtering, Gaussian noise, etc. We have provided comparative Table 7. The proposed method was examined by embedding the watermark in the 1st, 2nd, and 3rd levels of DWT with Haar wavelet. The implementations were done in MATLAB R2016b. After these evaluations, we also discuss the security of our algorithm against a targeted attack. Furthermore, we show the ability of our method to detect the tampered regions of the images in Figure 4. At each experiment, we compare the pros and cons of our current method with our previous one (see [31]).

To test the performance of the method, mean peak signal to noise ratio (PSNR) of watermarked images are calculated by:

$$PSNR = 10 \log_{10}(\frac{255^2}{MSE}), \tag{10}$$

where $MSE = \sum_{i=1}^{|w|} (w_i' - w_i)^2/|w|$. Another metric used to evaluate the quality of watermarked images is the Structural Similarity (SSIM) Index quality assessment index. It can be computed by

$$SSIM(x, y) = [l(x, y)]^{\alpha}[c(x, y)]^{\beta}[s(x, y)]^{\gamma}, \tag{11}$$

where

$$\begin{aligned} l(x, y) =& \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C1}, \\ c(x, y) =& \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}, \\ s(x, y) =& \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}. \end{aligned}$$

Where μ_x, μ_y, σ_x and σ_y are local means, standard deviations, and cross-covariance for images x and y. Since we have used ssim function of MATLAB, the default values for exponents is $\alpha = \beta = \gamma = 1$ and $C_3 = C_2/2$. Therefore, ssim index in Equation 11 reduces to

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C2)}. \tag{12}$$

To evaluate the extracted watermark, Bit Error Rate (BER) of the extracted watermarks are calculated by

$$BER = \sum_{i=1}^{|w|} numel(w_i \neq w_i')/|w|. \tag{13}$$

Here, $numel(w_i \neq w_i')$ shows the number of locations where the extracted watermark is not equal to the embedded one. Again, we use also another metric, Normalized Cross Correlation (NCC), to test the accuracy of the extracted bit:

$$NCC(W, W') = \frac{\sum (W - mean(W)) * (W' - mean(W'))}{len(W) * \sqrt{(var(W) * var(W')}}, \tag{14}$$

where, $len(W)$ is the lengh of watermarks and $var(W)$ denotes the variance of W.

Table 3. Mean PSNR, SSIM, BER and NCC values of 3035 images received from [46]

Q	d	PSNR	SSIM value	SSIM confidence interval	BER	NCC value	NCC confidence interval
4	4	44.02	0.98	[0.986 0.986]	0.00	0.00	[0.997 0.997]
	8	44.10	0.98	[0.986 0.987]	9.96	0.99	[0.997 0.997]
	12	44.13	0.98	[0.986 0.987]	8.44	0.99	[0.997 0.998]
	16	44.13	0.98	[0.986 0.982]	8.06	0.99	[0.998 0.998]
8	4	43.17	0.98	[0.981 0.982]	0.00	0.99	[0.994 0.994]
	8	43.63	0.98	[0.984 0.984]	0.00	0.99	[0.992 0.993]
	12	43.86	0.98	[0.985 0.986]	0.00	0.99	[0.993 0.994]
	16	43.88	0.98	[0.985 0.986]	0.00	0.99	[0.994 0.994]
12	4	41.87	0.97	[0.972 0.973]	0.00	0.99	[0.993 0.993]
	8	42.83	0.98	[0.980 0.980]	0.00	0.99	[0.989 0.990]
	12	43.25	0.98	[0.982 0.982]	0.00	0.98	[0.989 0.990]
	16	43.43	0.98	[0.983 0.984]	0.00	0.99	[0.989 0.990]
16	4	40.82	0.96	[0.963 0.964]	0.00	0.99	[0.993 0.993]
	8	42.13	0.97	[0.975 0.976]	0.00	0.98	[0.988 0.989]
	12	42.71	0.97	[0.979 0.979]	0.00	0.98	[0.987 0.988]
	16	42.99	0.98	[0.981 0.982]	0.00	0.98	[0.986 0.988]
20	4	39.98	0.95	[0.955 0.956]	0.00	0.99	[0.993 0.994]
	8	41.52	0.97	[0.971 0.972]	0.00	0.98	[0.988 0.989]
	12	42.00	0.97	[0.974 0.975]	0.00	0.98	[0.986 0.987]
	16	42.60	0.98	[0.980 0.980]	0.00	0.98	[0.985 0.986]

In Table 3, we have provided the results of our experiments on 3035 images from BOSS imageset in terms of PSNR, BER, SSIM, and NCC. This table presents the results by serving $N = 2$. Table 4 and Table 5 show the quality of the watermarked images and extracted watermarks in terms of PSNR and BER, respectively, for different choices of quantization step Q, group size d, and DWT decomposition levels N for our method as well as our previous one. In Table 6, we have reported the results of our statistical analysis using Wilcoxon signed-rank test. the null hypothesis H0 is taken as there is no significant difference between the proposed method and other schemes. On the other hand, hypothesis **H1** represents that a significant difference occurs between these comparison methods. With a 95% confidence level, the null hypothesis **H0** is denied if $\alpha \leq 0.05$. The null hypothesis **H0** cannot be denied if $\alpha \leq 0.05$. In the case of denying the null hypothesis $H0$ ($\alpha \leq 0.05$), we consider the critical value T_α for the Wilcoxon signed rank test and the sum of the positive and negative signed-ranks T^+ and T^-, respectively. We put $T = Min(T^+, T^-)$ and we say that our proposed method is better than the compared schemes whenever $T \leq T_\alpha$[54]. For starred values in Table 6 the null hypothesis **H0** cannot be denied and so we conclude that our scheme, in spite of using a single watermark and achieving perfect secrecy, has a good performance as [45] and [31] in terms of BER and PSNR. But for not starred values, as explained before, we need one more step to decide. We determine $T_\alpha = 152$. Therefore, in all other cases (except when $N = 1$ in [31]) our scheme outperforms better and is superior to [45] and [31]. Since the JPEG compression is the most common compression method, the robustness of our method is measured against this

Table 4. Mean PSNR values for 100 watermarked images

Q	d	$n = 1$			$n = 2$			$n = 3$		
		[45]	[31]	Ours	[45]	[31]	Ours	[45]	[31]	Ours
4	4	48.09	44.21	47.99	54.14	44.09	53.12	60.18	44.33	60.15
	8	51.09	44.35	50.84	57.16	44.29	55.87	63.18	44.32	64.09
	12	51.86	44.41	52.52	58.93	44.37	57.52	64.94	44.46	66.44
	16	5410	44.44	53.71	60.18	44.41	58.68	66.20	44.48	68.08
8	4	42.10	44.04	42.32	48.14	43.04	40.90	54.12	43.90	53.05
	8	43.71	44.92	45.23	43.69	50.77	57.20	57.20	44.17	55.80
	12	46.87	43.95	46.93	52.91	43.93	52.46	58.92	44.28	57.44
	16	48.10	44.08	48.13	54.16	44.06	53.67	60.22	44.34	58.61
12	4	38.62	40.96	38.88	44.61	41.71	44.58	50.64	43.46	50.62
	8	41.58	42.53	41.84	47.62	42.86	47.48	53.64	43.93	53.65
	12	43.33	43.11	43.56	49.38	43.32	49.19	55.37	44.11	55.44
	16	44.60	43.42	44.76	50.62	43.57	50.40	56.60	44.21	56.68
16	4	36.16	38.40	36.38	42.13	40.38	42.19	48.16	42.75	47.86
	8	39.09	40.68	39.39	45.11	41.94	45.10	51.14	43.49	50.74
	12	40.85	41.86	41.11	46.87	42.62	46.81	52.89	43.79	52.48
	16	42.10	42.41	42.33	48.13	43.00	48.03	54.20	43.95	53.67
20	4	34.26	35.73	34.43	40.20	39.11	40.32	46.19	42.16	46.25
	8	37.17	38.87	37.46	43.19	40.98	43.23	49.22	43.13	49.22
	12	38.90	40.25	39.20	44.94	41.83	44.93	51.00	43.52	50.99
	16	40.17	41.06	40.43	46.18	42.34	46.15	52.23	43.73	52.21

Table 5. Mean BER values for 100 watermarked images

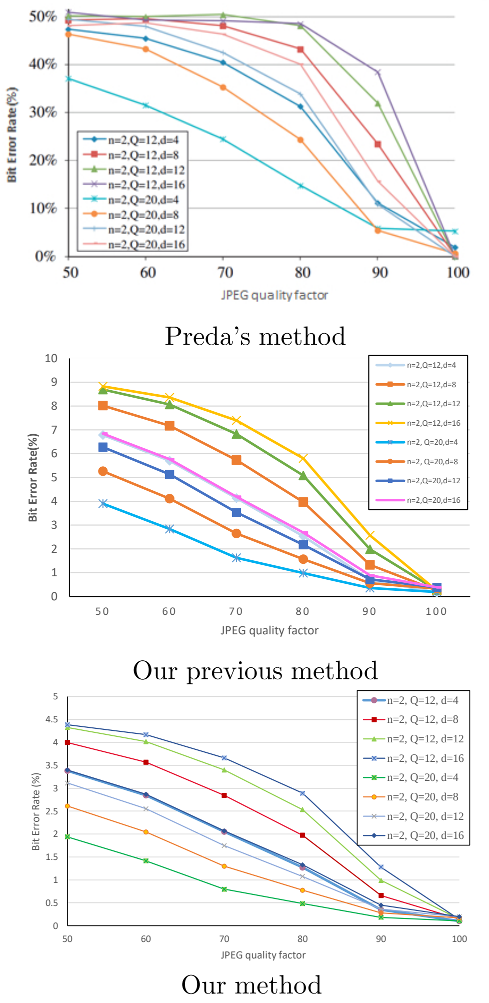
Q	d	$N = 1$			$N = 2$			$N = 3$		
		[45]	[31]	Ours	[45]	[31]	Ours	[45]	[31]	Ours
4	4	1.16	0.19	0.09	0.51	0.08	0.04	32.31	0.02	0.01
	8	0.24	0.37	0.18	0.36	0.07	0.03	37.58	0.65	0.02
	12	0.16	0.46	0.23	0.04	0.04	0.02	40.61	0.11	0.05
	16	0.15	0.50	0.25	0.39	0.03	0.01	41.74	0.17	0.08
8	4	4.85	0.19	0.09	0.75	0.14	0.06	0.24	0.03	0.01
	8	0.92	0.37	0.18	0.05	0.18	0.09	0.15	0.01	0.00
	12	0.34	0.44	0.22	0.02	0.16	0.08	0.22	0.01	0.00
	16	0.19	0.48	0.24	0.02	0.13	0.06	0.19	0.01	0.00
12	4	9.65	0.18	0.09	1.98	0.16	0.08	0.22	0.06	0.03
	8	2.52	0.42	0.21	1.16	0.25	0.12	0.02	0.03	0.01
	12	0.97	0.51	0.25	0.04	0.27	0.13	0.02	0.01	0.00
	16	0.49	0.55	0.27	0.02	0.25	0.12	0.01	0.01	0.00
16	4	14.53	0.16	0.08	3.53	0.18	0.08	0.48	0.08	0.04
	8	4.87	0.45	0.22	0.37	0.30	0.14	0.02	0.04	0.02
	12	2.15	0.58	0.29	0.08	0.33	0.16	0.02	0.03	0.01
	16	1.12	0.63	0.31	0.02	0.33	0.16	0.01	0.02	0.00
20	4	18.94	0.14	0.07	5.31	0.19	0.09	0.79	0.11	0.05
	8	7.56	0.44	0.22	0.78	0.33	0.16	0.06	0.17	0.03
	12	3.68	0.62	0.31	0.17	0.38	0.18	0.00	0.64	0.02
	16	2.10	0.71	0.35	0.07	0.39	0.19	0.01	0.02	0.01

Table 6. Wilcoxon statistical signed-rank test for comparison of our proposed scheme with[45] and [31]

	[45] and Ours			[31] and Ours		
for	$N = 1$	$N = 2$	$N = 3$	$N = 1$	$N = 2$	$N = 3$
PSNR	$0.134, T = 80$	$0.016, T = 129$	$0.344, T = 47$	$0.575, T = 210$	$1.401 \times 10^{-4*}$	$8.844 \times 10^{-5*}$
BER	$2.931 \times 10^{-4*}$	0.052	$4.848 \times 10^{-4*}$	$8.807 \times 10^{-5*}$	$8.695 \times 10^{-5*}$	$6.262 times 10^{-4*}$

compression with 50% to 100% quality factors. These results which are all under 5% show that because of the reconstruction ability of the proposed method, it is robust to compression experiment (Figure 2). Figure 2 also shows that the BERs of our new method against JPEG compression is about half of the BERs of our previous method. This is because half of the bits of secrets in our new proposed do not involve in the reconstructed message, although their existence is important for security and ability of finding tampered areas. So, if we consider only the bits which take part in reconstruction, which seems more fair, the BERs get doubled. In another experiment, we compare the performance of our method against JPEG compression with [31, 48] methods. Figure 3 shows the comparative results of Preda's method, our previous method, and our new method on Lena's image. As it clear from Figure 3, the BERs of our method are far less than Hou *et al.*'s method. The JPEG quality factor is changed from 40 to 100 during this experiment and all of the BER's of our method were less than 6. It is worth mentioning that our method uses two of the three embedded shares to extract each bit of information. Each share has also made by two parts to be able to recognize the correct shares blindly. So, in spite of all our advantages, the capacity of of our scheme is one sixth of [45].

Now, we show the ability of our method for copyright protection against various attacks including average filtering, gamma correction, median filtering, speckle noise, JPEG compression, low pass Gaussian filtering, sharpening, Wiener filter, and motion blur. In Table 7, we compare our method with one of the recent multipurpose watermarking methods, [12], using Lena's image which is accessible from the [12] dataset and also is related to our work. In this experiment, the watermark has been inserted at the 2nd level of DWT with quantization level of $Q = 20$ and step size $d = 4$. The α statistical value to test the significance of the difference between our results and the second column of Table 7 is 0.002. Since $\alpha \leq 0.05$, there is not enough evidence to reject the null hypothesis which is there is no significant difference between two vectors. We then determine $T = 64$ and $T_\alpha = 14$. We repeat the experiment with the third column and gain $\alpha = 0.01, T = 54$. So, generally in this case [12] has a better performance. Although in Table 7, [12] mainly performs better, instead we gain perfect secrecy and one single watermark for all goals along with acceptable NCC values. Now, we show the ability of our



Preda's method

Our previous method

Our method

Figure 2. Comparative detection performance after JPEG compression for resolution level $N = 2$ and different quantization step sizes Q and coefficients group size d

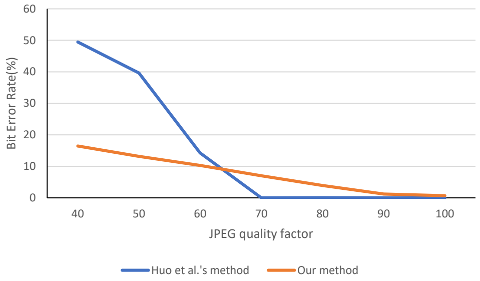


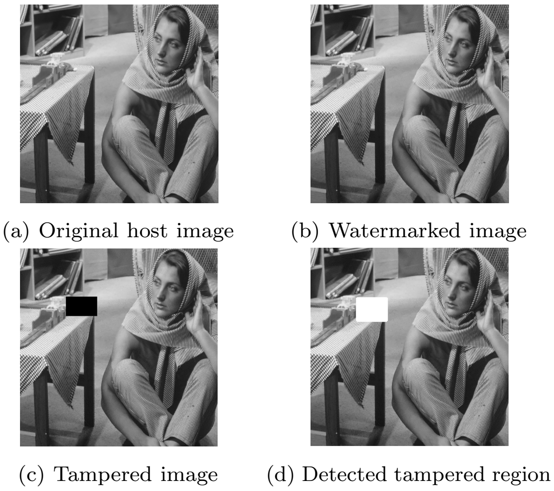
Figure 3. Comparative detection performance of our method, our previous method [31] and [48] method after JPEG compression for resolution level $N = 2$, $Q = 20$ and coefficient group size $d = 4$

Table 7. NCC values for Lena's image

	[12]		Ours
Attack	Logo	Man	
Average filtering (3 × 3)	0.8407	0.7349	0.4302
Gamma correction	0.7138	0.4958	0.4746
Median filter	0.9341	0.8462	0.8503
Speckle noise (0.001)	0.9792	0.9327	0.8278
Speckle noise (0.002)	-	-	0.7122
Speckle noise (0.003)	-	-	0.6542
Speckle noise (0.004)	-	-	0.5951
Speckle noise (0.005)	-	-	0.5719
Gaussian noise(M= 0, V= 0.001)	0.9019	0.7803	0.8648
Gaussian noise(M=0, V= 0.002)	-	-	0.4883
Gaussian noise(M=0.5, V= 0.001)	-	-	0.4123
JPEG (QF= 50)	0.9724	0.9076	0.7754
JPEG (QF= 60)	-	-	0.7871
JPEG (QF= 70)	-	-	0.8262
JPEG (QF= 80)	-	-	0.8812
JPEG2000(ratio=12)	0.9412	0.8583	0.6129
JPEG2000(ratio=10)	-	-	0.4499
JPEG2000(ratio=14)	-	-	0.7592
Low pass gaussian filter(3*3)	0.9882	0.9653	0.9109
Low pass gaussian filter(5*5)	-	-	0.9097
Sharpening	0.9464	0.8698	0.9655
Motion blur(theta= 4, len= 7)	0.8509	0.7194	0.3909
Motion blur(theta= 5, len= 3)	-	-	0.465
Motion blur(theta= 5, len= 7)	-	-	0.4558
Motion blur(theta= 4, len= 5)	-	-	0.5316
Wiener filter	0.9669	0.9173	0.6418
Wiener filter(5*5)	-	-	0.3434

method to localize tampered regions which are omitted from the image. Therefore, the Barbara image with the size of 1024 × 1024 has been tested (Figure 4a). We omit the pixels in the range of [250 :350, 240 : 400] in this watermarked image (Figure 4b and Figure 4c). Figure 4d shows that our method is able to find tampered regions correctly. These good and acceptable reported BERs are because of the usage of (2,3)-Pedersen's VTSS, in the light of the fact that it can recover the watermark correctly if any of two extracted shares (from three embedded ones) are correct. Our method utilizes different keys for permuting coefficients. So, they are arranged in different positions of the sub-bands coefficients of DWT. As a result they don't get corrupted altogether generally which results in better recovery rate of our method. Also, Pedersen's VTSS is equipped with the ability of verifying the shares, this ability enables us to detect our two required correct shares to recover the watermark.

In addition to what mentioned above, our method is secure against the attacks which use a smart modification to wavelet coefficients it is clear that if the attacker aims to change the wavelet coefficients using a smart modification, he must change it in a way


(a) Original host image (b) Watermarked image

(c) Tampered image (d) Detected tampered region

Figure 4. Testing the detection performance of the omitted region by tampering the Barbara image

that the extracted watermark does not change (otherwise, the extracted watermark shows that the image has been manipulated). If the extracted watermark remains the same, it means that the output of the Equation 6 must remain the same after modification. Therefore, in this formula m_i must be still unchanged. So, the output of Equation 7 must not change, which means that the attacker should do his modifications in a way that the summation of each group of coefficients still remains unchanged. But he does not have the data hiding key by which the permutation and grouping are done. Therefore, it appears that the attacker cannot modify the wavelet coefficients smartly. Therefore, the security of our algorithms against the smart modifications, and the good performance of our method at the mentioned experiments including JPEG compression, cropping, median filtering, salt & pepper and Gaussian noises, histogram equalization, and sharpening attack show the ability of our method to achieve its goals which are copyright protection and authentication.

6 Conclusion

In this paper, we modify our previous work, [31], to achieve perfect secrecy. This new method, in addition to have the previous method advantages of realizing image copyright protection and authentication with a single watermark, has the ability of blindly detecting tampered regions. With all this, our method shows a better performance in terms of BER of the extracted watermarks after the attacks such as JPEG compression, cropping, salt and pepper noise, median filtering, etc. This performance leads to a suitable scheme to protect the copyright of the images. We accomplish mentioned goals by means of (2,3)-Pedersen's verifiable threshold secret sharing.

References

[1] Zhi-Fang Yang, Chih-Ting Kuo, and Te-Hsi Kuo. Authorization identification by watermarking in log-polar coordinate system. *The Computer Journal*, 61(11):1710–1723, 2018.

[2] Kariman M Mabrouk, Noura A Semary, and Hatem Abdul-Kader. Fragile watermarking techniques for 3d model authentication. In *International Conference on Advanced Machine Learning Technologies and Applications*, pages 669–679. Springer, 2019.

[3] Pabitra Pal, Biswapati Jana, and Jaydeb Bhaumik. Robust watermarking scheme for tamper detection and authentication exploiting ca. *IET Image Processing*, 13(12):2116–2129, 2019.

[4] Ta Minh Thanh and Munetoshi Iwakiri. Fragile watermarking with permutation code for content-leakage in digital rights management system. *Multimedia Systems*, 22(5):603–615, Oct 2016.

[5] Zhe-Ming Lu, Dian-Guo Xu, and Sheng-He Sun. Multipurpose image watermarking algorithm based on multistage vector quantization. *IEEE Transactions on Image Processing*, 14(6):822–831, 2005.

[6] Taehae Kim, Yongwha Chung, Seunghwan Jung, and Daesung Moon. Secure remote fingerprint verification using dual watermarks. In *Digital Rights Management. Technologies, Issues, Challenges and Systems*, pages 217–227. Springer, 2006.

[7] Chokri Chemak, Mohamed Salim Bouhlel, and Jean Christophe Lapayre. A new scheme of robust image watermarking: the double watermarking algorithm. In *Proceedings of the 2007 summer computer simulation conference*, pages 1201–1208. Society for Computer Simulation International, 2007.

[8] Tzung-Her Chen, Tsung-Hao Hung, Gwoboa Horng, and Chia-Ming Chang. Multiple watermarking based on visual secret sharing. *International Journal of Innovative Computing Information and Control*, 4(11):3005–3026, 2008.

[9] Tien-You Lee and Shinfeng D Lin. Dual watermark for image tamper detection and recovery. *Pattern recognition*, 41(11):3497–3506, 2008.

[10] Rafiullah Chamlawi, Asifullah Khan, and Imran Usman. Authentication and recovery of images using multiple watermarks. *Computers & Electrical Engineering*, 36(3):578–584, 2010.

[11] Qi Han, Lei Han, Erfu Wang, and Jie Yang. Dual watermarking for image tamper detection and self-recovery. In *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on*, pages 33–36. IEEE, 2013.

[12] Irshad Ahmad Ansari and Millie Pant. Multipurpose image watermarking in the domain of dwt based on svd and abc. *Pattern Recognition Letters*, 94:228–236, 2017.

[13] Baiying Lei, Xin Zhao, Haijun Lei, Dong Ni, Siping Chen, Feng Zhou, and Tianfu Wang. Multipurpose watermarking scheme via intelligent method and chaotic map. *Multimedia Tools and Applications*, pages 1–23, 2017.

[14] Sohailah Alyammahi, Fatma Taher, Hussain Al-Ahmad, and Tim McGloughlin. A new multiple watermarking scheme for copyright protection and image authentication. In *Circuits and Systems (MWSCAS), 2016 IEEE 59th International Midwest Symposium on*, pages 1–4. IEEE, 2016.

[15] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy. A dual digital-image watermarking technique. In *International Journal of Computer and Information Engineering WEC (5)*, pages 1477–1480, 2005.

[16] Peng Zheng, Weihua Wang, and Juan Wang. A hybrid watermarking technique to resist tampering and copy attacks. In *2011 International Symposium on Intelligence Information Processing and Trusted Computing*, pages 111–114. IEEE, 2011.

[17] Irshad Ahmad Ansari, Millie Pant, Chang Wook Ahn, and Jaehun Jeong. PSO optimized multipurpose image watermarking using SVD and chaotic sequence. In *Bio-Inspired Computing-Theories and Applications*, pages 1–17. Springer, 2015.

[18] Irshad Ahmad Ansari and Millie Pant. Multipurpose image watermarking in the domain of DWT based on SVD and abc. *Pattern Recognition Letters*, 94:228–236, 2017.

[19] Frédéric Deguillaume, Sviatoslav Voloshynovskiy, and Thierry Pun. Secure hybrid robust watermarking resistant against tampering and copy attack. *Signal Processing*, 83(10):2133–2170, 2003.

[20] Alavi Kunhu and Hussain Al-Ahmad. Multi watermarking algorithm based on DCT and hash functions for color satellite images. In *Innovations in Information Technology (IIT), 2013 9th International Conference on*, pages 30–35. IEEE, 2013.

[21] Zhifang Wang, Bian Yang, Xiamu Niu, and Yijia Zhang. A practical multipurpose watermarking scheme for visual content copyright protection and authentication. In *Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on*, pages 461–464. IEEE, 2006.

[22] Peng Zheng, Weihua Wang, and Juan Wang. A hybrid watermarking technique to resist tampering and copy attacks. In *2011 International Symposium on Intelligence Information Processing and Trusted Computing*, pages 111–114. IEEE, 2011.

[23] Yanxia Zhao and Zenghui Zhou. Multipurpose blind watermarking algorithm for color image based on DWT and DCT. In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*, pages 1–4. IEEE, 2012.

[24] Yuwei Peng, Hai Lan, Mingliang Yue, and Yu Xue. Multipurpose watermarking for vector map protection and authentication. *Multimedia Tools and Applications*, 77(6):7239–7259, 2018.

[25] Hui Shi, Ming-chu Li, Cheng Guo, and Ru Tan. A region-adaptive semi-fragile dual watermarking scheme. *Multimedia Tools and Applications*, 75(1):465–495, 2016.

[26] Priyanka Singh and Suneeta Agarwal. A self recoverable dual watermarking scheme for copyright protection and integrity verification. *Multimedia Tools and Applications*, 76(5):6389–6428, 2017.

[27] Kai-xing Wu, Wei-wei Yan, and Jing Du. A robust dual digital-image watermarking technique. In *Computational Intelligence and Security Workshops, 2007. CISW 2007. International Conference on*, pages 668–671. IEEE, 2007.

[28] Zhe-Ming Lu, Dian-Guo Xu, and Sheng-He Sun. Multipurpose image watermarking algorithm based on multistage vector quantization. *IEEE Transactions on Image Processing*, 14(6):822–831, 2005.

[29] Chune Zhang, Lee Lung Cheng, Zhengding Qiu, and Lee-Ming Cheng. Multipurpose watermarking based on multiscale curvelet transform. *IEEE Transactions on Information Forensics and Security*, 3(4):611–619, 2008.

[30] Hanan S Alshanbari. Medical image watermarking for ownership and tamper detection. *Multimedia Tools and Applications*, pages 1–16, 2020.

[31] Sorour Sheidani and Ziba Eslami. Blind multipurpose image watermarking based on secret sharing. In *2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pages 1–8. IEEE, 2019.

[32] Rishi Sinhal and Irshad Ahmad Ansari. A multipurpose image watermarking scheme for digital image protection. *International Journal of System Assurance Engineering and Management*, pages 1–13, 2019.

[33] George Robert Blakley. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[34] Ziba Eslami and Saideh Kabiri Rad. A new verifiable multi-secret sharing scheme based on bilinear maps. *Wireless Personal Communications*,

63(2):459–467, 2012.

[35] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[36] Z Eslami and J Zarepour Ahmadabadi. A verifiable multi-secret sharing scheme based on cellular automata. *Information Sciences*, 180(15):2889–2894, 2010.

[37] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 383–395. IEEE, 1985.

[38] Rituraj Roy, Sayantani Bandyopadhyay, Shyamalendu Kandar, and Bibhas Chandra Dhara. A novel 3–4 image secret sharing scheme. In *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, pages 2072–2075. IEEE, 2015.

[39] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual International Cryptology Conference*, pages 129–140. Springer, 1991.

[40] Lin Liu. A survey of digital watermarking technologies. *Department of Electrical and Computer Engineering, State University of New York at Stony Brook, NY*, pages 1–12, 2005.

[41] Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Foundations of Computer Science, 1987., 28th Annual Symposium on*, pages 427–438. IEEE, 1987.

[42] Yanjun Liu, Lein Harn, and Chin-Chen Chang. A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets. *International Journal of Communication Systems*, 28(7):1282–1292, 2015.

[43] Zhuhong Shao, Yuanyuan Shang, Yu Zhang, Xilin Liu, and Guodong Guo. Robust watermarking using orthogonal fourier–mellin moments and chaotic map for double images. *Signal Processing*, 120:522–531, 2016.

[44] Douglas R Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.

[45] Radu O Preda. Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement*, 46(1):367–373, 2013.

[46] Bank of Standardized stimuli. *BOSStimpuli*, (Accessed September 02 2020). Retrieved from https://sites.google.com/site/bosstimuli/.

[47] Shabir A Parah, Javaid A Sheikh, Nazir A Loan, and Ghulam M Bhat. Robust and blind watermarking technique in dct domain using inter-block coefficient differencing. *Digital Signal Processing*, 53:11–24, 2016.

[48] Yaoran Huo, Hongjie He, and Fan Chen. A semi-fragile image watermarking algorithm with two-stage detection. *Multimedia tools and applications*, 72(1):123–149, 2014.

[49] The USC-SIPI Image Database. (Accessed July 21 2017). Retrieved from http://sipi.usc.edu/database/database.php?volume=misc.

[50] DECSAI. (Accessed July 21 2017). Retrieved from http://decsai.ugr.es/cvg/CG/base.htm.

[51] ECE Department at Polytechnic Institute of NYU. (Accessed July 21 2017). Retrieved from http://eeweb.poly.edu/~yao/EL5123/SampleData.html.

[52] ImageProcessingPlace: Standard_test_images. (Accessed July 21 2017). Retrieved from https://bit.ly/35OncHL.

[53] Gonzalez and Woods. *Image Processing Place: Images from Digital Image Processing*, 3 edition, (Accessed July 21 2017). Retrieved from https://bit.ly/2QMFdRx.

[54] Xiaobing Kang, Yajun Chen, Fan Zhao, and Guangfeng Lin. Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain. *Soft Computing*, 24(14):10561–10584, 2020.

Sorour Sheidani is currently persuing her Ph.D. degree in computer science in the department of Computer and Data Sciences at Shahid Beheshti University (SBU) in Iran, from 2016. Her research interests include cryptography, multimedia security, information theory and algorithm design.

Ziba Eslami received her B.S., M.S. and Ph.D. in applied mathematics from Tehran University in Iran. She received her Ph.D. in 2000. From 1991 to 2000, she was a resident researcher in the Institute for Studies in Theoretical Physics and Mathematics (IPM), Iran. During the academic years 2000–2003, she was a Post-doctoral fellow in IPM. She served as a non-resident researcher at IPM during 2003–2005. Currently, she is associate professor in the Department of Computer and Data Sciences at Shahid Beheshti University in Iran. Her research interests include design theory, combinatorial algorithms, cryptographic protocols and steganography.