

A multiple watermarking scheme based on orthogonal decomposition

Lizhi Xiong · Zhengquan Xu · Yanyan Xu

Received: 1 July 2013 / Revised: 5 November 2014 / Accepted: 8 February 2015 /

Published online: 29 March 2015

© Springer Science+Business Media New York 2015

Abstract This paper proposes a novel multiple watermarking scheme based on orthogonal decomposition (MWOD). In the first phase, based on orthogonal decomposition, the host data selected from multimedia data are divided into mutually independent multiple domains. Then multiple watermarks without need for considering the special correlation among them can respectively be embedded into these different domains even using different embedding algorithms. There is no mutual interference among watermarked domains so that multiple watermarks can be flexibly embedded in the distribution of the multimedia cover. Through theoretical analysis, the security of multiple watermarking operands is validated, which means that MWOD can ensure the security of watermarking operation domains. Therefore, media providers and service providers can embed their unique information step-by-step into digital multimedia using their own operation domain keys in MWOD, which can be used to identify media content's ownership or trace the illegal redistributors. Experimental results and analysis demonstrate the feasibility and robustness of MWOD.

Keywords Multiple watermarking · Orthogonal decomposition · Security · Multimedia distribution

1 Introduction

Digital watermarking is a technique which allows a user to embed some marks into a digital content for protecting his/her copyright or tracing illegal redistributors [1]. With the rapid development of Internet and digital media sharing services, the distribution of digital works is becoming more and more popular. In the meantime, there are more chances for piracy. To keep the benefits of media providers and service providers earned from network media

L. Xiong · Z. Xu (✉) · Y. Xu
State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, 129 Luoyu Road, Wuhan 430079, China
e-mail: xuzq@whu.edu.cn

L. Xiong
e-mail: xlzwhucs@gmail.com

Y. Xu
e-mail: xuyy@whu.edu.cn

consumption, anti-piracy is regarded as an urgent issue. In a media distribution process, media providers and service providers need to embed their own unique information step-by-step into media content to protect their benefit. However, a classical single watermarking cannot satisfy this requirement. Therefore, a multi-watermarking scheme has become highly desirable.

Multiple watermarking can be used to not only identify media content's owners or trace the illegal redistributors in media distributions, but also cope with different types of attacks, each of which may do harm to the media content from different perspectives [8]. Multi-watermarking scheme has more potential applications in the case of multiple content providers or users, such as in a cloud environment.

Current multi-watermarking schemes are as following. In [2], two watermarks are embedded simultaneously into two different sectors in the same DWT domain. They are used to verify the integrity and recover the tampered image. In [15], three different kinds of information: copyright management information, copy control information, and fingerprints are introduced as watermarks. The three kinds of information are embedded simultaneously into three different components of a single frame. These two schemes aim to simultaneously embed multiple watermarks into a same transform domain, but in fact, they are just a simple extension of single watermarking schemes to multiple watermarks embedding. In [18], a multiple watermarking model with side information is proposed. This model focuses on special correlations among watermarks. The correlation between the multimedia cover and watermarking, and the correlation among the watermarks themselves are considered as side information. Cox et al. [6] assumed that multiple watermarks are close to orthogonal and also applied a single watermark algorithm to embed multiple watermarks into multimedia data. Many more studies [14, 7, 9, 3] are similar. These schemes are based on an assumption of orthogonal relation among multiple watermarks. To overcome the restriction of orthogonal assumption, Peter H. W et al. [17] proposed a new multi-watermarking scheme, which embeds multiple watermarks in the same watermark space without orthogonal assumption among watermarks. But Peter's scheme still has a limited situation that multiple watermarks should be embedded simultaneously, not step-by-step, which reduces the flexibility of multi-watermarking scheme to some extent.

Meanwhile, the correlation among watermarks is easy to cause another issue: security of multiple watermarking. In a multiple watermarking scheme, if watermarks are embedded step by step into the same watermarking domain, malicious watermarking operators could easily attack other watermarks in the same watermarking domain. On the other hand, if there is a strong correlation among watermarks, it may be easily used by attackers. For example, attackers can derive other unknown watermarks from a known one owing to the correlation among watermarks. Therefore, users should select watermarks independently without need for considering the special correlation among watermarks.

Additionally, embedding rule of watermarking is also an important aspect that needs to be considered. According to current studies, embedding rules of the watermarking can be classified into additive watermarking [19, 10], multiplicative watermarking [4], quantization watermarking [11], and hybrid watermarking [16]. However, for different applications, especially in multiple watermarking users, the users should have the right to choose their own embedded rule of multiple watermarks. Therefore, a multiple watermarking scheme without restriction on embedding rules is desired.

From the discussions above, a practical multi-watermarking scheme needs to satisfy the following three basic requirements.

- 1) Watermarks can be selected independently without need for considering the special correlation among them.

- 2) Watermarks can be operated independently. It means that the embedding domain of watermarks can be different and the operation (embedding and extraction) of watermarks can be processed independently.
- 3) Various embedded rules are compatible in the scheme. That is to say, the multiple watermarking users have the right to choose their own embedded rule.

However, the above-mentioned schemes are unable to satisfy the three requirements simultaneously. Hence, in this paper, a multiple watermarking scheme based on orthogonal decomposition (MWOD) is proposed that could satisfy the three requirements. In MWOD, orthogonal decomposition is used to divide the protected data into multiple mutually independent domains. Each domain can be used to embed unique watermark with different embedding rules. Finally, they can be formed as a whole data through orthogonal composition. Thus, MWOD can offer a seamless fusion of multiple watermarking, and enable the users to embed their watermarks in different domains without need for considering the relationship of embedded watermarks. Meanwhile the security of each watermark can be validated by different watermarking operands (domain keys). Therefore, the proposed scheme can offer adequate flexibility for users to satisfy the requirements of multiple watermarking applications.

The main contributions of this paper can be summarized as follows. Firstly, MWOD is proposed to realize multiple watermarking, in which watermarks are embedded into different domains using different domain keys without need for considering the correlation among them. Secondly, MWOD is proved that multiple watermarks can be flexibly embedded in the distribution of the multimedia cover by different embedding algorithms and the security among watermarking operands is validated through theoretical analysis.

The rest of the paper is organized as follows. The definition of MWOD scheme is introduced in Section 2. The performance analysis of MWOD, including security analysis, is described in Section 3, the experimental results and analyses are shown in Section 4. Some additional issues of MWOD scheme and conclusions are finally described and future works are listed in Section 5.

2 MWOD

In this section, we propose a MWOD scheme to embed multiple watermarks into different domains. At the same time, the conditions of practical multi-watermarking scheme are also proposed.

2.1 Conditions of practical multiple watermarking scheme

A practical multiple watermarking scheme for multimedia distribution should satisfy three conditions:

Commutativity: it means that the processing order of watermarks should be commutative.

Mixture: the operation results of multiple watermarking should be mixed for the end users.

Applicability: multiple watermarking embedding algorithms should not be restricted, as are decided by users, such as various media providers and service providers.

Commutativity guarantees that the multiple watermarking orders do not affect the final result, and watermarks can be extracted from watermarked data. It provides the convenience

for practical applications. The Mixture condition ensures a seamless fusion of multiple watermarking so that they can finally forms a whole. Applicability ensures that users have the right to choose their own embedding rule for multiple watermarking. Most current multiple watermarking schemes cannot fully satisfy the above conditions. So MWOD scheme is proposed as following.

2.2 MWOD scheme

We group some selected image pixels or transform coefficients to form a vector and define it a host vector. Let the host vector be $X=(x_1,x_2,\dots,x_n)^T$ with length n . The i -th watermark $\mathbf{W}_i=\{w_1,w_2,\dots,w_q\}$ with number q , where $q\ll n$. The bit sequence of watermark may be a meaningful image such as the logo of the image owner or the information related to the host images such as the owner’s name, image ID, ..., etc. The watermark is modulated by the secret key which may be a pseudorandom bit sequence or other secret sequence for enhancing its security.

MWOD scheme consists of several multiple watermarking systems (MWS), each of which contains watermark embedded function $\mathcal{W}_i(\cdot, \cdot)$ corresponding with its key K_{iw} , extraction function $\mathcal{V}_i(\cdot, \cdot)$ corresponding with its key K_{iv} , and the i -th watermark \mathbf{W}_i . In MWS, multiple watermarks $\mathbf{W}=\{\mathbf{W}_1,\mathbf{W}_2,\dots,\mathbf{W}_u\}$ with number u , multiple watermarking embedding functions $\mathcal{W}(\cdot, \cdot, \cdot)=\{\mathcal{W}_1(\cdot, \cdot, \cdot), \mathcal{W}_2(\cdot, \cdot, \cdot), \dots, \mathcal{W}_u(\cdot, \cdot, \cdot)\}$ corresponding with its keys $K_w=\{K_{1w},K_{2w},\dots,K_{uw}\}$, extraction functions $\mathcal{V}(\cdot, \cdot)=\{\mathcal{V}_1(\cdot, \cdot), \mathcal{V}_2(\cdot, \cdot), \dots, \mathcal{V}_u(\cdot, \cdot)\}$ corresponding with its keys $K_v=\{K_{1v},K_{2v},\dots,K_{uv}\}$.

Denoted X_{iw} as the X embedded the i -th watermark, \mathbf{W}_i . $\mathcal{W}_i(\cdot, \cdot, \cdot)$ and $\mathcal{V}_i(\cdot, \cdot)$ are generic algorithms with no special requirements. Denote a transformation matrix $B = (b_1, b_2, \dots, b_n)$, of size $n \times n$, which satisfies the following:

$$\begin{cases} b_i^T \cdot b_j \neq 0 & \text{if } i = j \\ b_i^T \cdot b_j = 0 & \text{otherwise} \end{cases} \quad 1 \leq i, j \leq n \tag{1}$$

where $b_i=(b_{i1},b_{i2},\dots,b_{in})^T$ is a n -dimensional column vector in B . X can be represented as $X=B \cdot Y$ or $Y=B^{-1} \cdot X$ using orthogonal decomposition based on B .

Matrix B can be divided into multiple sub-matrixes, i.e., $B=(S_1,S_2,\dots,S_u)$ corresponding to multiple watermarks, respectively. And Vector Y is also divided into multiple sub-vectors, i.e., $Y=(Y_1,Y_2,\dots,Y_u)^T$. Then, X can be described as:

$$X = B \cdot Y = S_1 \cdot Y_1 + S_2 \cdot Y_2 + \dots + S_u \cdot Y_u \tag{2}$$

In MWOD scheme, watermarking operation function $\mathcal{W}(\cdot, \cdot, \cdot)$ is represented as:

$$X_w = \mathcal{W}(X, \mathbf{W}, K_w) = \sum_{i=1}^u \mathcal{W}_i(X, \mathbf{W}_i, K_{iw})$$

Assuming Y_i is used to embed the watermark, then, $\mathcal{W}(\cdot, \cdot, \cdot)$ is defined as:

$$X_w = \sum_{i=1}^u \mathcal{W}_i(X, \mathbf{W}_i, K_{iw}) = \sum_{i=1}^u S_i \cdot \mathcal{W}_i(Y_i, \mathbf{W}_i, K_{iw}) = \sum_{i=1}^u S_i \cdot Y_{iw} = B \cdot Y_w \tag{3}$$

where $\mathcal{W}_i(Y_i, \mathbf{W}_i, K_{iw}) = Y_{iw}$, $Y_w=(Y_{1w},Y_{2w},\dots,Y_{uw})^T$.

Equation (3) means that, in MWOD, watermarking for X are applied to its orthogonal decomposition coefficients Y_i instead of directly applied to X itself. Similarly, watermarking extraction is applied to Y_{iw} . They are defined as follows:

$$\begin{aligned}
 Y_w &= B^{-1} \cdot X_w \\
 \mathbf{W}_i &= \mathcal{V}_i(X_w, K_{iv}) = \mathcal{V}_i(Y_w, K_{iv}) \\
 &= \mathcal{V}_i(Y_{iw}, K_{iv})
 \end{aligned}
 \tag{4}$$

The processing orders of multiple watermarking embedding in MWOD do not affect the final result.

From Eqs.(3) and (4), it show that the transform matrix B is required to participate in watermarking embedding and extraction operations, which is not suitable for distribution to multiple watermarking operators. If each watermarking operator can get B , watermarking operation domains of other operators are insecure. MWOD is a promising multi-watermarking scheme which can be used to build the infrastructure of digital rights management (DRM) and asymmetric fingerprinting systems, if its security is validated.

From a security point of view, two aspects are mainly concerned with the security of MWOD, the one is that the embedding/extraction keys of watermarking operation is secured, such as K_w and K_v ; the another is that the operands of multiple watermarking are expected to be secure, such as sub-matrix S_i . It is necessary that the sub-matrix S_i , by which the operation domain of each watermarking operator are defined, is regarded as a secret key to the i -th operator and other operators cannot obtain it (security analysis in Section 3). Based on these ideas, we provide the reconstruction of MWOD for its security analysis as follows.

For the convenience of description, we take the two watermarking embedding for example. Let S_1 denotes the first watermark domain key and S_2 denotes the second watermark domain key, $S_1=(b_1, b_2, \dots, b_m)$ and $S_2=(b_{m+1}, b_{m+2}, \dots, b_n)$, where $B=(S_1, S_2)$.

From Eq. (1), assume that: $b_i^T \cdot b_i = \lambda_i$ and $\lambda_i \neq 0$, where $i \in [1, n]$. Given that $P=(B^T B)^{-1}$, then $P=diag(\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_n^{-1})$, and $Y_w = P \cdot B^T \cdot X_w$, based on Eq. (4). Similarly, assume the following:

$$P_{S_1} = (S_1^T \cdot S_1)^{-1} = diag(\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_m^{-1}) \text{ and } P_{S_2} = (S_2^T \cdot S_2)^{-1} = diag(\lambda_{m+1}^{-1}, \lambda_{m+2}^{-1}, \dots, \lambda_n^{-1}).$$

Assume the first watermarking domain is divided by S_{1P} and the second watermarking domain is divided by S_{2P} which satisfies: $(S_{1P}, S_{2P})^T = P \cdot B^T$. Then, Eq. (5) is derived as follows:

$$\begin{cases} Y = (S_{1P}, S_{2P})^T \cdot X \\ Y_w = (S_{1P}, S_{2P})^T \cdot X_w \end{cases}
 \tag{5}$$

Accordingly, $P \cdot (S_1, S_2)^T = (S_{1P}, S_{2P})^T$, $S_{1P}^T = P_{S_1} \cdot S_1^T$ and $S_{2P}^T = P_{S_2} \cdot S_2^T$. Then, the following is derived:

$$\begin{cases} Y_1 = S_{1P}^T \cdot X = P_{S_1} \cdot S_1^T \cdot X \\ Y_2 = S_{2P}^T \cdot X = P_{S_2} \cdot S_2^T \cdot X \end{cases}
 \tag{6}$$

$$\begin{cases} Y_{1w} = S_{1P}^T \cdot X_w = P_{S_1} \cdot S_1^T \cdot X_w \\ Y_{2w} = S_{2P}^T \cdot X_w = P_{S_2} \cdot S_2^T \cdot X_w \end{cases}
 \tag{7}$$

Finally, Eqs. (3) ~ (4) are redefined as follows:

$$\begin{aligned}
 X_{1w} &= S_1 \cdot \mathcal{W}_1(Y_1, \mathbf{W}_1, K_{1w}) + S_2 \cdot Y_2 \\
 &= S_1 \cdot \mathcal{W}_1(P_{S_1} \cdot S_1^T \cdot X, \mathbf{W}_1, K_{1w}) + X - S_1 \cdot Y_1 \\
 &= S_1 \cdot \mathcal{W}_1(P_{S_1} \cdot S_1^T \cdot X, \mathbf{W}_1, K_{1w}) + X - S_1 \cdot P_{S_1} \cdot S_1^T \cdot X \\
 &= S_1 \cdot \mathcal{W}_1\left((S_1^T \cdot S_1)^{-1} \cdot S_1^T \cdot X, \mathbf{W}_1, K_{1w}\right) + X - S_1 \cdot (S_1^T \cdot S_1)^{-1} \cdot S_1^T \cdot X \\
 &= \mathcal{W}_1(X, \mathbf{W}_1, S_1, K_{1w})
 \end{aligned}
 \tag{8}$$

Similarly,

$$\begin{aligned}
 X_{2w} &= S_2 \cdot \mathcal{W}_2\left((S_2^T \cdot S_2)^{-1} \cdot S_2^T \cdot X, \mathbf{W}_2, K_{2w}\right) + X - S_2 \cdot (\pi S_2^T \cdot S_2)^{-1} \cdot S_2^T \cdot X \\
 &= \mathcal{W}_2(X, \mathbf{W}_2, S_2, K_{2w})
 \end{aligned}
 \tag{9}$$

$$\begin{aligned}
 \mathbf{W}_1 &= \mathcal{V}_1(X_w, K_{1v}) = \mathcal{V}_1(Y_{1w}, K_{1v}) \\
 &= \mathcal{V}_1(P_{S_1} \cdot S_1^T \cdot X_w, K_{1v}) \\
 &= \mathcal{V}_1\left((S_1^T \cdot S_1)^{-1} \cdot S_1^T \cdot X_w, K_{1v}\right) \\
 &= \mathcal{V}_1(X_w, S_1, K_{1v})
 \end{aligned}
 \tag{10}$$

$$\begin{aligned}
 \mathbf{W}_2 &= \mathcal{V}_2(X_w, K_{2v}) = \mathcal{V}_2(Y_{2w}, K_{2v}) \\
 &= \mathcal{V}_2\left((S_2^T \cdot S_2)^{-1} \cdot S_2^T \cdot X_w, K_{2v}\right) \\
 &= \mathcal{V}_2(X_w, S_2, K_{2v})
 \end{aligned}
 \tag{11}$$

According to Eqs. (8) - (11), through reconstruction, the MWOD scheme has following characteristics:

- 1) The redefined processing functions all depend on matrixes S_1 or S_2 in addition to their own keys (K_v, K_w).
- 2) In addition to the existing keys, the first watermarking domain functions $\mathcal{W}_1(X, \mathbf{W}_1, S_1, K_{1w})$ and $\mathcal{V}_1(X_w, S_1, K_{1v})$ are related to the matrix S_1 only, and the second watermarking domain functions $\mathcal{W}_2(X, \mathbf{W}_2, S_2, K_{2w})$ and $\mathcal{V}_2(X_w, S_2, K_{2v})$ are related to matrix S_2 only.

The first allows S_1 or S_2 to be regarded as a secret key for these functions. The second implies that S_1 is the first watermarking domain key and S_2 is the second watermarking domain key. Thus, the reconstruction of MWOD allows the introduction of S_1 and S_2 to the MWOD scheme as a hidden key system for enhanced security. The embedding framework of MWOD is shown in Fig. 1. The security analysis in Section 3 will validate the increase in security of this method.

3 Performance analysis of MWOD

In performance analysis of previous multiple watermarking schemes, it has been more concerned about the potential use of the watermark. However, some performances, for example, the distortion and security of multiple watermarking operation domains, are not considered. So MWOD will be analyzed with respect to the robustness, distortion, capacity,

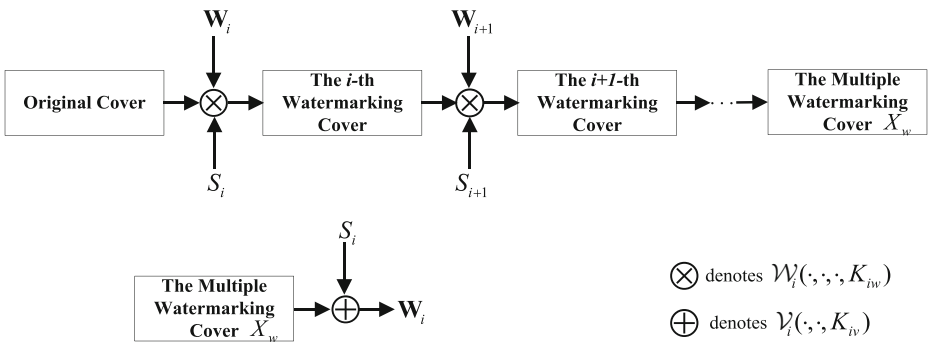


Fig. 1 The embedding framework of MWOD

and security of multiple watermarking operands, which can secure the security of watermarking operation domains.

3.1 Robustness analysis

The robustness of the multiple watermarking will be analyzed by focusing on the detection of watermark, i.e., cross correlation between the original watermark and decoded watermark in JPEG compression, high pass filter, median filter, low pass filter and noise.

To detect whether a modulated watermark \mathbf{W} is present in a testing image, we decode all the K bits of watermark from the image as \mathbf{W}' and evaluate a score. A possible score is the traditional normalized the detection score (cross correlation), DS , between the original watermark and the decoded watermark as follows.

$$DS = \frac{\sum_{i=1}^q (w_i - \bar{w}) \cdot (w'_i - \bar{w}')}{\sqrt{\sum_{i=1}^q (w_i - \bar{w})^2 \cdot \sum_{i=1}^q (w'_i - \bar{w}')^2}} \tag{12}$$

where w_i and w'_i represent respectively original watermark bit and extracted watermark bit, \bar{w} is the average of w and \bar{w}' is the average of w' . q is the size of \mathbf{W} .

If it can be guaranteed that the increment of the detection score DS is greater than that of the threshold, the multiple watermarking increases the successful detection rate of the watermark, or else, the multiple watermarking decreases the successful detection rate of the watermark. If the detection score is higher than a pre-defined threshold, the watermark is considered to be present in the testing image. The experiments of robustness analysis and results are explicitly shown in section 4.

3.2 Distortion analysis

Whatever the watermarking is additive or multiplicative, Y_{iw} can be described as:

$$Y_{iw} = Y_i + \widetilde{\mathbf{W}}_i \quad 1 \leq i \leq n \tag{13}$$

Where $\widetilde{\mathbf{W}}_i = \alpha_i \mathbf{W}_i$ denotes additive watermarking, and $\widetilde{\mathbf{W}}_i = \alpha_i Y_i \mathbf{W}_i$ denotes multiplicative watermarking. α_i denotes the watermarking strength, w_i denotes the element of the i -th watermark sequence. So, from the Eqs. (2-3), we have:

$$X_w = X + \sum_{i=1}^u S_i \widetilde{\mathbf{W}}_i \tag{14}$$

In the distortion analysis, peak signal to noise ratio (PSNR) value is used to evaluate the distortion degree of multi-watermarking. Here, from Eq. (14), the PSNR is defined by

$$P = 10\lg\left(\frac{LM255^2}{\sum_{i=1}^L \sum_{j=1}^M (\pi I'_{ij} - I_{ij})^2}\right) \tag{15}$$

$$\simeq 10\lg\left(\frac{LM255^2}{\sum_{i=1}^u S_i^2 \widetilde{\mathbf{W}}_i^2}\right)$$

Here, L and M denote the width and height of the cover, respectively. I' and I denote the watermarking cover and the original cover, respectively. u denotes the number of watermarks.

It is shown in Eq. (15) that the multiple watermarking can only make the PSNR decreasing with the number of embedded watermarks (N_{EW}), that is to say, it degrades the image perceptual quality. This means that regardless of the embedding rules, the N_{EW} should be rationally set.

3.3 Capacity analysis

The capacity analysis of the multiple watermarking mainly aims at the capacity change with N_{EW} increasing. In this paper, the analysis is assumed that the whole image has uniform watermark power constraint and noise power constraint in all pixel locations. Therefore, the capacity can be described as

$$C = \frac{1}{2} \log_2\left(1 + \left(P_w/P_n\right)\right) \tag{16}$$

Here, P_w and P_n represent the uniform power of watermark and noise, respectively. In MWOD, the Eq. (16) can be written by

$$C = \frac{1}{2} \log_2\left(1 + \left(\sum_{j=1}^u \sigma_{w_j}^2 / \sigma_X^2\right)\right) \tag{17}$$

$$\simeq \frac{1}{2} \log_2\left(1 + \left(\sum_{i=1}^u \sum_{j=1}^q S_{ij}^2 \widetilde{\mathbf{W}}_{ij}^2 / m\sigma_X^2\right)\right)$$

Here, $P_w = \sum_{j=1}^u \sigma_{w_j}^2$ and $P_n = \sigma_X^2$, S_{ij} denotes transformation sub-matrix, $\widetilde{\mathbf{W}}_{ij}$ denotes embedded watermark, u denotes the number of watermarks, q denote the size of each watermark.

Actually, the block-wise embedding of multi-watermarking does not change total capacity of the final embedded watermark. But, for the scheme we proposed, the final embedded watermark is not equal to the straightforward superimposition of the each single watermark (see Eq. (17)), so the summation of capacity of single watermarks can be more than the capacity of the final embedded watermark under appropriate S_i .

3.4 Security analysis

The security of MWOD includes two aspects: Firstly, the external attacker cannot erase the watermark by obtaining multiple watermarking covers. Secondly, for the sake of ensuring the security of watermarking domain, the operation domain keys of multiple watermarking embedded cannot be deduced with each other. For the first case, Wang and Lian [16] proved that the greater N_{EW} can decrease the security of

multi-watermarking scheme for the external attacker. Therefore, we can improve its security by setting rational the watermark number. For the second case, each watermark embedded operator cannot access the others watermark content. The security is analyzed as follows.

We take 2 watermarks embedding operation for example. S_1 and S_2 represent their watermarking operation domain keys, whose security depend on two conditions which will be validated as follows.

CONDITION 1: As secret keys, S_1 and S_2 can be adjusted independently to satisfy any predetermined security threshold, i.e. their key space have large enough to resist the brute force attack.

CONDITION 2: S_1 and S_2 are independent and cannot be mutually derived, i.e. it is difficult for the first operator to solve S_2 and the second operator to solve S_1 .

As it mentioned in Section 2, there exists related constraint between S_1 and S_2 from Eq. (1). If $n \times n$ is the size of B , the Eq. (1) consisted of $\frac{n(n-1)}{2}$ quadratic polynomial simultaneous equations with n^2 unknowns over a finite field F . The difference Δ is $\frac{n(n+1)}{2}$ between equations and unknowns. If the elements of B are k bits fix word-length integer, then F denotes the field of $[-2^{k-1}, 2^{k-1}-1]$.

This is an underdefined multivariate quadratic equations problem, generally referred to as an MQ difficult problem [5]. MQ is NP-hard. Some algorithms have been proposed for solving MQ faster than using an exhaustive search, but most of them did not change the general exponential, thus increasing the complexity characteristics.

With respect to this problem, the attacker who does not know any of the MWOD keys is considered first. Assume an attack on B by Eq. (1). Then, the complexity can be expressed as follows:

$$d_B = d_{MQ} + N_{MQ}d_0 \quad (18)$$

where d_B denotes the total measure of complexity for attacking B , d_{MQ} denotes the complexity for solving the MQ solutions of B , N_{MQ} denotes the number of all the expected solutions of B , and d_0 denotes the complexity for checking the solution is the correct solution.

Because there N_{MQ} possible solutions for B , the attacker must check the solutions one by one to find the true result. To do this, he has to substitute Eq. (4) with the candidates for B . However, K_{1v} or K_{2v} is unknown, thus the checking complexity nearly equals that of attacking K_{1v} or K_{2v} .

Equation (1) is an instance of MQ, where the number of unknowns is approximately 2 times the number of equations. In the practical application of Eq. (1), d_{MQ} can be roughly estimated as $2^{n^2k-k_m}$, where k_m is the factor that includes the efficiency improvement achieved over an exhaustive search by using a different algorithm. In most instances, k_m can be ignored because $k_m \ll n^2k$ if n and k are sufficiently large. N_{MQ} is approximately $2^{\Delta k} = 2^{\frac{n(n+1)k}{2}}$. To ensure the security of K_{1v} or K_{2v} , assume there is a threshold, k_0 , that the keys should exceed, thus d_0 can reasonably be set as 2^{k_0} . Thus the complexity for attacking B tends to increase exponentially as $O(n^2k)$ as follows:

$$d_B \sim 2^{n^2k-k_m} + 2^{\frac{n(n+1)k}{2}+k_0} \tag{19}$$

From Eq. (19), it shows that S_1 and S_2 , which are the B sub-matrixes, can be adjusted independently to satisfy any predetermined security threshold by set rational n and k . So the CONDITION 1 has been met.

If S_1 and S_2 cannot be mutually derived, the CONDITION 2 can be also met. We can prove THE CONDITION 2 as follows.

In MWOD, S_1 is known by the first operator and S_2 is known by the second operator, it is forbidden for the first operator to know S_2 . If the first operator knows S_2 , the second watermarking operation domain can be easily acquired, which would then lead to the breaking of the MWOD security. Similar reasoning is applied to S_1 and the second operator. Hence, S_1 and S_2 must have a difficulty designed for mutual derivation.

If the first operator is attacking the second watermarking, Eq. (1) and the known S_1 must be used to attack S_2 . If m denotes the number of columns in S_1 , and S_1 is known, then applying Eq. (1) to solve S_2 becomes the following:

$$\begin{cases} s_{1i}^T \cdot s_{1j} = 0 & i \neq j, \quad 0 \leq i, j \leq n-m \\ s_{1i}^T \cdot s_{2j} = 0 & 0 \leq i \leq m, \quad 0 \leq j \leq n-m \end{cases} \tag{20}$$

Equation system (20) consists of $(n-m) \frac{(n-m-1)}{2}$ quadratic equations and $m(n-m)$ linear equations with $n(n-m)$ unknowns. By using Gaussian elimination, $m(n-m)$ unknowns can be eliminated using the linear equations, which results in the computational complexity, $O(m^3(n-m)^3)$. Then, the quadratic parts are underdefined multivariate quadratic equations, with $(n-m) \frac{(n-m-1)}{2}$ quadratic equations and $(n-m)(n-m)$ unknowns. It is still a typical MQ equation system, similar to the equations of B , however, n is replaced by $n-m$. Referring to the result for B from Eq. (19), the complexity for attacking S_2 with a known S_1 can be estimated as follows:

$$d_{S_2} \sim 2^{3k \log_2^{m(n-m)} + (n-m)^2k - k_m} + 2^{\frac{(n-m)(n-m+1)k}{2} + k_0} \tag{21}$$

where $3k \log_2^{m(n-m)}$ in the exponent arises from the Gaussian elimination calculations.

Similarly, the complexity for attacking S_1 with a known S_2 is estimated as follows:

$$d_{S_1} \sim 2^{3k \log_2^{m(n-m)} + m^2k - k_m} + 2^{\frac{m(m+1)k}{2} + k_0} \tag{22}$$

According to Eqs. (20–22), the complexity of attacking S_1 and S_2 are all exponential, increasing with $O(m^2k)$ and $O((n-m)^2k)$, respectively, thus providing the criteria for the proper choice of the parameters S_1 and S_2 to achieve computational security of the MWOD scheme. For example, if $n=8$, $m=4$, and $k=16$, the complexity for S_1 and S_2 must be of order $2^{448} + 2^{160+k_0}$, $2^{448} + 2^{160+k_0}$, respectively, which satisfies the security requirements of most applications. The parameter k_m is neglected in the latter two cases because all currently available QM accelerated algorithms are more effective than an exhaustive search only for massively large cases.

It is difficult for the malice operators to solve the operands of extraction functions $\mathcal{V}_1(\cdot, \cdot)$ and $\mathcal{V}_2(\cdot, \cdot)$ because of S_1 and S_2 cannot be mutually derivate. The above analysis proved that the CONDITION 2 can be also met.

What has been discussed above, the security of multiple watermarks embedding operands has been proved, which ensure the security of watermarking operation domains. So, this proof allows that multiple watermarks can be flexibly embedded in the distribution of the multimedia cover, which makes MWOD better practicability.



Fig. 2 Original 256×256 “Lena” and “Baboon”

4 Experimental results

We tested the proposed scheme on many testing images selected from the USC-SIPI Image Database (freely available at <http://sipi.usc.edu/database/>). But only the experimental results of Lena and Baboon (in Fig. 2) will be given below due to the limited space. Four 32×32 binary logo images, as shown in Fig. 3, are used as perceptual meaningful watermarks in the experiments. The whole original image is transformed to DCT domain (suitable for other transform domains). The length of each watermark \mathbf{W}_i is 32×32=1024. We choose partial low-frequency components of DCT to form the host vector X , in which these components tend to have large energies so that embedded watermark tend to be robust against different kinds of attacks. We generate an orthogonal matrix $B=(b_1, b_2, \dots, b_8)$ with 8 by 8, which only satisfies Eq. (1). We divide B into 4 sub-matrixes, $S_1=(b_1, b_2)$, $S_2=(b_3, b_4)$, $S_3=(b_5, b_6)$, $S_4=(b_7, b_8)$ to embed 4 watermarks into images for facilitate description. The experiments use the hybrid watermarking embedding rule. We define $\mathcal{W}(\cdot, \cdot, \cdot) / \mathcal{V}(\cdot)$ as watermarking embedding/ extraction.

Like most multiple watermarking schemes, PSNR of watermarked image was selected in this paper to demonstrate the impact of watermarking embedding, on the image quality, varies with N_{EW} . So the image degradation with respect to multiple watermarking is tested. The typical results of the experiments, the MWOD-watermarked Lena and Baboon images (4 watermarks), are shown in Figs. 4 and 5 respectively. The results show that the visual quality of 4-watermarked image is acceptable.

In the condition of the same embedded information, we compared the PSNR of watermarked images of proposed MWOD scheme, with the schemes proposed by Wang and Lian [16] and Peter et al. [17]. The results are shown in Fig. 6. Though all PSNR curves with N_{EW} are descending obviously, but the proposed scheme has higher PSNR than Wang and Lian [16] and Peter et al. [17]. It generally means that the proposed scheme has better visual quality than others under the same conditions.

Additionally, for demonstrating the robustness of MWOD, the average detection scores of watermarks (ADS) vary with capacity and N_{EW} is considered for examination. The ADS is computed by Eq. (23). The following is ADS equation:



Fig. 3 Original logo “Alphabet” (Right)



Fig. 4 MWOD-watermarked Lena image with 4 watermarks embedded. PSNR=46.096 dB. 4 Extracted watermark (Right)

$$ADS = \text{mean}(DS(\mathbf{W}_1 + \mathbf{W}_2 + \mathbf{W}_3 + \mathbf{W}_4)) \quad (23)$$

where \mathbf{W}_i denotes the detection score of i -th watermark.

Certainly, the whole equivalent capacity of embedded watermarks is positively correlated to the N_{EW} . In the experiment, the N_{EW} in multi-watermarking is valued from 1 to 10, and each embedded watermark is restricted in equal size given as 16×16 , 32×32 , and 64×64 respectively. The ADS of watermarks in different size vary with the number watermarks for proposed scheme is shown in Fig. 7. It has been shown that, a greater N_{EW} result in the worse ADS of watermarks in same size of single watermark, and a larger capacity of single watermark has the lower of ADS under the same N_{EW} . It is also shown that, the proposed scheme has good ADS (>0.9) when N_{EW} less than 5. For a further insight of Fig. 7, it can be found that, under the same whole equivalent capacity of embedded watermarks, greater N_{EW} lead to a clearly lower ADS value. For example, 2 watermarks in the size of 32×32 and 8 watermarks in the size of 16×16 , their ADS values are 0.9978 and 0.8813 respectively. The fact reminds us that the N_{EW} surely impact the ADS. The reason could be that there is a relative greater error caused by the finite word-length precision of orthogonal transform and watermarking extraction threshold when the N_{EW} is greater.

From the perspective of the PSNR in Fig. 6 and average watermark detection scores in Fig. 7, we got the following results by testing various images: 4 watermarks were embedded into original images is acceptable. More than 4 watermarks may affect visual quality of watermarked image. From requirements of most multiple watermarking applications, 4 users are enough. So, we choose 4 watermarks to investigate the performance of multiple watermarking schemes with respect to JPEG compression, Additive Gaussian White Noise

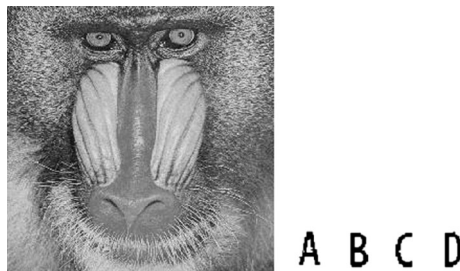


Fig. 5 MWOD-watermarked Baboon image with 4 watermarks embedded. PSNR=43.428 dB. 4 Extracted watermark (Right)

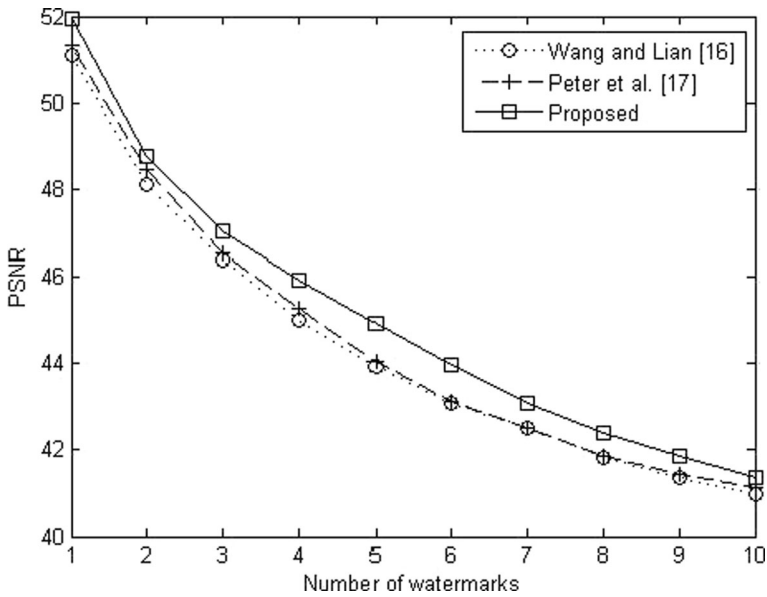


Fig. 6 PSNR versus N_{EW}

(AWGN), different filtering (high pass, median, low pass) and Geometric transformation attacks.

Several unintentional attacks are simulated for Lena image, including JPEG compression, high pass filter, median filter, low pass filter and noise. In the JPEG compression attack, the watermarked images are JPEG compressed with the default quantization matrix scaled by various the quality factor (QF) to achieve different compression ratio.

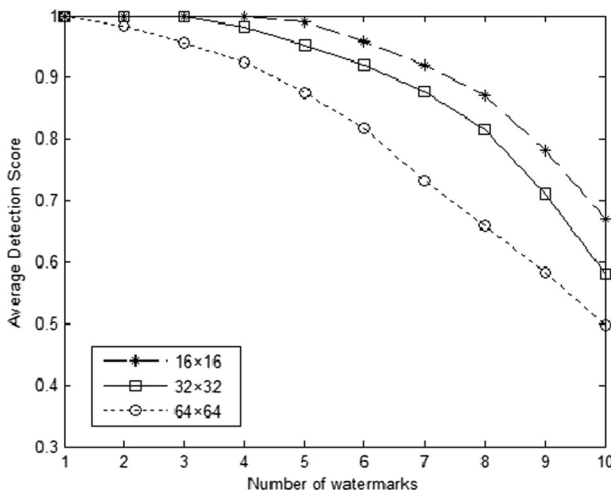


Fig. 7 Average detection score and capacity versus N_{EW}

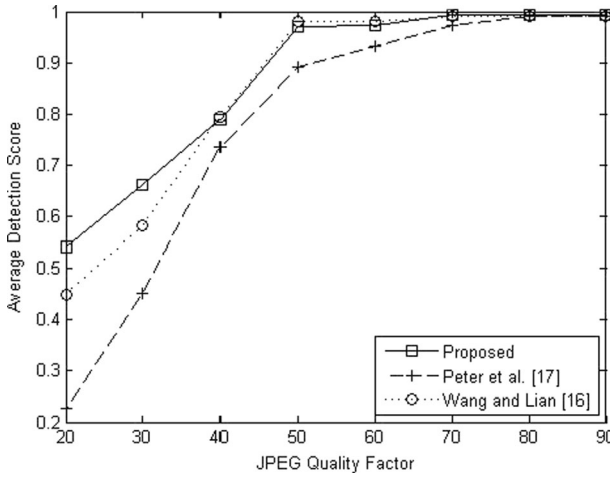


Fig. 8 Average detection score versus JPEG quality factor

In the JPEG attack on MWOD, we compute the ADS by Eq. (23). In Fig. 8, if JPEG Quality Factor ≥ 40 , there are little difference between MWOD and Wang et al. [16] in ADS value. In JPEG Quality Factor ≤ 40 , the proposed scheme is clearly better. The results mean that the proposed scheme has better robustness than Peter et al. [17] and Wang and Lian [16].

In the AGWN attacks on MWOD, the simulated results with different AGWN signal-to-noise ratio (SNR) are shown in Fig. 9. It can be seen that MWOD performs more and more remarkable robustness with the rise of AGWN SNR. The ADS of the proposed scheme is greater than Peter et al. [17] and Wang and Lian [16].

In the usual filters attacks on MWOD, a Lena image embedded four watermarks is attacked by High Pass Filter, Median Filter and Low Pass Filter with 3×3 filter. The simulated results are listed in Table 1. It can be shown that the proposed scheme has the highest ADS and better

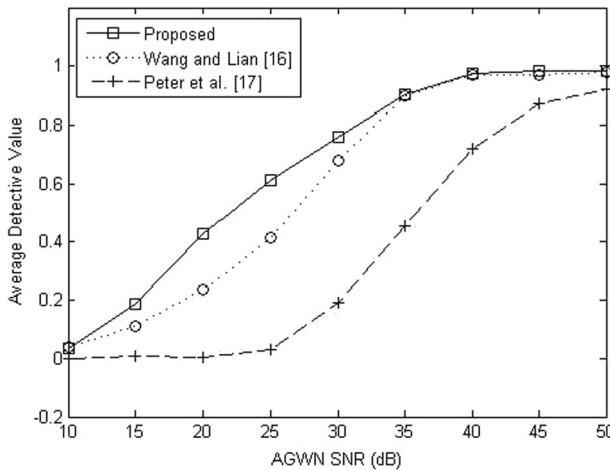


Fig. 9 Average detection score versus different AGWN SNR

Table 1 Average watermark scores with 3×3 filter

Algorithm	Average watermark detection scores		
	High pass filter	Median filter	Low pass filter
The proposed scheme	0.9072	0.9165	0.9251
Wang and Lian [16]	0.8945	0.7541	0.7145
Peter et al. [17]	0.8484	0.8431	0.8102

robustness. The resisting filter attacks performance of the proposed scheme is better than Peter et al. [17] and Wang and Lian [16].

In contrast to the above attacks, geometrical attacks do not attempt to remove the embedded watermark itself. Geometrical attacks usually make the watermark detector losing the synchronization information. The mostly well-known integrated tool for these kinds of attacks is StriMark [12, 13]. StriMark introduces the global distortions include scaling, rotation and cropping that belong to a class of general affine transformations.

For the scaling attacks on MWOD, the simulated results of various approaches for rescaling attacks with different sizes are list in Table 2. For example, the watermarked Lena with embedded 4 watermarks is scaled from 256×256 to 200×200. In order to recover the watermarks, the scaled image was rescaled to its original dimensions, and then extracting watermarks. The results show that the larger watermarked image scaling, the worse extracted watermark effect. It can be seen that the proposed scheme has the highest ADS and Peter et al. [17] scheme has the lowest ADS in every scale size.

For the rotation attacks on MWOD, the simulated results of various approaches for rotation attacks with different degrees are listed in Table 3. After the watermarked Lena image is rotated with various degrees (such as 5°, 15°, 20° and 30°), we selected the pixel densest portions and most complete image as watermarking extraction object. And the missing portions of the image were replaced with portions from the original *unwatermarked* Lena image. It can be seen that MWOD's ADS is higher than Wang and Lian [16] and Peter et al. [17].

Table 2 Average watermark scores with scaling attacks







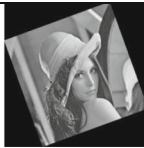

Different scaling size	Average Watermark Detection Scores			
	200×200	150×150	100×100	50×50
Watermarked Lena				
The Proposed Scheme	0.9201	0.7994	0.6895	0.5223
Wang and Lian [16]	0.8891	0.7721	0.6429	0.4887
Peter et al. [17]	0.7948	0.6935	0.5813	0.4321

Table 3 Average watermark scores with rotation attacks

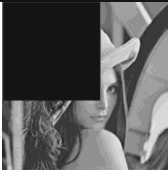
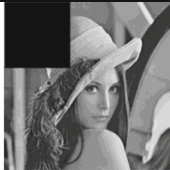
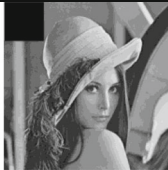
Average Watermark Detection Scores				
Different rotation degree	5°	15°	20°	30°
Watermarked Lena				
The Proposed Scheme	0.9143	0.8488	0.7986	0.7034
Wang and Lian [16]	0.9012	0.8113	0.7564	0.6596
Peter et al. [17]	0.8311	0.7721	0.6901	0.5943

For the cropping attacks on MWOD, the simulated results of various approaches for cropping attacks with different cropping size are listed in Table 4. We cropped different sizes from watermarked Lena image. In order to extract the watermarks from this image, the cropped portions of the image were replaced with portions from the original *unwatermarked* Lena image. It can be shown that a less cropping size results in less impact on watermarking detection. MWOD's ADS is higher than Wang and Lian [16] and Peter et al. [17].

From what has been discussed above, we could conclude that resisting geometric attacking performance of the proposed scheme is better than that of Wang and Lian [16] and Peter et al. [17].

In this section, unintentional and geometric attacking experiments have been accomplished. All results show that, MWOD can provide accepted visual quality under rational number of embedded watermarks, has better anti-attacks performance and watermarking robustness than Peter et al. [17] and Wang and Lian [16] in suffering various attacks.

Table 4 Average watermark scores with cropping attacks

Average Watermark Detection Scores			
Different cropping size	150×150	100×100	60×60
Cropped watermarked Lena			
The Proposed Scheme	0.6575	0.7895	0.9093
Wang and Lian [16]	0.5742	0.7543	0.8621
Peter et al. [17]	0.5476	0.7161	0.8498

5 Conclusions and future work

This paper proposes a multiple watermarking scheme based on orthogonal decomposition. The MWOD scheme can embed multiple watermarks into different domains using multiple orthogonal operation domain keys, without need for considering the correlation among them. Therefore, multiple watermarks can be flexibly embedded in the distribution of the multimedia cover. The security among watermarking operation domains was validated by theoretical analyses and the validity of the scheme was verified through experiments. The performance analysis and experimental results can also provide the reference information for user to select suitable algorithm and strategy for adapting different application scenarios and adjust rational parameters for optimizing the performance, such as the choice of watermarking number, hybrid watermarking strategy, setting rational the word length and dimension of transform matrix B etc. Through some comparative experiments, MWOD has been demonstrated a better robustness. That gives us the confidence that MWOD will be a promising practical protection tools for digital multimedia.

MWOD will have more application and prospects in the protection for multimedia in the scenario of multiple media providers or service providers, especially for cloud environment; there at least exists two basic application scenarios for multiple watermarking, the one based on different computing clouds and the other based on different servers in the same or different computing clouds. Meanwhile, MWOD has potential to combine re-encryption algorithm conveniently to construct a full protection scheme for digital multimedia in cloud. In the future, the combination of MWOD with re-encryption algorithm and the complete protocol based on MWOD for protecting digital multimedia in cloud will be the main research direction of our study.

Acknowledgments This work was supported by the National Basic Research Program of China (973 Program) under Grant 2011CB302306, 2011CB302204, the National Natural Science Foundation of China under Grant 41371402, 41101416 and the Research Fund for Doctoral Program of Higher Education of China under Grant 20110141110056.

References

1. Badran EF, Sharkas MA, Attallah OA (2009) Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images, National Radio Science Conference (NRSC 2009). IEEE Press, Cairo, pp 1–8
2. Chamlawi R, Khan A, Usman I (2010) Authentication and recovery of images using multiple watermarks. *Comput Electr Eng* 36(1):578–584
3. Chen W (2008) Multiple-watermarking scheme of the European Article Number Barcode using similar code division multiple access technique. *Appl Math Comput* 197:243–261
4. Cheng Q (2009) Generalized embedding of multiplicative watermarks. *IEEE Trans Circuits Syst Video Technol* 19(7):978–988
5. Courtois N, Goubin L, Meier W, and J-D Tacier (2002) Solving Underdefined Systems of Multivariate Quadratic Equations. Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography, pp 211–227, February 12–14
6. Cox JJ, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. *IEEE Trans Signal Process* 6(12):1673–1687
7. Lie WN, Lin GS, Wu CL, Wang TC (2000) Robust image watermarking on the DCT domain. *Proc IEEE Int Symp Circuits Syst* 1(5):228–231

8. Li-jun C, Rui L, Ye-qing Y (2012) A multiple watermarks algorithm for image content authentication. *J Cent South Univ* 19:2866–2874
9. Lu C, Hsu C (2007) Near-optimal watermark estimation and its countermeasure: anti-disclosure watermark for multiple watermark embedding. *IEEE Trans Circuits Syst Video Technol* 17(4):454–467
10. Mairgiotis A, Galatsanos N, Yang Y (2008) New additive watermark detectors based on a hierarchical spatially adaptive image model. *IEEE Trans Inf Forensics Secur* 3(1):29–37
11. Perez-Gonzalez F, Mosquera C (2008) Quantization-based data hiding robust to linear-time-invariant filtering. *IEEE Trans Inf Forensics Secur* 3(2):137–152
12. Petitcolas FAP (2000) Watermarking schemes evaluation. *IEEE Signal Process* 17(5):58–64
13. Petitcolas F, Stirmark Benchmark (2002) <www.petitcolas.net/fabien/watermarking/stirmark/>.
14. Stankovic S, Djurovic I, Pitas I (2001) Watermarking in the space/spatial-frequency domain using two-dimensional Radon-Wigner distribution. *IEEE Trans Signal Process* 10(5):650–658
15. Takahashi A, Nishimura R, Suzuki Y (2005) Multiple watermarks for stereo audio signals using phase-modulation techniques. *IEEE Trans Signal Process* 53(2):806–815
16. Wang J, Lian S (2012) On the hybrid multi-watermarking. *Signal Process* 92:893–904
17. Wong PHW, Au OC, Yeung YM (2003) A novel blind multiple watermarking technique for images. *IEEE Trans Circuits Syst Video Technol* 13(8):813–830
18. Xiao J, Wang Y (2009) Multiple Watermarking with Side Information. In *International Workshop on Digital Watermarking 2008*. Spring-Verlag, Busan, Korea, LNCS 5450, 379–387
19. Zhang Y, Niu X, Zhao D (2005) A method of protecting relational databases copyright with cloud watermark. *J Inf Commun Eng* 1(7):337–341



Lizhi Xiong is a Ph. D. candidate of communication and information system in the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, China. His research interests include digital multimedia processing and information security.



Zhengquan Xu received the B. S. and M. S. degrees from Tsinghua University, China, in 1985 and 1988, and the Ph. D. degree from the Hong Kong Polytechnic University, HK, in 1999. He is currently a professor with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan, China. His current research interests include multimedia forensics, video encryption, and spatial data security.



Yanyan Xu is currently a professor with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan, China. Her current research interests include multimedia information processing and information security.