International Journal of Automation and Computing

DOI: 10.1007/s11633-016-1010-6

Quantization Based Watermarking Methods Against Valumetric Distortions

Zai-Ran Wang[1,2] Jing Dong[2] Wei Wang[2]

[1]College of Engineering and Information Technology, University of Chinese Academy of Sciences, Beijing 100049, China

[2]Center for Research on Intelligent Perception and Computing,

National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

Abstract: Most of the quantization based watermarking algorithms are very sensitive to valumetric distortions, while these distortions are regarded as common processing in audio/video analysis. In recent years, watermarking methods which can resist this kind of distortions have attracted a lot of interests. But still many proposed methods can only deal with one certain kind of valumetric distortion such as amplitude scaling attack, and fail in other kinds of valumetric distortions like constant change attack, gamma correction or contrast stretching. In this paper, we propose a simple but effective method to tackle all the three kinds of valumetric distortions. This algorithm constructs an invariant domain first by spread transform which satisfies certain constraints. Then an amplitude scale invariant watermarking scheme is applied on the constructed domain. The validity of the approach has been confirmed by applying the watermarking scheme to Gaussian host data and real images. Experimental results confirm its intrinsic invariance against amplitude scaling, constant change attack and robustness improvement against nonlinear valumetric distortions.

Keywords: Quantization index modulation (QIM), watermarking, valumetric distortions, amplitude scaling, constant change attack.

1 Introduction

With the rapid development of computer sciences and technology, digital multimedia data is more and more popular to facilitate our daily life. At the same time, digital multimedia data is more easily to be accessed, tampered, duplicated and distributed, which results in problems of multimedia tampering, unauthorized usage and transmissions. To settle these problems, digital watermarking is proposed as a promising technique. The basic idea of digital watermarking is to embed some information into multimedia data and the embedded information can be extracted for copyright protection or authentication. Generally, watermarking has three characteristics: robustness, transparency and capacity. Robustness is the ability to resist signal processing operations such as digital-to-analog-to-digital conversions, lossy compression, geometric distortions, etc. Transparency means that the degradation introduced by watermarking should be very difficult for a viewer to perceive. And capacity is the number of bits of information embedded in multimedia data. According to robustness, watermarking can fall into three categories of robust, semi fragile and fragile methods. Robust watermarking mainly serves for copyright protection while semi-fragile and fragile watermarking are usually used for data authentication applications. Typically, there are two basic watermarking schemes: spread spectrum (SS) based watermarking[1, 2] and quantization based watermarking[3, 4]. In SS based watermarking methods, a pseudo-random noise-like watermark is added into the host signal. The advantage of insertion of a watermark under this regime is its robustness to signal processing operations and common geometric transformations. Ruanaidh and Pun[5] introduced the fourier-mellin-based approach and code division multiple access (CDMA) spread spectrum encoding methods to resist any combination of rotation and scale transformations. Malvar and Florencio[6] proposed an improved spread spectrum watermarking, in which the host signal does not act as a noise source, and this leads to significant gains compared with traditional spread spectrum based watermarking. Barni et al.[7] addressed the problem of optimum decoding and detection of a multibit, multiplicative watermark hosted by Weibull-distributed features in the magnitude-of-DFT domain. Liu et al.[8] derived a locally optimum detectors in closed forms for arbitrary host signal distributions and arbitrary just noticeable difference models that exploit the self-masking property of the human visual system (HVS).

The class of quantization index modulation (QIM) algorithms[3] is one of the most popular watermarking schemes because of its robustness against the additive white gaussian noise (AWGN) channel and high capacity. In QIM, the hidden message is embedded by quantizing the host signal samples with a quantizer chosen among a set of quantizers that are associated with the hidden message. The basic implementation of QIM is the dither modulation (DM)[9], which adopts a set of scalar and uniform quantizers. Later, the distortion compensated QIM (DC-QIM)[9] was introduced by combining distortion compensation technique with QIM to improve the achievable

Research Article

Manuscript received June 17, 2015; accepted September 22, 2015

The work presented in this paper was supported by Nature Science Foundation of China (Nos. 61303262 and U1536120).

rate distortion-robustness tradeoffs of QIM methods. The spread-transform dither modulation (STDM)[9] extended the original DM by quantizing the projection of the host signal vector along a random direction. Perez-Gonzalez et al.[10] and Bartolini et al.[11] theoretically investigated the performance of the QIM based watermarking methods.

In practical applications, the watermarked multimedia may undergo some attacks, intentionally or unintentionally, such as JPEG compression, image filtering, geometric distortions, etc. To resist these kinds of attacks, many watermarking schemes have been presented. For example, Run[12−15] proposed several robust watermarking methods for e-government document copyright protection. Two fragile watermarking methods[16, 17] were proposed for content authentication. To deal with geometric attacks, Dong[18] introduced an image normalization procedure before watermark embedding to transform image into a domain, which is invariant to affine transform attacks. Pereira and Pun[19] embedded a template in images to detect transformations undergone by the image, then the geometric distortions were inverted before applying the watermark detector. The operations applied at the watermark embedding or extraction stage can be seen as certain preprocessing stage. The objective of preprocessing is to seek or construct robust regions/features for watermark embedding, or invert the distortions applied on the watermarked signal.

Recently, quantization based watermarking has grabbed the attention of researchers because of its high capacity and robustness to the AWGN channel. As many researchers have addressed, the main weakness of QIM based watermarking is its sensitivity to valumetric distortions (i.e., any kind of amplitude scaling or gamma compensation)[20]. These kinds of distortions are rather commonly observed in video processing. For instance, nonlinear valumetric correction is used for better cathode ray tube (CRT) display or the contrast of an image may be adjusted to improve the visual effect. Valumetric distortions usually have small impacts on the quality of the attacked multimedia, but they can dramatically degrade the performance of quantization based watermarking schemes, because these distortions will result in the mismatch of quantization step between the encoder and decoder. Hence, researching watermarking methods that are robust against valumetric distortions has great significance.

In general, valumetric distortions can be classified into linear valumetric distortions and nonlinear valumetric distortions. Linear valumetric distortions include valumetric scaling attack (VSA) and constant change attack, and nonlinear valumetric distortions include gamma-correction, contrast stretching, etc. In the last few years, a lot of quantization based watermarking schemes have been proposed to deal with this problem, but these methods can only tackle the amplitude scaling attack. Guccione and Scagliola[21] made use of proper mapping of the pixel values from the Cartesian to hyperbolic coordinates to solve the nonlinear valumetric distortion modelled by a power-law attack, which is a combination of constant exponentiation and constant gain scaling of the amplitudes of the watermarked signal. But this method ignores the constant change attack. In our previous work[22], we proposed a spread transform based quantization watermarking method, which considers amplitude scaling distortion, constant change attack and nonlinear valumetric distortion. However, this paper improves the performance of our previous method. The main idea of this paper is that: an invariant domain is first constructed by spread transform, in which an amplitude scale invariant watermarking scheme is applied to obtain both amplitude scale and constant change invariant properties. As we use the previously watermarked samples to construct the invariant domain, the length of the embedding space will not be decreased, compared with our previous work. Hence, the capacity of the method of this paper is larger than that of our previous method[22]. Several typical amplitude scale invariant watermarking schemes are implemented in our experiments, including RDM[23], AQIM[24], Zareian′s method[25] and NCDM[26]. Experimental results demonstrate that our method not only solves the drawback of sensitivity to constant change attack, but also significantly improves the robustness to resist gamma correction distortion and contrast stretching. What is more, our method has very small effect on their robustness to other common attacks.

The rest of this paper is structured as follows. In Section 2, we introduce some notations and problem model of the digital watermarking. Section 3 gives an overview of the related work. Section 4 presents our watermarking method. Then, experimental results are shown in Section 6. Conclusions are given in Section 7.

2 Problem formulation

2.1 Notation

In this paper, uppercase letters denote random variables, lowercase letters denote their individual values, and boldface fonts indicate sequences or vectors. For instance, $\boldsymbol{x} = (x_1, x_2, \cdots, x_N)$, where x_k refers to the k-th element, and the length of the vector will be clear from the context.

We assume that the host signal is represented by vector $\boldsymbol{x}$. The host signal could be a vector of pixel values, DCT/DWT coefficients or any other transform domain coefficients from a host content. For analytical purposes, the samples x_k can be considered as generated according to a random variable X, X_k are assumed independent and identically distributed (i.i.d.) Gaussian random variables with mean u_x and variance σ_x^2. The watermarked signal is denoted by $\boldsymbol{y}$. The difference vector $\boldsymbol{w} \triangleq \boldsymbol{y} - \boldsymbol{x}$ is called the watermark signal. The embedding distortion D_e is measured by the average power of the watermark signal

$$D_e = \frac{1}{N}\mathrm{E}\{\|\boldsymbol{w}\|^2\} \tag{1}$$

where L is the length of the vector $\boldsymbol{w}$, $\|\cdot\|$ stands for Euclidean (i.e., l_2) norm and $\mathrm{E}\{\cdot\}$ is the expectation operator. The document-to-watermark ratio (DWR), which is used to

measure the embedding strength and fidelity of the watermarked signal, is defined as $\zeta \triangleq \frac{\mathrm{E}\{\|\boldsymbol{x}\|^2\}}{\mathrm{E}\{\|\boldsymbol{w}\|^2\}}$.

2.2 Channel

When the watermarked signal $\boldsymbol{y}$ is transmitted on a channel, it might be attacked by various common signal processing manipulations (e.g., lossy compression and addition of noise) or even intentional attempts to remove the embedded information. Without loss of generality, the channel distortion can be modeled as an unknown source additive white noise $\boldsymbol{n}$, which has zero mean with variance σ_n^2 and is independent of the watermarked signal. Then the distorted watermarked signal can be written as $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{n}$. And the channel distortion D_c is defined as

$$D_c = \frac{1}{L}\mathrm{E}\{\|\boldsymbol{n}\|^2\}. \tag{2}$$

Similar to DWR, the document-to-noise ratio (DNR) is defined as $\eta \triangleq \frac{\mathrm{E}\{\|\boldsymbol{y}\|^2\}}{\mathrm{E}\{\|\boldsymbol{n}\|^2\}}$ and the watermark-to-noise ratio (WNR) is defined as $\lambda \triangleq \frac{\mathrm{E}\{\|\boldsymbol{w}\|^2\}}{\mathrm{E}\{\|\boldsymbol{n}\|^2\}}$.

Recently, valumetric distortions to the quantization based watermarking have grabbed much attention of researchers. Valumetric distortions can be seen as a generic function applied pointwise to all the image pixels that modified their original values[21]. Valumetric scale attack $\boldsymbol{z} = \rho\boldsymbol{y}$ is a typical linear valumetric distortion, which is a scale of the pixel amplitude and results in brightness and contrast change for images and video. Another typical linear valumetric distortion is the constant change distortion $\boldsymbol{z} = \boldsymbol{y} + c$, where a constant value c is added to the pixel value. Gamma correction is a typical nonlinear valumetric distortion, which is a more widely used valumetric distortion. For example, Gamma correction is always applied when the signal has passed through digital-to-analog/analog-to-digital conversions. The Gamma correction function is given by

$$\Gamma_\gamma(p) = p_{\max}(\frac{p}{p_{\max}})^\gamma \tag{3}$$

where γ is the correction factor and $p_{\max}$ is the maximum value of the image pixels.

3 Related work

In recent years, quantization based watermarking methods that can resist valumetric distortions have aroused great interest of researchers. A lot of work has been done in this kind of watermarking method. In this section, we give a brief overview of the watermarking methods that have been proposed to resist valumetric attacks, and classify these methods into four categories.

Among valumetric distortions, valumetric scale attack has received special attention. These methods can be divided into four categories as follows.

1) Estimating amplitude scale parameter: Egger et al.[27] embedded an auxiliary pilot signal in the host data, which was used by the decoder to estimate the amplitude scale parameter. The disadvantage of this scheme is that it reduces the embedding capacity and decreases the algorithm security[20]. Shterev et al.[28, 29] proposed a maximum likelihood technique to estimate the amplitude scale in the watermark extraction process. The problem of this kind of scheme is its high computational complexity.

2) Using spherical codewords: Miller et al.[30] embedded watermark by using the lattice codes, which is inherently robust to amplitude scale. This scheme also has high computational complexity.

3) Adaptive quantization step: Perez-Gonzalez et al.[23] proposed the rational dither modulation (RDM) watermarking method, where an amplitude scale invariant adaptive quantization step size at both embedder and decoder was used. Li and Cox[31] proposed an improved version of the RDM. Bas[32] presented a quantization watermarking technique by use of a fractal quantization structure during the detection but also a content dependent quantization grid to achieve both global constant robustness and the ability to recover the watermark after nonlinear valumetric distortions.

4) Constructing amplitude scale invariant features: In the angle QIM (AQIM)[24], the angle of a vector of image samples was quantized. Akhaee et al.[20] proposed a robust image watermarking scheme which was invariant to the gain attack. In this scheme, a line segment in the 2-D space was first constructed by use of four samples of the approximation coefficients of the image blocks, then the slope of this line segment was employed for watermarking purpose. In RDM, the ratio between a sample and several previously watermarked samples was utilized as a feature to embed watermark, so RDM also can be seen as feature based watermarking method. In the recent two years, Zhu et al.[26, 33] proposed a normalized coefficients dither modulation (NCDM) watermarking, which embedded watermark by quantizing the normalized cross correlation between the host signal vector and a random vector. Zareian et al.[25, 34] constructed the ratio of the root mean square of two host signal vectors to embed watermark. However, these methods only take linear amplitude scale attack into account. Guccione and Scagliola[21] presented an extension of the RDM data hiding scheme by use of proper mapping of the pixel values from the Cartesian to hyperbolic coordinates, which provided robustness against nonlinear distortions modeled by a power-law attack. Guerrini et al.[35] proposed a QIM based watermarking system, which embedded watermark into the kurtosis of selected image blocks to cope with nonlinear valuemetric scale attacks such as histogram stretching and gamma correction.

Although, there has been a wide research on the watermarking schemes robust to valumetric distortions, most of the methods mentioned above have the drawback that they cannot cope with the constant change attack and nonlinear valumetric distortions. Hence, in this paper, we propose a novel watermarking method, which considers the three types of valumetric distortions.

4 Proposed method

In our method, the host signal is firstly projected into a domain with a vector which satisfies certain constraint. Then an invariant domain is constructed, and a watermarking method that is invariant to amplitude scale attack is applied on this domain to embed watermark. Hence, our method can be seen as a preprocessing before watermark embedding. In this way, our method is intrinsically invariant to constant change attack and amplitude scale attack, and significantly improves the robustness against nonlinear valumetric distortions. In this chapter, we first introduce a method to construct the invariant domain. As this construction method will decrease the embedding capacity, we will introduce an improved method, which uses the previously watermarked samples to construct the invariant domain.

4.1 Construction method of the invariant domain

4.1.1 Invariant domain construction by spread transform

Let us represent $\boldsymbol{s}$ as the host signal vector consisting of L_s un-watermarked signal samples $\boldsymbol{s} = \{x_k, x_{k+1}, \cdots, x_{k+L_s-1}\}$, let $\boldsymbol{u} = \{u_1, u_2, \cdots, u_{L_s}\}$ be a spread vector which is randomly obtained by a key k_u. The key idea is to project $\boldsymbol{s}$ onto $\boldsymbol{u}$ to obtain an invariant domain. The projection of $\boldsymbol{s}$ onto $\boldsymbol{u}$ is defined as the dot product of the two vectors:

$$f_s = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{u} = \sum_{i=1}^{L_s} s_i u_i. \tag{4}$$

When a constant value c is added to the host signal $\boldsymbol{x}$, then $\boldsymbol{s}$ is changed to be $\boldsymbol{s}'$: $\boldsymbol{s}' = \{x_k + c, x_{k+1} + c, \cdots, x_{k+L_s-1} + c\}$, and f_s is changed to be f_s':

$$f_s' = (\boldsymbol{s} + c)^{\mathrm{T}}\boldsymbol{u} = \sum_{i=1}^{L_s} s_i u_i + c\sum_{i=1}^{L_s} u_i. \tag{5}$$

Compared with (4), there is an extra part $c\sum_{i=1}^{L_s} u_i$ in (5), which is the product of the constant value c and the sum of the elements of the spread vector $\boldsymbol{u}$. Hence, to eliminate the effect of the constant value c and construct an invariant domain f_s, the extra part $c\sum_{i=1}^{L} u_i$ must be zero. In other words, the spread vector $\boldsymbol{u}$ must satisfy the constraint that the sum of its elements must be zero, illustrated as the following equation:

$$\sum_{i=1}^{L_s} u_i = 0. \tag{6}$$

In addition to the constant change invariant property, the projection also holds the property of multiplication. When the signal samples $\boldsymbol{x}$ are scaled by a factor ρ, it is apparent that the vector $\boldsymbol{s}$ is also scaled by ρ. And the projection becomes:

$$f_s' = (\rho \cdot \boldsymbol{s})^{\mathrm{T}}\boldsymbol{u} = \rho \cdot \sum_{i=1}^{L} s_i u_i = \rho \cdot f_s \tag{7}$$

which means that if the vector $\boldsymbol{x}$ is scaled by ρ the projection f_s will also be scaled by ρ. Hence, when an amplitude scale invariant watermarking method, such as RDM, AQIM, NCDM and Zareian′s method, is applied on the constructed domain, both amplitude scale and constant change invariant properties can be obtained. This is the basic idea of the proposed method.

4.1.2 Inverse spread transform

After watermark embedding, the projection f_s is modified to be f'_s. Then, the inverse spread projection is applied to obtain the watermarked signal vector $\boldsymbol{s}' = \{y_k, y_{k+1}, \cdots, y_{k+L_s-1}\}$, so that the following equation is satisfied:

$$\sum_{i=1}^{L_s} s'_i u_i = f'_s. \tag{8}$$

Obviously, there are many solutions of $\boldsymbol{s}'$ to satisfy (8). But in watermarking systems, the distortion resulting from watermark embedding should be as small as possible. To this end, combined with (4) and (8), we can easily obtain $\boldsymbol{s}'$ by the following equation:

$$\boldsymbol{s}' = \frac{f'_s}{f_s}\boldsymbol{s}. \tag{9}$$

Notice that the above results are just applicable for the situation $f_s \neq 0$. In the case of $f_s = 0$, that is, f_s is identical to zero, it is easy to construct the vector $\boldsymbol{s}'$ satisfying the conditions $\sum_{i=1}^{L_s} s'_i u_i = f'_s$ in the following way:

$$s'_i = s_i + \frac{f'_s}{L \cdot u_i}. \tag{10}$$

4.2 Alternative construction method of the invariant domain

In this paper, we propose an alternative construction method of the invariant domain. The difference between the proposed method and our previous work is the way of the invariant domain construction. In the previous work, we constructed the invariant domain by a vector of non-watermarked samples. But in this paper, we construct the sample vector in this way: $\boldsymbol{s} = \{y_{k-L_s+1}, \cdots, y_{k-1}, x_k\}$. The first $L_s - 1$ elements of $\boldsymbol{s}$ are the previously watermarked samples, and the last element $s_{L_s} = x_k$ is the un-watermarked signal sample. The invariant domain is constructed by use of (4), which is same with our previous work.

In the process of inverse spread transform, the previously watermarked samples in vector $\boldsymbol{s}$ cannot be modified, and only the last element of $\boldsymbol{s}$ can be modified to embed watermark. In other words, the modification to the vector $\boldsymbol{s}$

must meet the following constraints:

$$\begin{cases} \sum_{i=1}^{L_s} s'_i u_i = f_s^{'} \\ s_i^{'} = s_i, \qquad 1 \le i < L_s. \end{cases} \tag{11}$$

Combined (4) and (11), the last element of the vector s is modified to be

$$s'_{L_s} = \frac{f_s^{'} - f_s}{u_{L_s}} + s_{L_s}. \tag{12}$$

Then, the watermarked signal vector $\boldsymbol{s}'$ is obtained as: $\boldsymbol{s}' = \{y_{k-L_s+1} \cdots y_{k-1}, y_k\}$, where $y_k = s'_{L_s}$.

As to the spread vector $\boldsymbol{u}$, there are many choices that meet the constraint (6). In this paper, we use the following spread vector:

$$\boldsymbol{u} = [-\frac{1}{L_s - 1}, -\frac{1}{L_s - 1}, \cdots, -\frac{1}{L_s - 1}, 1]. \tag{13}$$

4.3 Capacity influence

In the process of the invariant domain construction of our previous work, a sample vector $\boldsymbol{s}$ with length L_s is projected to a feature f_s with one dimension. Hence, the length of the constructed embedding space f_s becomes $\frac{1}{L_s}$ of the original embedding space $\boldsymbol{x}$. As a result, watermark capacity is degraded. However, in this paper, only the L_s-th element x_k of the vector $\boldsymbol{s}$ is the un-watermarked sample, and the length of the constructed embedding space f_s is equal to that of the original embedding space $\boldsymbol{x}$. Hence, this construction method has larger embedding capacity than our previous work.

5 Watermark embedding and extraction

5.1 Watermark embedding

5.1.1 Embedding process

There are three stages of the proposed watermark embedding method; the first one is the invariant domain construction, the second one is the actual embedding stage, and the third one is the inverse spread projection.

Fig. 1 illustrates the flowchart of our approach, where m denotes the embedded watermark information. The details are described in the following.

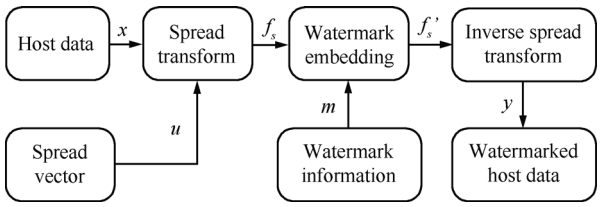

Fig. 1 Block diagram of the proposed watermark embedding method

1) Host signal vector $\boldsymbol{x}$ is first projected on a spread vector $\boldsymbol{u}$, which satisfies certain constraint, e.g., (6). Then an invariant domain f_s is obtained.

2) Watermark m is embedded by an amplitude scale invariant watermarking scheme on f_s. Then f_s is changed to $f_s^{'}$.

3) The inverse spread transform is applied to obtain the watermarked vector $\boldsymbol{y}$ according to $f_s^{'}$ and $\boldsymbol{u}$.

5.1.2 Embedding methods

In the second step of the embedding process, an amplitude scale invariant watermarking is applied on the invariant domain. There are several schemes which can be selected, in this paper, we chose RDM, AQIM, NCDM and Zareian′s method, which are typical and proposed in recent years. In the following, we will introduce basic ideas of the four watermarking methods.

1) Rational dither modulation (RDM):

In the basic RDM, the set of rational functions $g : \mathbf{R}^L \to \mathbf{R}, L \ge 1$ are used, which have the property that:

$$g(\rho \boldsymbol{y}) = \rho g(\boldsymbol{y}), \text{for all } \rho > 0,\ \boldsymbol{y} \in \mathbf{R}^L. \tag{14}$$

Given a host signal vector, $\boldsymbol{x} = (x_1 \cdots x_N)$ and a watermarked signal vector, $\boldsymbol{y} = (y_1 \cdots y_N)$, then the k-th bit $m_k \in \{0, 1\}$ of a watermark message is embedded in the L-th-order RDM as

$$y_k = g(y_{k-L}^{k-1}) Q_{m_k}\left(\frac{x_k}{g(y_{k-L}^{k-1})}\right) \tag{15}$$

where y_{k-L}^{k-1} denotes the set of watermarked samples $(y_{k-L} \cdots y_{k-1})$ and L is the number of previous watermarked samples used to calculate the function $g(\cdot)$, the function $Q_{m_k}(\cdot)$ is the standard quantization operation.

When a scale factor ρ is multiplied with the host signal vector, the variable in the quantization function will not be changed, as shown in the following:

$$\frac{x_k}{g(y_{k-L}^{k-1})} = \frac{\rho x_k}{g(\rho y_{k-L}^{k-1})} = \frac{x_k}{g(y_{k-L}^{k-1})}. \tag{16}$$

2) Angle quantization index modulation (AQIM):

Instead of embedding information by quantizing the amplitude of pixel values, AQIM works by quantizing the angle formed by the host-signal vector with the origin of a hyperspherical coordinate system.

In the 2-Dimensional case, let $x_i \in \mathbf{R}$ for $i = 1, 2$ be two samples taken from an arbitrary domain of the original image. The two samples x_1, x_2 may be viewed as a point in a two dimensional plane. This point can be described by its polar coordinates representation (r, θ). For that end, the angle θ is given by 17, as indicated below

$$\theta = \arctan(\frac{x_2}{x_1}). \tag{17}$$

Then, the angle θ is quantized as follows:

$$\theta^Q = Q_{m_i}(\theta, \Delta) = \left\lfloor \frac{\theta + m_i \Delta}{2\Delta} \right\rfloor 2\Delta + m_i \Delta \tag{18}$$

where $m_i \in \{0, 1\}$ is the watermark, and Δ is the quantization step size.

When a scale factor ρ is multiplied with the host signal vector, the angle of the two host signal samples will not be

changed, as shown in the following:

$$\theta^{'} = \arctan(\frac{\rho x_2}{\rho x_1}) = \theta. \tag{19}$$

3) Normalized correlation based dither modulation (NCDM):

In the NCDM, watermark embedding is performed through modulating the normalized correlation coefficients between the host vector and a random vector with dither modulation. Let $\boldsymbol{x} \in \mathbf{R}^L$ be a host signal vector in which the watermark message $m \in \{0, 1\}$ is embedded. First, a random vector $\boldsymbol{u} \in \mathbf{R}^L$ is generated by a random number generator initialized with the key K. Then, the normalized coefficient (NC) between $\boldsymbol{x}$ and $\boldsymbol{u}$ is computed as

$$f_x = \frac{\boldsymbol{x}^{\mathrm{T}}\boldsymbol{u}}{\|\boldsymbol{x}\| \, \|\boldsymbol{u}\|} \tag{20}$$

where $\|\cdot\|$ stands for Euclidean (i.e., l_2) norm. Obviously, f_x is in the range of -1 to 1. Taking the binary DM with uniform quantization into account, the feature signal f_x is quantized using the quantization function, yielding

$$f_m = Q_{m_k}(f_x). \tag{21}$$

When a scale factor ρ is multiplied with the host signal vector, the normalized correlation coefficients f_x will not be changed, as shown in the following:

$$f_x^{'} = \frac{(\rho\boldsymbol{x})^{\mathrm{T}}\boldsymbol{u}}{\|\rho\boldsymbol{x}\| \, \|\boldsymbol{u}\|} = f_x. \tag{22}$$

4) Zareian′s method:

In this scheme, the host signal vector is first divided into two parts, then l_p-norm of each vector is calculated. The watermark bits are embedded by quantizing the ratio of the l_p-norm of each part. Let $\boldsymbol{u}$ represents the host signal vector consisting of L variables $\boldsymbol{u} = \{u_1, u_2, \cdots, u_L\}$. The L samples of $\boldsymbol{u}$ are divided into two subsequences $\boldsymbol{x}$ and $\boldsymbol{y}$ containing the even and odd indexed terms, respectively: $x_i = u_{2i}$, $y_i = u_{2i+1}, i = 1, \cdots, \frac{L}{2}$. In order to embed the watermark message $m_k \in \{0, 1\}$ in $\boldsymbol{u}$, l_p-norm of $\boldsymbol{x}$ and $\boldsymbol{y}$ are calculated:

$$l_x = \left(\frac{2}{L}\sum_{i=1}^{\frac{L}{2}} |u_{2i}|^p\right)^{\frac{1}{p}}, \quad l_y = \left(\frac{2}{L}\sum_{i=1}^{\frac{L}{2}} |u_{2i-1}|^p\right)^{\frac{1}{p}} \tag{23}$$

where l_x and l_y are the l_p-norm of $\boldsymbol{x}$ and $\boldsymbol{y}$, respectively and $p \geq 1$. Then, the QIM method is applied to the ratio of l_x and l_y , $z = \frac{l_x}{l_y}$, as follows:

$$z_q = Q_{m_k}(z). \tag{24}$$

When a scale factor ρ is multiplied with the host signal vector, the l_p-norm of the signal vector will also be multiplied by ρ, as shown in the following:

$$l_x^{'} = \left(\frac{2}{L}\sum_{i=1}^{\frac{L}{2}} |\rho u_{2i}|^p\right)^{\frac{1}{p}} = \rho l_x. \tag{25}$$

And it is the same with $l_y^{'}$, hence, the ratio z' will be identical with z.

From (16), (19), (22) and (25), we can know that the features of the four methods used for quantizing to embed watermark are invariant to valumetric scale attacks. Hence, the four methods are all robust to this attack.

5.2 Watermark extraction

Fig. 2 illustrates the extraction process of the proposed method, which can be divided into the following steps:

1) The watermarked host data $\boldsymbol{y}$ is projected on the spread vector $\boldsymbol{u}$, which is same with the embedding process. Then the invariant domain is constructed, where watermark was embedded.

2) Extract the embedded information using the extraction method corresponding to the applied watermark embedding method. Then the extracted watermark information m' is obtained.

For the sake of simplicity, we only introduce the extraction method of RDM here, extraction methods of NCDM[26, 33], AQIM[24] and Zareian′s algorithm[25, 34] can be referred to corresponding papers. The hidden bit is retrieved from z_k by applying the standard DM decoding procedure to the rational function $\left(\frac{z_k}{g(z_{k-L}^{k-1})}\right)$, where z_k is the received signal in the spread transformed domain. Ideally, the received sample should be divided by $g(y_{k-L}^{k-1})$ to recover the same quantized quantity at the encoder, but due to the unavailability of $g(y_{k-L}^{k-1})$, $g(z_{k-L}^{k-1})$ is used as its estimate. Hence, the hidden information bit is estimated according to

$$m_k{}' = \arg \min_{m_k \in \{0,1\}} \left| \frac{z_k}{g(z_{k-L}^{k-1})} - Q_{m_k}(\frac{z_k}{g(z_{k-L}^{k-1})}) \right|. \tag{26}$$

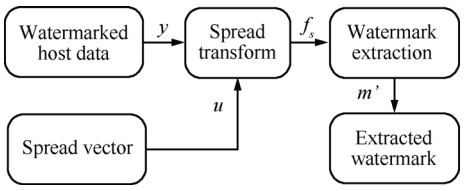

Fig. 2 Block diagram of the proposed watermark extraction method

6 Experimental results

In this section, a set of experiments are conducted to evaluate the performance of the proposed approach against different attacks. In Section 6.1, the experimental results for a Gaussian host signal are presented, while the experimental results for real images are presented in Section 6.2. We implement spread transform with four feature based amplitude scale invariant watermarking methods, RDM, AQIM, NCDM and Zareian′s method, and we denote them as STRDM, STAQIM, STNCDM and STZareian respectively.

6.1 Gaussian host

In this simulation, a sequence of 8192 i.i.d random samples is generated from the generalized Gaussian distribution, constrained to have values within the range $[0, 255]$. We first plot the empirical DWRs of our method in Fig. 3 as a function of the step size Δ, where the empirical DWRs are obtained using the host signal with the shape parameter $v_x \in \{8, 10\}$. Δ is in the range from 0.2 to 1, and the step size interval is 0.1. The empirical DWRs are obtained by averaging over 10 runs with 10 different host sequences. The length of the spread vector is 12 and 512 bits information are embedded in each method. One bit is embedded in 1, 2, 16, 16 samples on the constructed domain for the four methods respectively. Hence, watermark is repeatedly embedded for 8 times in STAQIM and 16 times for STRDM. As expected, the DWR decreases with Δ increasing. We can also observe that the four methods are insensitive to the probability density function of the host signal.

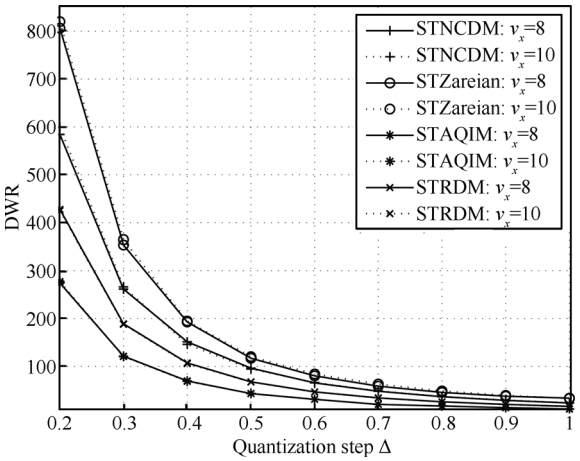

Fig. 3 Empirical DWR versus the quantization step Δ for our method

Figs. 4−7 shows the empirical bit-error probability of our methods as a function of WNR with different vector length L_s, which is in the range from 2 to 20, and the length interval is 2. The results are obtained using the host signal with $v_x = 8$ and the DWR is set to be 25. It can be seen that the bit error rate (BER) of the four methods are changed with the value of L_s. In general, the BER is decreased in case of the value of L_s is increased, but the results will be insensitive to L_s when the spread vector length is large enough. For example, the results of STNCDM and STZareian change very slightly when L_s is larger than 8, and the results of STAQIM and STRDM have little change when L_s is larger than 12. Hence, in the following experiments, L_s is set to be 12.

Fig. 8 illustrates the empirical bit-error probability of the proposed watermarking method and the original method under Gaussian noise addition, where the results are obtained using the host signal with $v_x = 8$. The WNR value is in the range from -20 to 0, and the interval is 2. We can see that the four methods show different characteristics against noise addition. The results of STNCDM, STZareian and STAQIM are better than their corresponding original methods NCDM, Zareian and AQIM, when the noise strength is

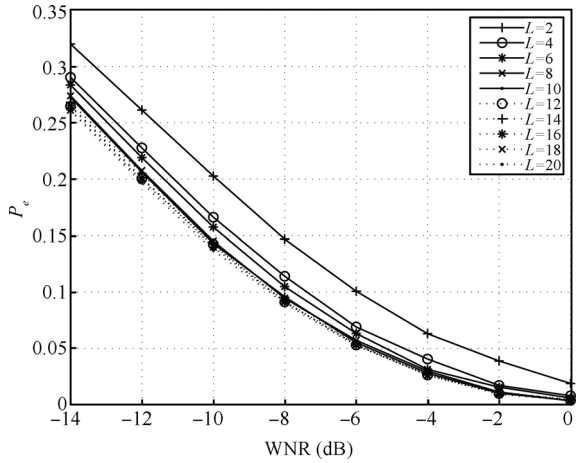

Fig. 4 Empirical bit-error probability of STNCDM with different vector length L_s under Gaussian noise attack

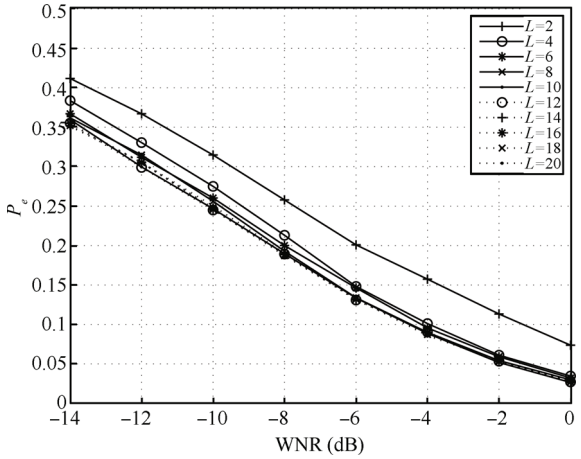

Fig. 5 Empirical bit-error probability of STZareian with different vector length L_s under Gaussian noise attack

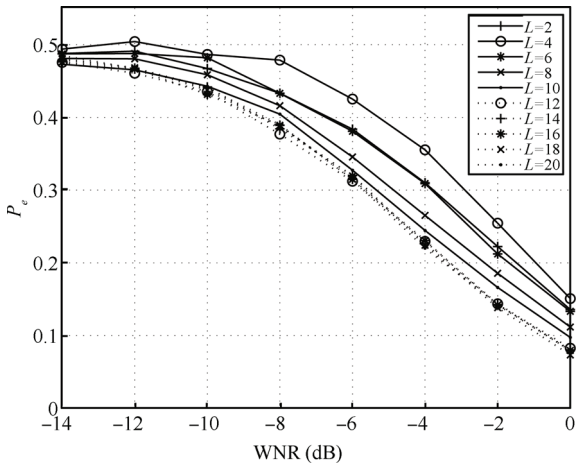

Fig. 6 Empirical bit-error probability of STAQIM with different vector length L_s under Gaussian noise attack

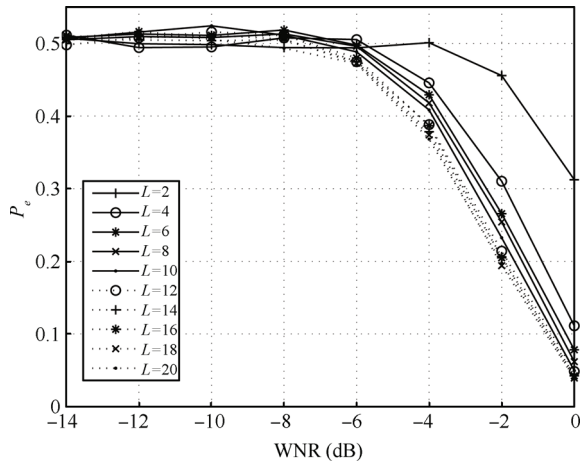

Fig. 7 Empirical bit-error probability of STRDM with different vector length L_s under Gaussian noise attack

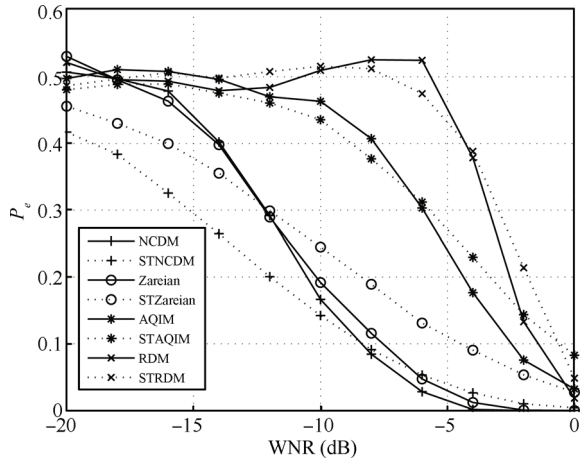

Fig. 8 Empirical bit-error probability of different watermarking methods versus WNR

large, and when the noise strength is small, this phenomenon is reversed. The robustness of STRDM and RDM under Gaussian noise attack are very similar on the whole range.

6.2 Real images

To show the performance of the proposed watermarking method on real applications, we implement our method in the wavelet transform domain of images. The lowest wavelet coefficients are selected to embed watermark in order to deal with some common attacks, such as lossy JPEG compression and filtering. Specifically, a three level wavelet transform with "db1" filter is applied to the test images. The obtained lowest wavelet coefficients are randomized and further transformed with a spread vector of length L_s. Then an invariant domain is obtained and watermark is embedded on this domain with RDM, AQIM, NCDM and Zareian. We test our method on some typical images with size of 512×512, and compared with the four original methods. The spread vector length L_s is set to 12 and vector dimensionality L of SNCDM and SZareian is set to 16, which allows a 256-bit message to be embedded into each image. For fair comparison, SRDM are embedded for 16 and 8 times respectively. Peak signal to noise ratio (PSNR) is utilized to measure the imperceptibility of the watermarked images and BER is used to measure the robustness. Various types of attacks are implemented in experiments. The four original watermarking methods (RDM, AQIM, NCDM, Zareian) and a nonlinear invariant watermarking method are also implemented for comparison. Parameters of all the methods are adjusted so that PSNR for all images is equal to 48 dB.

6.2.1 Watermark imperceptibility

Fig. 9 illustrates four original and watermarked images embedded with four watermarking methods. The parameters of the four methods are adjusted to make all the watermarked images have the same peak signal to noise ratio. As shown in this figure, all the watermarked images are almost the same as the original ones and it is very difficult to perceive the difference between them by human eyes. This confirms the imperceptibility of the proposed method.

Fig. 9 Original images (first row) and corresponding watermarked copies with a 256-bit message embedded and PSNR=48 dB, STRDM (second row), STAQIM (third row), STZareian (fourth row) and STNCDM (fifth row)

6.2.2 Watermark robustness

The robustness of the proposed method is tested against some typical image processing operations and compared with the original watermarking methods. For fair comparison, all the watermarked images are made to have the same perceptual quality and contain the same amount of watermark information. We select 100 images in our experiment and the results are the averaged BERs of the 100 test images.

1) Robustness against constant change attack: The re-

sults against constant change attack are shown in Fig. 10. The constant change value c ranges from -30 to 30. The dashed lines indicate BERs of four original methods, and the corresponding solid lines represent BERs of the four methods applied on our invariant domain. It can be seen that watermarking methods with spread transform are very robust to this attack, while the original four watermarking methods are very sensitive to the attack. In the four methods, STRDM, STAQIM and STNCDM show better performance compared with STZareian, and the BERs lie within the range $[0, 0.1]$.

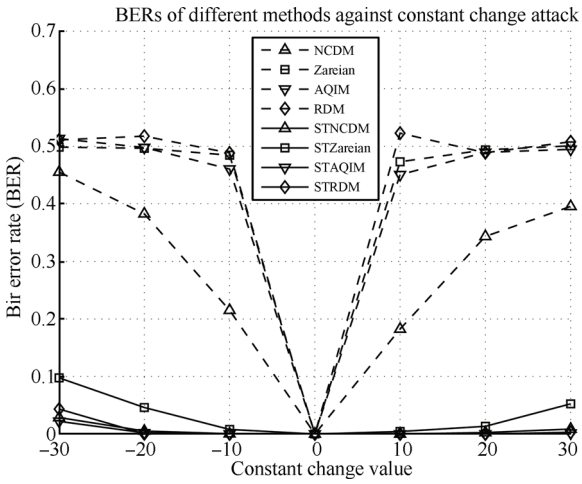

Fig. 10 BERs comparison of four methods with and without spread transform under constant change attack

2) Robustness against Gamma correction: Gamma correction is a typical nonlinear valumetric distortion, which is especially considered in video watermarking applications. We implement Gamma correction attack on the watermarked images in spatial domain. The Gamma factor γ ranges from -0.5 to 1.5, and the results are illustrated in Fig. 11. We can observe that our methods outperform the four original methods under Gamma correction attack. STNCDM and STZareian show better performance than NCDM and Zareian on the whole range, while STAQIM and STRDM have better robustness than AQIM and RDM when the Gamma correction strength is small.

3) Robustness against amplitude scale attack: Amplitude scale is a typical linear valumetric distortion. We implement this attack on the pixel values in spatial domain with gain factor ρ which ranges from 0.7 to 1.3. Fig. 12 illustrates the results of the proposed method and its original version against this attack. It can be seen that the BERs of STRDM, STAQIM and STNCDM are almost identical to their original version, and STZareian shows superior robustness compared to Zareian for $\rho < 1$. But the robustness of the four methods with spread transform shows a little worse when $\rho > 1$. The performance degradation in case of $\rho > 1$ may be ascribed to cropping and roundoff of the pixel values which results from amplitude scale.

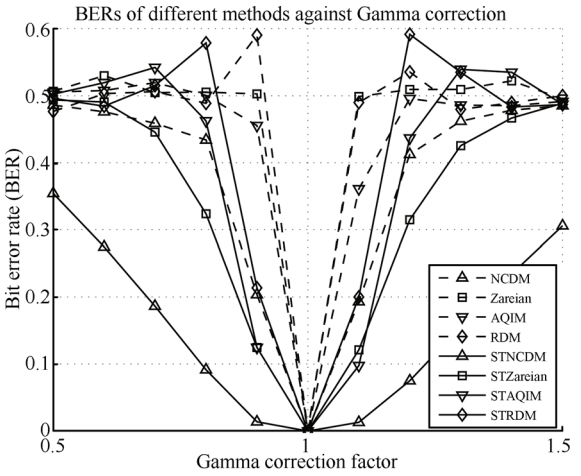

Fig. 11 BERs comparison of four methods with and without spread transform under gamma correction

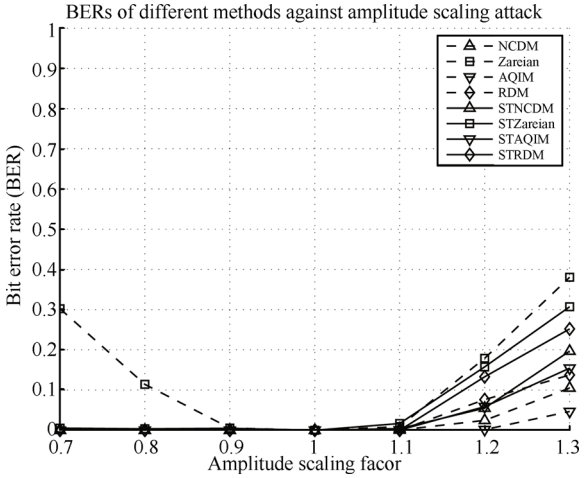

Fig. 12 BERs comparison of four methods with and without spread transform under amplitude scale attack

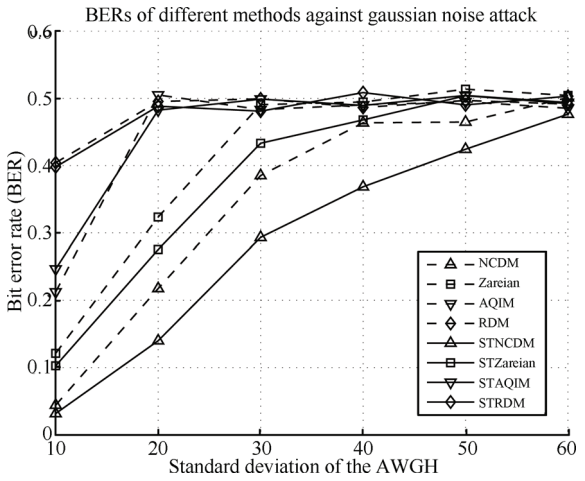

Fig. 13 BERs comparison of four methods with and without spread transform under Gaussian noise addition

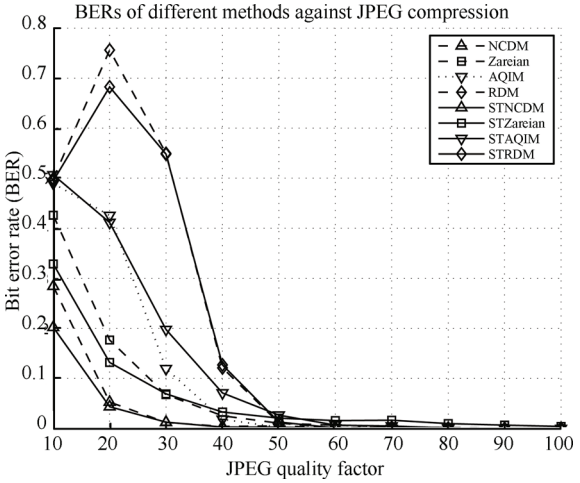

Fig. 14 BERs comparison of four methods with and without spread transform under lossy JPEG compression

4) Robustness against Gaussian noise addition: White Gaussian noise is a typical noise in image processing. We test this attack with different standard deviation σ_n, and the results are shown in Fig. 13. As can be seen, STNCDM and STZareian show better robustness compared to their corresponding original version, while the robustness of STAQIM and STRDM is very similar to AQIM and RDM on the whole range.

5) Robustness against lossy JPEG compression: Lossy JPEG compression is also a common image processing. Fig. 14 illustrates the results under this attack with different quality factors. It can be seen that the BERs of STAQIM and STNCDM have little difference compared to their corresponding version, while STNCDM and STZareian show better robustness than NCDM and Zareian in the case of low quality factors.

6) Robustness against image filtering: Three types of filtering attacks are implemented on the watermarked images, including average filtering, median filtering and wiener filtering with window size of 3×3. The results are shown in Table 1. It can be seen that the spread transform may result in some robustness degradation under filtering attacks, but the degradation degree is small, which is smaller than 3 percentage points.

Table 1 BERs comparison of four methods with and without spread transform under image filtering

Method	Average 3×3	Median 3×3	Wiener 3×3
NCDM	0.019 1	0.036 7	0.003 9
STNCDM	0.031 6	0.057 4	0.011 3
Zareian	0.048 4	0.095 7	0.013 7
STZareian	0.049 2	0.086 7	0.024 2
AQIM	0.023 4	0.069 1	0.004 7
STAQIM	0.048 0	0.094 5	0.021 1
RDM	0.021 9	0.064 8	0.012 1
STRDM	0.027 3	0.105 9	0.011 3

Table 2 BERs comparison of four methods with and without spread transform under contrast stretching

Method	Contrast stretching	Method	Contrast stretching
NCDM	0.377 0	AQIM	0.494 1
STNCDM	0.002 7	STAQIM	0
Zareian	0.485 2	RDM	0.512 9
STZareian	0.037 5	STRDM	0

Table 3 Comparing BER of the proposed method and HRDM under different types of attacks

Method	VSA (ρ)		Constant (c)		Gamma (γ)		JPEG (QF)		AWGN (σ_n)		Avg.	Med.	Wien.	Cont.
	0.7	1.1	−30	30	0.9	1.1	30	50	10	20	3×3	3×3	3×3	
STNCDM	**0**	0.003 9	0.028 5	0.008 6	0.013 7	0.012 9	**0.012 5**	**0.002 3**	**0.031 6**	**0.139 8**	0.031 6	**0.057 4**	**0.011 3**	0.002 7
STZareian	0.005 1	0.016 8	0.097 7	0.052 3	0.124 6	0.121 1	0.069 1	0.020 7	0.102 7	0.275 4	0.049 2	0.086 7	0.024 2	0.037 5
STAQIM	**0**	0.000 4	**0.021 9**	**0.001 6**	0.1246	0.097 7	0.198 0	0.0266	0.246 5	0.482 4	0.048 0	0.094 5	0.021 1	**0**
STRDM	**0**	**0**	0.043 4	0.002 7	0.213 7	0.200 0	0.548 0	0.012 9	0.398 0	0.488 3	**0.027 3**	0.105 9	**0.011 3**	**0**
HRDM	0.002 0	0.002 7	0.479 3	0.453 5	**0.009 0**	**0.009 0**	0.435 5	0.107 4	0.380 9	0.491 0	0.066 4	0.126 6	0.047 7	0.460 9

Table 4 Comparing BER of the two invariant domain construction methods under different types of attacks

Method	VSA (ρ)		Constant (c)		Gamma (γ)		JPEG (QF)		AWGN (σ_n)		Avg.	Med.	Wien.	Cont.
	0.7	1.1	−30	30	0.9	1.1	30	50	10	20	3×3	3×3	3×3	
STNCDM1	0	0.003 9	0.028 5	0.008 6	0.013 7	0.012 9	0.012	0.002 3	0.031 6	0.139 8	0.031 6	0.057 4	0.011 3	0.002 7
STNCDM2	0.000 4	0.003 1	0.034 0	0.010 2	0.023 8	0.021 1	0.025 8	0.004 3	0.041 0	0.175 4	0.042 6	0.062 1	0.015 2	0.009 0
STZareian1	0.005 1	0.016 8	0.097 7	0.052 3	0.124 6	0.121 1	0.069 1	0.020 7	0.102 7	0.275 4	0.049 2	0.086 7	0.024 2	0.037 5
STZareian2	0.004 3	0.018 4	0.103 1	0.048 8	0.186 7	0.164 1	0.106 3	0.027 0	0.161 7	0.419 1	0.068 0	0.122 7	0.027 3	0.032 4
STAQIM1	0	0.000 4	0.021 9	0.001 6	0.124 6	0.097 7	0.198 0	0.026 6	0.246 5	0.482 4	0.048 0	0.094 5	0.021 1	0
STAQIM2	0.003 1	0.005 5	0.019 1	0.005 5	0.049 6	0.042 6	0.121 9	0.028 5	0.1723	0.430 5	0.048 8	0.096 5	0.022 7	0.007 4
STRDM1	0	0	0.043 4	0.002 7	0.213 7	0.200 0	0.548 0	0.012 9	0.398 0	0.488 3	0.027 3	0.105 9	0.011 3	0
STRDM2	0	0	0.07 9	0.000 4	0.078 9	0.077 0	0.112 9	0.001 2	0.237 1	0.471 5	0.021 5	0.084 8	0.003 1	0

7) Robustness against contrast stretching: Contrast stretching is one kind of nonlinear valumetric distortions. We also test this attack on the watermarked images, and the results are quite impressive, as shown in Table 2. The original four methods are very sensitive to this attack, but this problem can be solved with spread transform. For example, the BER of RDM under this attack is decreased from 0.5129 to 0 by use of spread transform.

6.2.3 Comparison with HRDM[21]

Pietro presented a hyperbolic rational dither modulation data hiding scheme which provides robustness against nonlinear distortions modeled by a power-law attack[21], and we denote this scheme as HRDM. In HRDM, a proper mapping of the pixel values from the Cartesian to hyperbolic coordinates is used to transform the exponentiation of a nonlinear distortion into a gain scale, then watermark is embedded using RDM. The main idea of HRDM is very similar to our proposed method, besides HRDM is the state-of-the-art method to cope with nonlinear distortions. Hence, we compare our method with HRDM. In experiments, we also embed 256 bits information in each image and adjust parameters so that the PSNR value of each image is 48 dB, and we average BERs of the test images to obtain the final results.

Table 3 shows the comparison of the proposed method and HRDM. It can be seen that HRDM has superior robustness against Gamma correction compared to our method, but it is very sensitive to constant change attack, while our method is very robust to such attacks. For example, when the constant change value c is 30, the BERs of HRDM and SRDM are 0.453 5 and 0.002 7 respectively, while the BERs of HRDM and SRDM are 0.009 and 0.2 respectively, when the Gamma factor γ is 1.1. The reason is that HRDM constructs a domain which is invariant to Gamma nonlinear distortion and SRDM constructs a domain which is invariant to constant change distortion. But our method can improve the robustness against nonlinear distortion, while HRDM cannot solve the problem of constant change attack. In addition, the proposed method also has better robustness against lossy JPEG compression, Gaussian noise addition, contrast stretching and image filtering attacks, especially for the low quality JPEG compression and contrast stretching attacks. Overall, the proposed watermarking method has superior performance than HRDM.

6.2.4 Comparison with previous method[22]

In this part, we compare the results of the two different construction methods of the invariant domain. For fair comparison, the same 256 bits information is embedded in the two methods. To this aim, the length of the spread vector of the new construction method is 12, while the length of the previous construction method is 2. In embedding process, the vector dimensionality L of SNCDM and SZareian in the new construction method is set to 16, while L in the previous method is set to 8. Watermark is embedded for 16 and 8 times respectively in SRDM and SAQIM in the new construction method, while watermark is embedded for 8 and 4 times respectively in the previous method. The mean PSNR values of the test images are about 48 dB. The final results are the average BERs of the test images, which is shown in Table 4, where "1" denotes the new construction method and "2" denotes the previous method. It can be seen that the performance of the two methods under the attacks is very similar. But, as stated in Section 4.3, this new construction method has larger embedding capacity than our previous method.

6.3 Performance analysis

As mentioned above, the proposed watermarking method is invariant to both constant change and amplitude scale distortion. For the nonlinear valumetric distortion, Gamma correction is very typical. Suppose a signal sample x is corrected by a Gamma factor γ, it will be changed to x^γ. The difference of them is $d(x) = x^\gamma - x$, which can be represented by the Taylor expansion at value a as follows:

$$d(x) = d(a) + d^{'}(a)(x-a) + R_1(x) = (1-\gamma)a^\gamma + (\gamma a^{\gamma-1} - 1)x + R_1(x). \quad (27)$$

where $R_1(x)$ is the remainder of the Taylor expansion. It can be seen that $d(x)$ is composed of three parts: the first part is a constant value $(1-\gamma)a^\gamma$, the second part is $(\gamma a^{\gamma-1} - 1)x$ which can be viewed as an amplitude scale version of x, and the third part is the remainder $R_1(x)$ which is a function correlated with x. In other words, Gamma correction can be seen as a combination of three kinds of distortions: constant change distortion, amplitude scale attack and random amplitude distortion. As our method is invariant to the first two kinds of attacks, hence the robustness of the watermarking methods to Gamma correction can be improved.

6.4 Discussion

From the experimental results, we can see that the four methods (STNCDM, STZareian, STAQIM, STRDM) show different robustness under the experimental sets of this paper. Under constant change and valumetric scale attacks, the four methods have similar robustness, as shown in Figs. 10 and 12. For the Gamma correction distortion, AWGN noise addition and JPEG compression attacks, the four methods are sorted in descending order as STNCDM, STZareian, STAQIM and STRDM, according to robustness. Especially for the Gamma correction distortion, STNCDM has obvious advantages. For image filtering attacks, STNCDM also has the best performance and STZareian has the worst robustness, while STAQIM and STRDM have similar robustness. Under the contrast stretching attack, STAQIM and STRDM have the best performance and STZareian has the worst robustness. Overall, STNCDM has the best robustness and STRDM has the worst performance among the four methods, and the four methods can be sorted in descending order as STNCDM, STZareian, STAQIM and STRDM, according to robustness under the experimental set of this paper. However, in the term of embedding capacity of the watermarking meth-

ods, STRDM has the largest embedding capacity, which is 2 times of STAQIM, and 16 times of STNCDM and STZareian.

Geometric distortion is a common attack and is very challenging in watermarking systems. To resist geometric distortion, our scheme can be combined with some existing techniques. For example, before invariant domain in watermark extraction process, geometric invariant domain could be constructed[18] or geometric distortion parameters could be calculated[36, 37] firstly. Then watermark can be extracted correctly under geometric attacks.

7 Conclusions

In this paper, we have presented a simple but effective watermarking method to resist linear and nonlinear valumetric distortions. We first construct an invariant domain by spread transform that satisfies certain constraint. Then an amplitude scale invariant watermarking method is applied to embed watermark on the domain. Four different watermarking schemes and a nonlinear invariant watermarking method are implemented for comparison. In experiments, several attacks are tested to evaluate the effectiveness of our method, including valumetric distortion attacks and common image processing attacks. Experimental results demonstrate that: 1) our approach can solve the drawback of the compared methods which are very sensitive to constant change attack; 2) our method has better performance than the compared watermarking methods to resist nonlinear valumetric distortions, such as Gamma correction and contrast stretching; 3) our method has very small influence on the robustness of original methods and even obtain better performance in some cases to resist common image processing attacks. In the future work, methods that are robust to nonlinear valumetric distortions with combination of our proposed scheme and some existing techniques to resist geometric attacks may be considered.

References

[1] I. J. Cox, J. Kilian, F. Leighton, T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[2] C. Podilchuk, W. J. Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, 1998.

[3] B. Chen, G. W. Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[4] P. Moulin, R. Koetter. Data-hiding codes. *Proceedings of the IEEE*, vol. 93, no. 12, pp. 2083–2126, 2005.

[5] J. J. K. O. Ruanaidh, T. Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, vol. 66, no. 3, pp. 303–317, 1998.

[6] H. S. Malvar, D. A. F. Florencio. Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.

[7] M. Barni, F. Bartolini, A. De Rosa, A. Piva. Optimum decoding and detection of multiplicative watermarks. *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1118–1123, 2003.

[8] W. Liu, L. N. Dong, W. J. Zeng. Optimum detection for spread-spectrum watermarking that employs self-masking. *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 645–654, 2007.

[9] J. J. Eggers, R. Bauml, R. Tzschoppe, B. Girod. Scalar costa scheme for information embedding. *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[10] F. Perez-Gonzalez, F. Balado, J. R. H. Martin. Performance analysis of existing and new methods for data hiding with known-host information in additive channels. *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 960–980, 2003.

[11] F. Bartolini, M. Barni, A. Piva. Performance analysis of stdm watermarking in presence of nonadditive attacks. *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2965–2974, 2004.

[12] R. S. Run, S. J. Horng, J. L. Lai, T. W. Kao, R. J. Chen. An improved SVD-based watermarking technique for copyright protection. *Expert Systems with Applications*, vol. 39, no. 1, pp. 673–689, 2012.

[13] D. Rosiyadi, S. J. Horng, P. Z. Fan, X. Wang, M. K. Khan, Y. Pan. Copyright protection for e-government document images. *IEEE MultiMedia*, vol. 19, no. 3, pp. 62–73, 2012.

[14] S. J. Horng, D. Rosiyadi, T. R. Li, T. Takao, M. Y. Guo, M. K. Khan. A blind image copyright protection scheme for e-government. *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, pp. 1099–1105, 2013.

[15] S. J. Horng, D. Rosiyadi, P. Z. Fan, X. Wang, M. K. Khan. An adaptive watermarking scheme for e-government document images. *Multimedia Tools and Applications*, vol. 72, no. 3, pp. 3085–3103, 2014.

[16] M. E. Farfoura, S. J. Horng, J. L. Lai, R. S. Run, R. J. Chen, M. K. Khan. A blind reversible method for watermarking relational databases based on a time-stamping protocol. *Expert Systems with Applications*, vol. 39, no. 3, pp. 3185–3196, 2012.

[17] S. J. Horng, M. E. Farfoura, P. Z. Fan, X. Wang, T. R. Li, J. M. Guo. A low cost fragile watermarking scheme in H.264/AVC compressed domain. *Multimedia Tools and Applications*, vol. 72, no. 3, pp. 2469–2495, 2014.

[18] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Y. Yang, F. Davoine. Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2140–2150, 2005.

[19] S. Pereira, T. Pun. Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*, vol. 9, no. 6, pp. 1123–1129, 2000.

[20] M. A. Akhaee, S. M. E. Sahraeian, C. Jin. Blind image watermarking using a sample projection approach. *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 883–893, 2011.

[21] P. Guccione, M. Scagliola. Hyperbolic rdm for nonlinear valumetric distortions. *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 25–35, 2009.

[22] Z. R. Wang, J. Dong, W. Wang, T. N. Tan. An effective watermarking method against valumetric distortions. In *Proceedings of IEEE International Conference on Image Processing*, IEEE, Paris, France, pp. 5487–5491, 2014.

[23] F. Perez-Gonzalez, C. Mosquera, M. Barni, A. Abrardo. Rational dither modulation: A high-rate data-hiding method invariant to gain attacks. *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3960–3975, 2005.

[24] F. Ourique, V. Licks, R. Jordan, F. Perez-Gonzalez. Angle QIM: A novel watermark embedding scheme robust against amplitude scaling distortions. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, IEEE, Philadelphia, USA, vol. 2, pp. 797–800, 2005.

[25] M. Zareian, H. R. Tohidypour, Z. J. Wang. A novel quantization-based watermarking approach invariant to gain attack. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE, Vancouver, Canada, pp. 2945–2948, 2013.

[26] X. S. Zhu, S. L. Peng. A novel quantization watermarking scheme by modulating the normalized correlation. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE, Kyoto, Japan, pp. 1765–1768, 2012.

[27] J. J. Eggers, R. Bäuml, B. Girod. Estimation of amplitude modifications before scs watermark detection. In *Proceedings of SPIE Security and Watermarking of Multimedia Contents IV*, SPIE, San Jose, USA, vol. 4675, pp. 387–398, 2002.

[28] I. D. Shterev, R. L. Lagendijk, R. Heusdens. Statistical amplitude scale estimation for quantization-based watermarking. In *Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents VI*, SPIE, San Jose, USA, vol. 5306, pp. 796–804, 2004.

[29] I. D. Shterev, R. L. Lagendijk. Amplitude scale estimation for quantization-based watermarking. *IEEE Transactions on Signal Processing*, vol. 54, no. 11, pp. 4146–4155, 2006.

[30] M. L. Miller, G. J. Dorr, I. J. Cox. Dirty-paper trellis codes for watermarking. In *Proceedings of International Conference on Image Processing*, IEEE, Rochester, USA, vol. 2, pp. 129–132, 2002.

[31] Q. Li, I. J. Cox. Rational dither modulation watermarking using a perceptual model. In *Proceedings of IEEE the 7th Workshop on Multimedia Signal Processing*, IEEE, Shanghai, China, pp. 1–4, 2005.

[32] P. Bas. A quantization watermarking technique robust to linear and non-linear valumetric distortions using a fractal set of floating quantizers. In *Proceedings of International Conference on Information Hiding*, Barcelona, Spain, vol. 3727, pp. 106–117, 2005.

[33] X. S. Zhu, J. Ding, H. H. Dong, K. F. Hu, X. B. Zhang. Normalized correlation-based quantization modulation for robust watermarking. *IEEE Transactions on Multimedia*, vol. 16, no. 7, pp. 1888–1904, 2014.

[34] M. Zareian, H. R. Tohidypour. A novel gain invariant quantization-based watermarking approach. *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1804–1813, 2014.

[35] F. Guerrini, R. Leonardi, M. Barni. Image watermarking robust against non-linear value-metric scaling based on higher order statistics. In *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE, Toulouse, France, vol. 5, pp. V–V, 2006.

[36] V. Q. Pham, T. Miyaki, T. Yamasaki, K. Aizawa. Geometrically invariant object-based watermarking using sift feature. In *Proceedings of IEEE International Conference on Image Processing*, IEEE, San Antonio, USA, vol. 5, pp. 473–476, 2007.

[37] Y. T. Lin, C. Y. Huang, G. Lee. Rotation, scaling, and translation resilient watermarking for images. *IET Image Processing*, vol. 5, no. 4, pp. 328–340, 2011.

Zai-Ran Wang received the B. Eng. degree in computer science and technology from the College of Information Science and Engineering, Shandong Normal University, China in 2009. He is currently Ph. D. candidate in the College of Engineering & Information Technology, University of Chinese Academy of Sciences, China.

His research interests include digital watermarking, image processing and pattern recognition.

E-mail: wzr1201@163.com

ORCID iD: 0000-0002-8483-7742

Jing Dong received the B. Sc. degree in electronic information science and technology from Central South University, China in 2005, and the Ph. D. degree in pattern recognition from the Institute of Automation, Chinese Academy of Sciences, China. Since 2010, she has been with the National Laboratory of Pattern Recognition,Institute of Automation, Chinese Academy of Sciences, China, where she is currently an assistant professor. She is a member of the IEEE Computer Science Society, the Signal Society, and the IEEE Communication Society.

Her research interests include pattern recognition, image processing, and digital image forensics, including watermarking, steganalysis, and tampering detection.

E-mail: jdong@nlpr.ia.ac.cn (Corresponding author)
ORCID iD: 0000-0002-2763-7832

Wei Wang received the B. Eng. degree in computer science and technology from North China Electric Power University, China in 2007. Since 2012, he has been with the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, China, where he is currently an assistant professor.

His research interests include pattern recognition, image processing, and digital image forensics, including watermarking, steganalysis, and tampering detection.

E-mail: wwang@nlpr.ia.ac.cn