AN EFFECTIVE WATERMARKING METHOD AGAINST VALUMETRIC DISTORTIONS

Zairan Wang[1,2]*, Jing Dong*[1]*, Wei Wang*[1] *and Tieniu Tan*[1]

[1]Center for Research on Intelligent Perception and Computing,
National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences.
[2]College of Engineering and Information Technology, University of Chinese Academy of Sciences.

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 as amplitude scaling, and fail in other kinds of valumetric distortions like constant change attack or gamma correction. In this paper, we propose a very simple method to tackle all the three kinds of valumetric distortions. A constant change invariant domain is first constructed by spread transform, in which the watermark is embedded using a certain amplitude scaling invariant based watermarking scheme. Several typical watermarking methods and attacks have been implemented in our experiments to demonstrate the effectiveness of the proposed method.

Index Terms— QIM, watermarking, valumetric distortions, amplitude scaling

1. INTRODUCTION

Digital watermarking has always drawn extensive attention for digital copyright protection since it was born. So far, many watermarking schemes have been proposed in the literature. The class of Quantization Index Modulation (QIM) algorithms [1] is one of the most popular watermarking schemes because of its robustness to the AWGN (Additive White Gaussian Noise) channel and high capacity. 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) [2]. These kinds of distortions are rather common in audio or video processing. For instance, non-linear valumetric correction is used for better CRT display or the contrast of an image may be adjusted to improve the visual effect. Valumetric distortions usually have small impact on the quality of the attacked media, but they can dramatically degrade the performance of quantization based watermarking schemes because of the mismatch of quantization step between the encoder and decoder. Hence, researching watermarking methods which can be robust to valumetric distortions has great significance.

In general, valumetric distortions can be classified into linear valumetric distortions and non-linear valumetric distortions. Linear valumetric distortions include amplitude scaling and constant change distortion. A typical example of non-linear valumetric distortion is gamma-correction. Let $\mathbf{x} = \{x_1, x_2...x_n\}$ be the host signal vector in which we wish to embed watermark and $\mathbf{y} = \{y_1, y_2...y_n\}$ be the corresponding watermarked signal vector. Amplitude scaling attack means that $\mathbf{y}$ is scaled by a factor ρ, i.e., $\mathbf{z} = \rho \cdot \mathbf{y}$, and $\mathbf{z}$ is the attacked version of $\mathbf{y}$. Constant change distortion means that a constant change value c is added on $\mathbf{y}$, i.e., $\mathbf{z} = \mathbf{y} + c$. In the last few years, a lot of quantization based watermarking schemes have been proposed to deal with this problem [2, 3, 4, 5, 6, 7, 8], but these methods can only tackle the amplitude scaling attack. In [9], Pietro et al. made use of proper mapping of the pixel values from the Cartesian to hyperbolic coordinates to solve the amplitude scaling and non-linear valumetric distortion, but this method ignores the constant change attack. In this paper, we propose a solution to consider all the three attacks. Our approach is that: a constant change invariant domain is first constructed by spread transform, in which an amplitude scaling invariant watermarking scheme is applied to obtain both amplitude scaling and constant change invariant properties. Several typical amplitude scaling invariant watermarking schemes are implemented in our experiments. Experimental results demonstrate that our method not only solves their drawbacks of sensitivity to constant change attack, but also has better performance to resist non-linear valumetric distortion. 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. Section 2 gives an overview of related work. Section 3 presents our watermarking method. Then, experimental results are shown in Section 4. Conclusions are given in Section 5.

2. RELATED WORK

There has been a wide research on the watermarking schemes robust to valumetric distortions. Amplitude scaling invariant

watermarking schemes have attracted many attentions, which can be divided into four categories as follows.

1) Estimating amplitude scaling parameter: Egger [10] embedded an auxiliary pilot signal to be used by the decoder to estimate the amplitude scaling parameter. The disadvantage of this scheme is that it reduces the embedding capacity and decreases the algorithm security [2]. Shterev [4] 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: In [11], Miller embedded watermark by using the lattice codes, which is inherently robust to amplitude scaling. This scheme also has high computational complexity.

3) Adaptive quantization step: Fernando proposed the rational dither modulation (RDM) watermarking method, where an amplitude scaling invariant adaptive quantization step size at both embedder and decoder was used. Li et al. [12] proposed an improved version of the RDM.

4) Constructing amplitude scaling invariant features: In the angle QIM (AQIM) [6], the angle of a vector of image samples was quantized. In the recent two years, Zhu [7] embedded watermark by quantizing the normalized cross correlation between the host signal vector and a random vector. In [8], the ratio of the root mean square of two host signal vectors was constructed to embed watermark.

As we have mentioned above, most of the amplitude scaling invariant watermarking methods ignore constant change attack and non-linear valumetric distortions, so we propose a method against all the three kinds of distortions in this paper.

3. PROPOSED METHOD

As stated earlier, our approach is a projection based method that satisfies certain constraint. A constant change invariant domain is constructed to embed watermark in our approach. This can be seen as a preprocessing before watermark embedding. Let $\mathbf{x} \in \Re^L$ be a vector extracted from host signal samples and $\mathbf{u} \in \Re^L$ be a spread vector which is randomly obtained by a key k_v. The key idea is to project $\mathbf{x}$ onto $\mathbf{u}$ to obtain a domain which is intrinsically invariant to constant change distortion. The projection of $\mathbf{x}$ onto $\mathbf{u}$ is defined as:

$$f_x = \mathbf{x}^T\mathbf{u} = \sum_{i=1}^{L} x_i u_i. \tag{1}$$

When a constant change value c is added on $\mathbf{x}$, f_x is changed to $f_x^{'}$:

$$f_x^{'} = (\mathbf{x}+c)^T\mathbf{u} = \sum_{i=1}^{L} x_i u_i + c\sum_{i=1}^{L} u_i. \tag{2}$$

Our aim is to eliminate the effect of the constant change value c. In other words, $f_x^{'}$ should be equal to f_x after c is added on $\mathbf{x}$. Combined with Equation 1 and Equation 2, we notice that if $f_x^{'}$ is equal to f_x, the sum of the elements of the spread vector $\mathbf{u}$ must be zero. Hence, in order to construct a constant change invariant domain, the spread vector $\mathbf{u}$ must satisfy the following constraint:

$$\sum_{i=1}^{L} u_i = 0. \tag{3}$$

In addition to the constant change invariant property, the projection also holds the property of multiplication as illustrated by the following equations:

$$f_x^{'} = (\rho\cdot\mathbf{x})^T\mathbf{u} = \rho\cdot\sum_{i=1}^{L} x_i u_i = \rho\cdot f_x, \tag{4}$$

which means that if the vector $\mathbf{x}$ is scaled by ρ the projection f_x will also be scaled by ρ. As amplitude scaling invariant watermarking schemes, such as RDM, AQIM and NCDM, are invariant to this kind of amplitude change, therefore when such a watermarking scheme is applied on the constructed constant change invariant domain, both constant change and amplitude scaling invariant properties can be obtained.

For gamma correction, 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:

$$\begin{aligned} d(x) &= d(a) + d^{'}(a)(x-a) + R_1(x) \\ &= (1-\gamma)a^\gamma + (\gamma a^{\gamma-1}-1)x + R_1(x). \end{aligned} \tag{5}$$

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 scaling 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 scaling attack and random amplitude distortion. As our method is invariant to the first two kinds of attacks, hence the performance of the watermarking methods to resist gamma correction can be improved.

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

1. Host signal vector $\mathbf{x}$ is first projected on a spread vector $\mathbf{u}$, which satisfies certain constraint. Then a constant change invariant domain f_x is obtained.
2. Watermark m is embedded by an amplitude scaling invariant watermarking scheme on f_x, such as RDM, AQIM, NCDM or Zareian's method. Then f_x is changed to $f_x^{'}$.
3. The watermarked vector $\mathbf{y}$ is constructed according to $f_x^{'}$.
4. In the transmission process, $\mathbf{y}$ may be attacked by pirates and changed to $\mathbf{z}$. Before watermark decoding, the receiver performs the projection using the same vector $\mathbf{u}$ to recover the hidden information $m^{'}$.

To describe how the watermarked vector $\mathbf{y}$ is constructed, we let $f_x^{'} = \mathbf{y}^T\mathbf{u}$. Combined with Equation 1, we can easily get the following equation:

$$(\frac{f_x^{'}}{f_x}\mathbf{x} - \mathbf{y})^T\mathbf{u} = 0. \quad (6)$$

Denote $\mathbf{v}$ as $\frac{f_x^{'}}{f_x}\mathbf{x} - \mathbf{y}$, hence vector $\mathbf{v}$ and $\mathbf{u}$ are orthogonal with each other. Here we let $\mathbf{v}$ be a zero vector for simplicity, therefore $\mathbf{y}$ is obtained by:

$$\mathbf{y} = \frac{f_x^{'}}{f_x}\mathbf{x}. \quad (7)$$

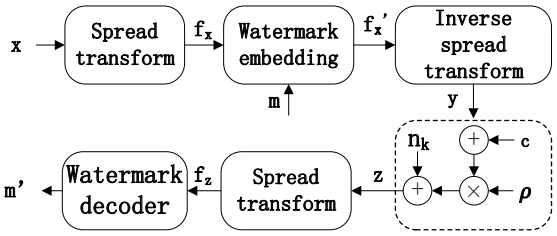

Fig. 1. Flowchart of our approach.

4. EXPERIMENTAL RESULTS

In this section, some experimental results will be shown to demonstrate the effectiveness of our method. Four different QIM based techniques, RDM, AQIM, NCDM and Zareian's method, are implemented. RDM and AQIM are two typical QIM based techniques which are invariant to amplitude scaling distortion, and NCDM and Zareian's method are proposed in the recent two years. We collect 100 test images with size of 512×512 in gray-scale. Fig. 2 shows ten typical test images of them. All the methods are applied on the approximate sub-band with three level wavelet decomposition. PSNR values of all the watermarked test images are set to 42dB. Vector length L is set to 2 and the watermark capacity is 256 bits. For fair comparison, the 256 bits watermark is embedded repeatedly for the four original watermarking methods. To reduce correlations between image blocks, we pseudo-randomly select low frequency coefficients to construct the sample vector.

Fig. 2. Ten test samples of size 512×512.

To evaluate the effectiveness of our method, several attacks are implemented, such as constant change attack, gamma correction, amplitude scaling, JPEG compression and Gaussian noise addition. All the results are obtained by the mean of the results of 100 test images.

Fig. 3 shows BERs of different methods against constant change attack. The dashed lines indicate BERs of four original methods, and the corresponding solid lines represent BERs of the four methods applied on our constant change invariant domain. It can be seen that with our approach, the BERs of the four methods are significantly decreased as expected.

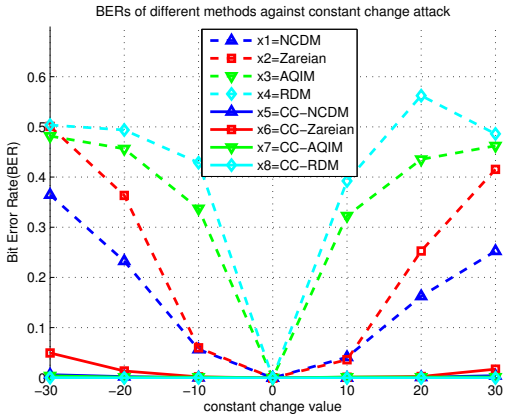

Fig. 3. BERs comparison of four methods with and without our approach under constant change attack.

Gamma correction is the non-linear valumetric distortion. Fig. 4 shows the BERs against gamma correction. We can notice that BERs of the four methods are decreased with different levels as we have analyzed in Section 3.

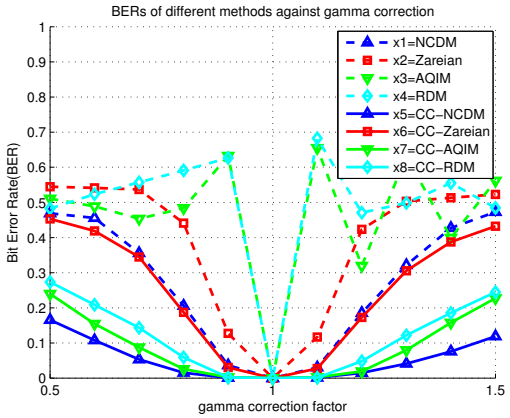

Fig. 4. BERs comparison of four methods with and without our approach under gamma correction.

The four test methods are all intrinsically invariant to amplitude scaling attack. We also test the effect of our method under this kind of distortions. The comparison results are depicted in Fig. 5. Experimental results show that our approach has very small influence on the performance of the original methods to against amplitude scaling attack.

Lossy JPEG compression with different quality factors is tested in our experiments, as exhibited in Fig. 6. Experimental results reveal that our method has little effect on the robustness of the original methods against JPEG compression.

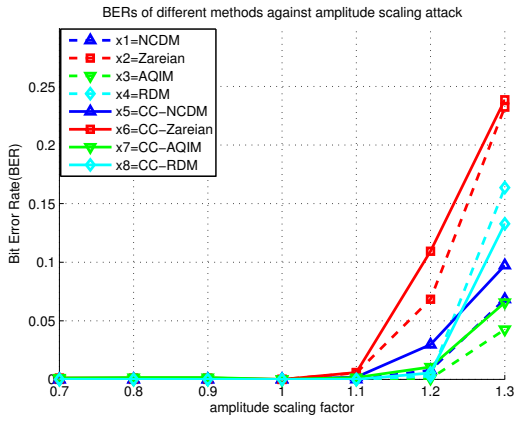

Fig. 5. BERs comparison of four methods with and without our approach under amplitude scaling attack.

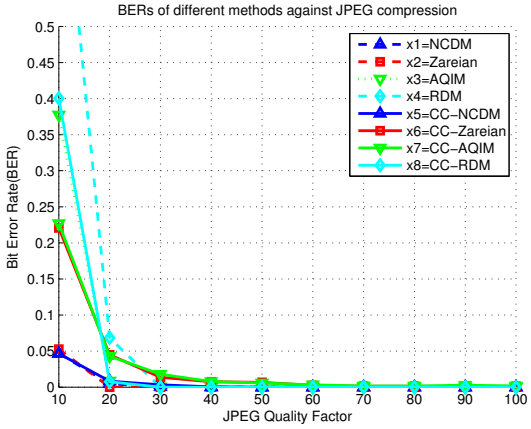

Fig. 6. BERs comparison of four methods with and without our approach under JPEG compression.

Finally we have compared the results under the addition of white Gaussian noise. The watermarked images are distorted by AWGN with standard deviation from 10 to 60 (in the range of $[0, 255]$). The results are illustrated in Fig. 7. We can see that all the methods can get better results in our framework except Zareian's method. This may be benefited from the use of spread transform in our method.

At last, we investigate the effect of the spread vector length and watermark capacity on the performance of the watermarking schemes. Without loss of generality, we take NCDM watermarking method as an example, and the results are depicted in Table 1. The vector length L varies from 2 to 4 and watermark capacity C changes from 256 to 128. Experimental results show that L has small influence on the performance of the watermarking method. But the longer the length of spread vector, the smaller the size of the invariant domain we construct, then the smaller of the watermark capacity. Hence, In practical applications we set $L = 2$.

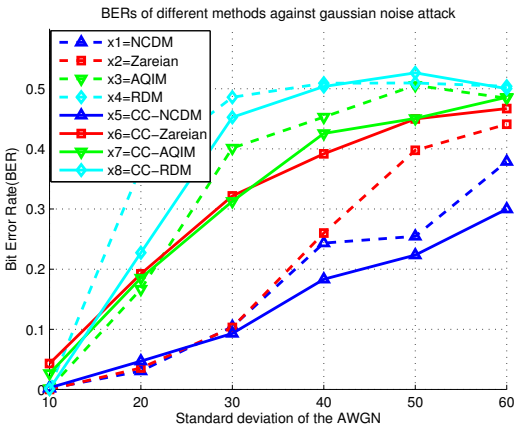

Fig. 7. BERs comparison of four methods with and without our approach under gaussian noise addition.

Table 1. BERs under different vector length and watermark capacity

Attacks/BER	$L = 2$ C=256	$L = 3$ C=170	$L = 4$ C=128
Constant change($C = -30$)	0.0020	0.0024	0.0016
Constant change($C = 30$)	0.0012	0	0
Amplitude scaling($\rho = 0.7$)	0.0012	0.0018	0.0016
Amplitude scaling($\rho = 1.3$)	0.0934	0.0988	0.0813
Gamma correction($\gamma = 0.7$)	0.0531	0.0541	0.0352
Gamma correction($\gamma = 1.3$)	0.0410	0.0453	0.0273
Gaussian noise($\sigma = 30$)	0.0930	0.1288	0.0516
JPEG compression($Q = 20$)	0.0082	0.0059	0.0039

5. CONCLUSIONS

In this paper, we have presented a simple but effective watermarking method to resist constant change and non-linear valumetric distortions. To this aim, we first construct a constant change invariant domain by spread transform that satisfies certain constraint. Then an amplitude scaling invariant watermarking method is used to embed watermark on the domain. Four different watermarking schemes and several attacks are implemented 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 watermarking methods which is very sensitive to constant change attack; 2) Our method has better performance than the compared watermarking methods to resist gamma correction; 3) Our method has very small influence on the robustness of original methods and even get better performance in some cases to resist common image processing attacks.

Acknowledgments

The work presented in this paper was supported by Nature Science Foundation of China (Grant No.61303262) and National Key Technology R&D Program (Grant No.2012BAH-04F02).

6. REFERENCES

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

[2] Mohammad Ali Akhaee, Sayed Mohammad Ebrahim Sahraeian, and Craig Jin, "Blind image watermarking using a sample projection approach," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 883–893, 2011.

[3] Ivo D Shterev, Reginald L Lagendijk, and Richard Heusdens, "Statistical amplitude scale estimation for quantization-based watermarking," in *Proceedings of SPIE*, 2004, vol. 5306, pp. 796–804.

[4] Ivo D Shterev and Reginald L Lagendijk, "Amplitude scale estimation for quantization-based watermarking," *Signal Processing, IEEE Transactions on*, vol. 54, no. 11, pp. 4146–4155, 2006.

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

[6] F. Ourique, V. Licks, R. Jordan, and F. Perez-Gonzalez, "Angle qim: a novel watermark embedding scheme robust against amplitude scaling distortions," in *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on*, march 2005, vol. 2, pp. ii/797 – ii/800 Vol. 2.

[7] Xinshan Zhu and Shuoling Peng, "A novel quantization watermarking scheme by modulating the normalized correlation," in *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*. IEEE, 2012, pp. 1765–1768.

[8] Mohsen Zareian, Hamid Reza Tohidypour, and Z Jane Wang, "A novel quantization-based watermarking approach invariant to gain attack," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*. IEEE, 2013, pp. 2945–2948.

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

[10] Joachim J Eggers, Robert Baeuml, and Bernd Girod, "Estimation of amplitude modifications before scs watermark detection," in *Electronic Imaging 2002*. International Society for Optics and Photonics, 2002, pp. 387–398.

[11] Matthew L Miller, GJ Dorr, and Ingemar J Cox, "Dirty-paper trellis codes for watermarking," in *Image Processing. 2002. Proceedings. 2002 International Conference on*. IEEE, 2002, vol. 2, pp. II–129.

[12] Qiao Li and Ingemar J Cox, "Rational dither modulation watermarking using a perceptual model," in *in Proc. IEEE Workshop on Multimedia Signal Processing, MMSP05*. Citeseer, 2005.