An improved sample projection approach for image watermarking

Yuan-Gen Wang\(^{a,c}\), Guopu Zhu\(^{b}\), Jiwu Huang\(^{a,*}\)

\(^{a}\) School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
\(^{b}\) Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China
\(^{c}\) School of Information, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China

ARTICLE INFO

Article history:
Available online 23 September 2013

Abstract

Very recently, a novel watermarking scheme named sample projection approach (SPA) has been proposed by Akhaee et al.\(^{[1]}\) to improve the watermarking performance against gain attacks. The SPA embeds one message symbol into four signal samples by projecting the line segment formed by the four samples on a certain specific codeline. Based on the SPA, this paper presents an improved sample projection approach (ISPA) by introducing a set of modified codelines to decrease embedding distortion and constructing the long line segments to increase robustness. According to our theoretical analysis of document-to-watermark ratio (DWR), the modified codelines result in a lower embedding distortion than the SPA’s codelines in the same conditions with regard to payload and robustness. We also derive a theoretical expression for the symbol error rate (SER) of the ISPA against additive white Gaussian noise (AWGN) attack. The numerous experiments conducted on both artificial Gaussian signals and the natural images show that the proposed ISPA outperforms the SPA in terms of robustness against attacks.

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

Digital watermarking is seen as a solution to copyright protection by embedding identification information permanently into digital media\(^{[2]}\). Generally, a good watermarking scheme should first be able to resist various unintentional attacks\(^{[3,4]}\). Thus robustness is the key issue for watermarking technique to protect copyrights. The two kinds of watermarking schemes, namely, the spread-spectrum (SS) watermarking\(^{[5]}\) and the quantization index modulation (QIM) watermarking\(^{[6,7]}\), have been most widely studied regarding embedding distortion, payload, and robustness\(^{[8,9]}\). Compared with the SS method, the QIM method can achieve better rate-distortion-robustness trade-offs. However, the basic QIM algorithm is fragile to gain attacks (i.e., valumetric distortion), such as amplitude scaling and gamma compensation. So far, in the framework of QIM watermarking, three types of solutions have been proposed to deal with the valumetric distortion. The first solution is to insert a pilot sequence into the watermarked signal, and the pilot sequence is shared by the encoder and the decoder\(^{[10]}\). The second one is to design the direction-based embedding schemes, such as the angle QIM (AQIM)\(^{[11]}\) as well as the absolute AQIM (AAQIM)\(^{[12]}\). And the last one is to introduce a robust embedding domain being invariant to the gain attacks\(^{[13,14]}\). However, the first solution is very vulnerable to malicious attacks, since the adversaries could easily detect the deterministic pilot sequence and further tamper with it. The AQIM and the AAQIM achieve relatively low robustness against additive white Gaussian noise (AWGN) attack. The problems brought by the works\(^{[13,14]}\) are the high peak-to-average power ratio due to their momentarily large quantization step and the high computational complexity. In order to resist the gain attacks, Akhaee et al.\(^{[1]}\) proposed a novel watermarking scheme called as sample projection approach (SPA), which is essentially invariant to the gain attacks, meanwhile can obtain lower embedding distortion than the AQIM. But, the SPA still has two main weaknesses: 1) the codelines designed for the SPA are an ineffective coding scheme in terms of embedding distortion; 2) the selected embedding domain is not robust to various attacks. In addition, the authors of\(^{[1]}\) have not discussed the document-to-watermark (DWR), which is a fundamental measure for the embedding distortion.

This paper focuses on tackling the above issues. In order to decrease the embedding distortion caused by the messages embedding and increase the robustness of the watermark, we propose an improved sample projection approach (ISPA) for image watermarking by introducing a set of modified codelines and constructing the long line segments. Meanwhile, we give a theoretical DWR analysis for both the SPA’s and the modified codelines. The analytical results show that the modified codelines can obtain the lower embedding distortion than the SPA’s codelines in the same conditions with regard to payload and robustness. The symbol error rate (SER) of the ISPA against AWGN attack is also derived based on the maximum likelihood (ML) decoder. And the extensive experiments tested on both artificial Gaussian signals and the natural...
images show that the proposed ISPA outperforms the SPA in terms of robustness against various attacks.

The remainder of the paper is organized as follows. In Section 2, we briefly introduce the SPA. Then, we propose two strategies to improve the SPA in Section 3. Section 4 provides the performance analysis of both the DWR and the SER under AWGN attack. The remainder of the paper is organized as follows. In Section 2, we briefly introduce the SPA [1]. Let’s consider a special case in the embedding of the SPA. Given a line segment $pq$ with a tiny positive or negative slope (i.e., a tiny angle between the line segment and the $x$-axis), we can see from Fig. 1 that it will result in a relatively large angular distortion if the to-be-embedded message is $M$. This is because the given line segment needs to be rotated by a large angle to the $M$-th codeline, no matter in which quadrant the $M$-th codeline to be projected is.

Fig. 1. Messages embedding of the SPA.

Fig. 2. The modified codelines.

is. Considering that the SPA embeds the $M$-ary message by projecting the line segment on the closest codeline corresponding to the to-be-embedded message, thus, as shown in Fig. 2, if we invert the order of the codelines in the fourth quadrant, then the given line segment will be projected on the $M$-th codeline in the fourth quadrant of Fig. 2. In this case, it is obvious that the angular distortion caused by the embedding is relatively very small. In fact, as analyzed below, the modified codelines shown by Fig. 2 are always superior to the SPA’s codelines with regard to the angular distortion.

Here, we first provide an analysis to compare the maximum angular distortion between the SPA’s and the modified codelines. To simplify the analysis, we set $\alpha = \frac{\pi}{2}$ for the SPA, thus we can obtain $\beta = \frac{\pi}{2M}$. By referring to Fig. 1(b) and Fig. 2, we can find out that the maximum angular distortion of the SPA’s codelines is $\left(\frac{\pi}{2} - \frac{\pi}{2M}\right)$, but that of the modified codelines is only $\frac{\pi}{2}$, which is independent of the number $M$. Table 1 gives the comparison of the maximum angular distortion between the two codelines schemes. We can see from Table 1 that for any $M$, the modified codelines outperform that of the SPA in terms of the maximum angular distortion.

We further qualitatively compare the average angular distortion between the SPA’s and the modified codelines. Without loss of generality, we consider the case of $M = 2$, as shown in Fig. 3. It is reasonable to assume that the angle of the line segment is distributed uniformly over $[0, \frac{\pi}{2}]$. We can see from Fig. 3(a) that for the codelines of the SPA, only the line segment whose angle is in the ranges of $[0, L_2]$ and $[L_2, 2\pi]$, can cause the angular distortion produced by projecting it on the codeline $L_1$, where $L_2$ denotes the angle between the codeline $L_2$ and the $x$-axis. While, as shown in Fig. 3(b) for the modified codelines, only the line segment in the ranges of $[L_2, 0]$ and $[0, L_2]$ can cause the above-described distortion, where $-L_2$ denotes the codeline $L_2$ in the fourth quadrant. It can be easily inferred from Fig. 3 that for both the SPA’s and the modified codelines, the line segment in the range of $[0, L_2]$ causes the same distortion. However, the line segment in the range of $[L_2, \frac{\pi}{2}]$ causes a quite larger distortion than that in the range of $[L_2, 0]$. By the symmetry of the codelines, the analysis on the codeline $L_2$ has the same results. Therefore, based on the above assumption, we can conclude that the average angular distortion of the SPA’s codelines is always larger than that of the modified ones.

We remark that this section aims to propose the modified codelines and also to explain our motivation of the modification by simply analyzing the superiority of the modified codelines over the SPA’s codelines in angular distortion. The derivation of theoretical closed-form expression in terms of DWR, which measures the embedding distortion of host signal, will be given in Section 4.1. In fact, we can see from Fig. 2 that the $M$ codelines of the modified codelines repeat two times over the whole of the first and fourth quadrants. We can further extend the repetition to each quadrant.

\[ L = \text{Line segment projection}\]

\[ \text{Codelines}\]

\[ \text{Fig. 1. Messages embedding of the SPA.}\]

\[ \text{Fig. 2. The modified codelines.}\]
Here we illustrate a simple example in Fig. 4, in which the certain threshold may change to be smaller (larger) than it due to the embedding operation and/or later image distortion. An attempt to solve this kind of asynchronous problem is to employ some extra codes to label the watermarked line segments. And these codes received by the decoder are used for identifying the watermarked line segments during messages extraction. However, this will result in too much side-information. In order to achieve better robustness while avoiding the asynchronous problem, we present a novel strategy for the ISPA to obtain the long line segments, which is described as follows:

(i) Perform 2-D 3-level wavelet decomposition on each non-overlapped block of a gray-scale image;

(ii) Produce a key-dependent uniform random sequence of numbers 0, 1, 2, and 3. And the four numbers 0, 1, 2, and 3 are used to represent four states, respectively. Note that the key that generates the random sequence is shared by both the message embedder and decoder;

(iii) For state 0, extract the pair of samples \( p = [u_1, u_2] \) from LL3 subband, and \( q = [u_3, u_4] \) from HH3 subband; for state 1, extract \( [u_2, u_3] \) from LL3 and \( [u_1, u_4] \) from HH3; for state 2, extract \( [u_1, u_2, u_3] \) from LL3 and \( [u_4] \) from HH3; for state 3, extract \( [u_1, u_2, u_4] \) from LL3 and \( [u_3] \) from HH3. Please note that we select the coefficients as host signal samples from the LL3 and HH3 blocks in raster-scan order;

(iv) Based on the SPA described in Section 2, embed one message into each group of samples \( u = [u_1, u_2, u_3, u_4] \).

3.2. Constructing long line segments

We can see from Fig. 1(a) that the shorter the line segment \( pq \) is, the easier the line segment \( pq \) moves away from its codeline when the watermarked signal is distorted by attacks, thus the less robust the watermark is against noise-interference. Fig. 5 shows the difference in robustness when using the line segments with different lengths to embed the message. It can be observed that there is a significant improvement in robustness when the longest line segments are used for watermarking, especially in the case of weak attacks. For instance, there is a 2 orders of magnitude improvement in the case of WNR = 10 dB. Therefore, in order to improve the robustness of the watermark signal against attacks, we suggest using only the long line segments to embed messages. According to the definition of the length of the line segment \( pq \), which can be expressed by \( \|p - q\|_2 = \sqrt{(u_1 - u_1)^2 + (u_2 - u_2)^2} \), even if all of \( u_1, u_2, u_3, \) and \( u_4 \) take large values, the length of \( pq \) is still small when the values of \( u_1 \) and \( u_2 \) are near to that of \( u_3 \) and \( u_4 \), respectively. In the SPA, the host signal is extracted from the LL subband of the DWT domain of each image block. Although the extracted four samples are large, their values approach the mean length (about 50% proportion), and the use of the samples whose lengths are larger than the mean length (about 50% proportion), respectively.

To illustrate a simple example in Fig. 4, in which the certain threshold may change to be smaller (larger) than it due to the embedding operation and/or later image distortion. An attempt to solve this kind of asynchronous problem is to employ some extra codes to label the watermarked line segments. And these codes received by the decoder are used for identifying the watermarked line segments during messages extraction. However, this will result in too much side-information. In order to achieve better robustness while avoiding the asynchronous problem, we present a novel strategy for the ISPA to obtain the long line segments, which is described as follows:

(i) Perform 2-D 3-level wavelet decomposition on each non-overlapped block of a gray-scale image;

(ii) Produce a key-dependent uniform random sequence of numbers 0, 1, 2, and 3. And the four numbers 0, 1, 2, and 3 are used to represent four states, respectively. Note that the key that generates the random sequence is shared by both the message embedder and decoder;

(iii) For state 0, extract the pair of samples \( p = [u_1, u_2] \) from LL3 subband, and \( q = [u_3, u_4] \) from HH3 subband; for state 1, extract \( [u_2, u_3] \) from LL3 and \( [u_1, u_4] \) from HH3; for state 2, extract \( [u_1, u_2, u_3] \) from LL3 and \( [u_4] \) from HH3; for state 3, extract \( [u_1, u_2, u_4] \) from LL3 and \( [u_3] \) from HH3. Please note that we select the coefficients as host signal samples from the LL3 and HH3 blocks in raster-scan order;

(iv) Based on the SPA described in Section 2, embed one message into each group of samples \( u = [u_1, u_2, u_3, u_4] \).

It is known that the samples extracted from LL3 subband are much larger than those extracted from HH3 subband, which means that the value difference between the samples from the two subbands is generally quite large. So, again according to the definition of the length of the line segment \( pq \), the line segments constructed by the above proposed strategy likely have large lengths, especially, in the case of state 0 and state 1. Fig. 6 shows the comparison of the lengths of the line segments constructed by the SPA and the proposed strategy. It should be pointed out that the test image used for the comparison is gray-scale “Lena” image of 512 x 512 pixels. It can be observed from Fig. 6 that the probability of occurrence of the long line segments for the proposed

<table>
<thead>
<tr>
<th>Method</th>
<th>( M = 2 )</th>
<th>( M = 4 )</th>
<th>( M = 8 )</th>
<th>( M = 16 )</th>
<th>( M = 32 )</th>
<th>( M = 64 )</th>
<th>( M = 128 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPA</td>
<td>1.1781</td>
<td>1.3744</td>
<td>1.4726</td>
<td>1.5217</td>
<td>1.5463</td>
<td>1.5585</td>
<td>1.5647</td>
</tr>
<tr>
<td>ISPA</td>
<td>0.7854</td>
<td>0.7854</td>
<td>0.7854</td>
<td>0.7854</td>
<td>0.7854</td>
<td>0.7854</td>
<td>0.7854</td>
</tr>
</tbody>
</table>

Fig. 3. Illustration of the average angular distortion.

Fig. 4. Codelines with two repetitions, where \( \beta = \pi / 4 \).

Fig. 5. Difference in robustness when using different lengths of the line segments to embed the messages. In the testing, we generate 10000 Gaussian host signals with zero mean and \( \sigma_x = 40 \). The curves marked by circle, square, and triangle represent the use only the line segments whose lengths are larger than a certain threshold may change to be smaller (larger) than it due to the embedding operation and/or later image distortion. An attempt to solve this kind of asynchronous problem is to employ some extra codes to label the watermarked line segments. And these codes received by the decoder are used for identifying the watermarked line segments during messages extraction. However, this will result in too much side-information. In order to achieve better robustness while avoiding the asynchronous problem, we present a novel strategy for the ISPA to obtain the long line segments, which is described as follows:

(i) Perform 2-D 3-level wavelet decomposition on each non-overlapped block of a gray-scale image;

(ii) Produce a key-dependent uniform random sequence of numbers 0, 1, 2, and 3. And the four numbers 0, 1, 2, and 3 are used to represent four states, respectively. Note that the key that generates the random sequence is shared by both the message embedder and decoder;

(iii) For state 0, extract the pair of samples \( p = [u_1, u_2] \) from LL3 subband, and \( q = [u_3, u_4] \) from HH3 subband; for state 1, extract \( [u_2, u_3] \) from LL3 and \( [u_1, u_4] \) from HH3; for state 2, extract \( [u_1, u_2, u_3] \) from LL3 and \( [u_4] \) from HH3; for state 3, extract \( [u_1, u_2, u_4] \) from LL3 and \( [u_3] \) from HH3. Please note that we select the coefficients as host signal samples from the LL3 and HH3 blocks in raster-scan order;

(iv) Based on the SPA described in Section 2, embed one message into each group of samples \( u = [u_1, u_2, u_3, u_4] \).

It is known that the samples extracted from LL3 subband are much larger than those extracted from HH3 subband, which means that the value difference between the samples from the two subbands is generally quite large. So, again according to the definition of the length of the line segment \( pq \), the line segments constructed by the above proposed strategy likely have large lengths, especially, in the case of state 0 and state 1. Fig. 6 shows the comparison of the lengths of the line segments constructed by the SPA and the proposed strategy. It should be pointed out that the test image used for the comparison is gray-scale “Lena” image of 512 x 512 pixels. It can be observed from Fig. 6 that the probability of occurrence of the long line segments for the proposed
strategy is much larger than that for the SPA. In addition, from the analysis of Section 4.1, we can see that the proposed strategy for constructing the long line segments does not change the DWR of the SPA essentially.

It is worth noting that the above strategy of constructing long line segments can also provide certain security due to the key-dependent generation of embedding stages. Any attacker without knowing the keys will not know in which subband the watermarked signal samples are, thus having difficulty to remove watermarks, and also being prevented from unauthorized embedding and unauthorized decoding. Furthermore, inspired by some existing works [15–17] and [18], two ways can be used to further improve the security of ISPA. Considering that the coefficients in LL subband have approximately the same statistical characteristics, the first way is to randomly select the coefficients from LL subband of wavelet image as host signals, and the selection is controlled by a secret key. This can also be applied to the selection of coefficients in HH subband. In this case, the unauthorized removal of watermarks becomes much more difficult. Furthermore, the attackers without knowing the keys also have no authority to embed and decode watermarks. The second one is to rotate the codelines of ISPA by a key-dependent angle, as done in [18]. In this case, the unauthorized users are prevented from watermarks embedding and decoding as well.

4. Performance evaluation

In this section, we theoretically compare the ISPA with the SPA in terms of the embedding distortion (DWR) and robustness against AWGN attack (SER), respectively.

4.1. DWR analysis on codelines

As we know that, like robustness and payload, the DWR is a fundamental measure for the performance of digital watermarking. Without loss of generality, here we analyze the theoretical DWRs of the SPA’s and the modified codelines for \( M = 2 \). We assume that each sample \( u_i \) in the host signal is an independently and identically distributed (i.i.d.) Gaussian random variable with mean zero and variance \( \sigma_u^2 \), i.e. \( u_i \sim N(0, \sigma_u^2) \). Note that, in practice, the host signals do not strictly satisfy this point. However, for easy analysis and comparison from a theoretical point of view, the i.i.d. Gaussian assumption is common and acceptable. As shown in Fig. 7, the SPA projects the line segment \( P \) on the codeline \( L_1 \) to attain the watermarked line segment \( Y \), where \( p_1 = \frac{\pi - \alpha}{2} \), \( p_2 = \frac{\pi - \alpha}{2} \), and thus \( p_1 \sim N(0, \frac{1}{2} \sigma_u^2) \). In the message embedding described in Fig. 7, one can write the embedding distortion \( W \) (i.e., watermarked signal) caused by moving the two samples \( p_1 \) and \( p_2 \) as a function of the angular distortion \( \theta \). That is,

\[
W = P \sin(\theta). \tag{1}
\]

When we embed messages by projecting the line segments on the codeline \( L_1 \), the average energy of the watermark signal over each sample is given by

\[
\sigma_w^2 = \frac{1}{2} E[W^2] = \frac{1}{2} E[P^2 \sin^2(\theta)]. \tag{2}
\]

According to probability theory, the angle between the x-axis and the vector formed by two i.i.d. Gaussian random variables in a 2-D space is uniformly distributed in the range of \([-\pi, \pi]\) [19], and the length and the angle of the line segment \( P \) are independent mutually, hence we can rewrite Eq. (2) as

\[
\sigma_w^2 = \frac{1}{2} E[P^2] E[\sin^2(\theta)]. \tag{3}
\]

Then, we further compute the two terms \( E[P^2] \) and \( E[\sin^2(\theta)] \) by, respectively,

\[
E[P^2] = E[p_1^2 + p_2^2] = \sigma_u^2, \tag{4}
\]

and

\[
E[\sin^2(\theta)] = \int_{-\alpha}^{\pi-\alpha} \frac{\sin^2(\theta)}{2\pi} d\theta = \frac{\pi - 2 \sin(2\alpha)}{2\pi}. \tag{5}
\]

By the symmetry of the codelines, the average energy of the watermark signal over the samples \( p_3 \) and \( p_4 \) is the same as that of \( p_1 \) and \( p_2 \), moreover, the average embedding energy corresponding to the codeline \( L_2 \) is also the same as that corresponding to the codeline \( L_1 \). Then, according to Eqs. (3), (4), and (5), we have that

\[
DWR = 10 \log_{10} \frac{\sigma_w^2}{\sigma_u^2} = 10 \log_{10} \frac{4\pi}{\pi - 2 \sin(2\alpha)} = 10 \log_{10} \frac{8\beta}{2\beta - \sin(2\beta)}. \tag{6}
\]

In a similar way, we can derive the DWR of the ISPA, which is given by

\[
DWR = 10 \log_{10} \frac{8\beta}{2\beta - \sin(2\beta)}. \tag{7}
\]

When \( \beta = \frac{\pi}{4} \) and \( \alpha = \frac{\alpha}{2} \), according to Eqs. (6) and (7), the DWRs of the SPA and the ISPA are 8.6182 dB and 10.4170 dB, respectively, which coincides with the analysis of the angular distortion presented in Section 3.1. This means that the modified codelines can achieve the better fidelity of the watermarked signal than the SPA’s codelines. It should be pointed out that, according to our analysis, the increase of \( M \) cannot change the DWRs of both the SPA and ISPA too much.

4.2. SER under AWGN attack

In this subsection, we further analyze the SER\(^1\) of the extracted messages for the ISPA in the presence of AWGN. Again, we assume

\(^1\) We remark here that in this paper, we use the SER instead of the bit error rate (BER) to measure the error probability of the extracted messages, where SER
that the samples of the host signal are i.i.d. Gaussian random variables with mean zero and variance $\sigma_n^2$ (i.e., $u \sim N(0, \sigma_n^2)$), and the received samples are corrupted by AWGN $n \sim N(0, \sigma_n^2)$. Let’s denote $c$ and $P_e$ as the slope of the extracted line segment and the error probability of the extracted message symbols, respectively. Denote $\phi_i$ and $\phi_{i+1}$ as the angle of the extracted line segment and the error probability of the extracted message symbols, respectively, and $\alpha_i$ as the slope of the codeline $L_i$. Then, we can obtain that

$$P_e = \frac{1}{M} \sum_{i=1}^{M} P(e|i),$$

and

$$\phi_i = \frac{\pi}{4} - \frac{M - 2(i - 1)}{2} \beta,$$

and

$$\alpha_i = \tan \left( \frac{\pi}{4} - \frac{M - 2i + 1}{2} \beta \right),$$

where $P(e|i)$ represents the decoding error probability when the message $i$ is embedded.

We denote $p_C(c|i)$ as the probability density function (PDF) of the slope $c$ conditioned by the embedding of the message $i$, which, based on the analysis in Section III-B of Ref. [1], is given by the conditional PDF

$$p_C(c|i) = \frac{1}{\pi} \frac{\sigma_{b_i} \sigma_{\phi_i}}{\sigma_b^2 \sigma_{\phi}^2} \sqrt{1 - \frac{1}{r_i^2}},$$

where $\sigma_{b_i}^2 = \frac{2\alpha_i^2}{1 + \alpha_i^2} \sigma_n^2 + 2\sigma_n^2$, $\sigma_{\phi_i}^2 = \frac{2}{1 + \alpha_i^2} \sigma_n^2 + 2\sigma_n^2$, $r_i = \frac{\alpha_i \sigma_n^2}{\sigma_{\phi_i}^2}$

And the cumulative distribution function (CDF) of $p_C(c|i)$ can be computed as

$$F_C(c|i) = \frac{1}{2} + \frac{1}{\pi} \arctan \left( \frac{d_i - r_i}{\sqrt{1 - r_i^2}} \right),$$

where $d_i = \frac{\sigma_{b_i}}{\sigma_{\phi_i}}$. The maximum likelihood detector works as follows:

$$\hat{i} = \arg \max_{i \in \{1, \ldots, M\}} p_C(c|i).$$

Then, the error probability of the above detector can be written as

$$P(e|i) = \frac{1}{\pi} \left[ \tan \left( \frac{\phi_{i+1} - \pi}{2} \right) \right] < c < \tan(\phi_i) \left| i \right| + \frac{1}{\pi} \left[ \tan(\phi_{i+1}) < c \left| i \right| \right].$$

According to Eq. (12), we can rewrite Eq. (14) as

$$P(e|i) = 1 + G_i(\phi_i) - G_i(\phi_{i+1}),$$

where $G_i(\phi) = \frac{1}{\pi} \arctan \left( \frac{d_i \tan(\phi) - r_i}{\sqrt{1 - r_i^2}} \right) - \frac{1}{\pi} \arctan \left( \frac{d_i \tan(\phi) + r_i}{\sqrt{1 - r_i^2}} \right).$ Substituting Eq. (15) in Eq. (8), we further have

$$P_e = 1 + \frac{1}{M} \sum_{i=1}^{M} \left[ G_i(\phi_i) - G_i(\phi_{i+1}) \right].$$

5. Experimental results

We have conducted several experiments to test the performance of the improved SPA against different attacks. 

5.1. Tests on artificial Gaussian signals

In the experiment, the host signals for testing are the Gaussian signals under AWGN attack. We first investigate the performance of the modified codelines. We can see from Fig. 9(a) that the ISPA without constructing long line segments has almost the same robustness as the SPA. However, in the test the DWRs of the ISPA and the SPA are 10.4 dB and 8.6 dB, respectively, which means that the modified codelines mainly improve the SPA in terms of the fidelity of the watermarked signal. The experimental DWR results also further validate our theoretical analysis in the Section 4.1. From Fig. 9(b), we can still see that both the ISPA and the SPA outperform the AQIM. While, Fig. 9(b) shows that the ISPA with the two proposed strategies achieves a great improvement of robustness over the SPA, which is mainly due to the use of the long line segments.

5.2. Tests on image signals

Then, we conduct some experiments to verify the performance of the ISPA in real application. The test images include “Lena”, “Baboon”, “Plane”, “Pirate”, “Boat”, and “Bridge”, which are all of the ISPA in real application. The test images include “Lena”, “Baboon”, “Plane”, “Pirate”, “Boat”, and “Bridge”, which are all of the ISPA in real application. The test images include “Lena”, “Baboon”, “Plane”, “Pirate”, “Boat”, and “Bridge”, which are all of the ISPA in real application. The test images include “Lena”, “Baboon”, “Plane”, “Pirate”, “Boat”, and “Bridge”, which are all of the ISPA in real application.
The ISPA, the SPA and the AQIM set \( M = 2 \) and embed one message bit into one block to obtain the embedding payload of 256 bits. Both the SPA and the AQIM embed the message into the \( LL_3 \) subband, while the ISPA uses the \( LL_3 \) and the \( HH_3 \) subbands for messages embedding. The results are obtained by averaging over 100 runs with 100 different pseudorandom binary message sequences. In order to make the three compared schemes have approximately the same quality of watermarked image (i.e., PSNR), we set \( \beta = \frac{\pi}{8} \) for the ISPA, \( \beta = \frac{\pi}{4} \) for the SPA, and set the angle quantization step to be \( \frac{\pi}{16} \) for the AQIM [11], respectively, which are obtained empirically. Note that we repeat the ISPA's code-lines two times to make that \( \beta = \frac{\pi}{8} \). (Please see Fig. 4.) Fig. 10 shows the original test images and the corresponding images watermarked by the ISPA. We can see that the ISPA can achieve good visual quality of the watermarked images. The PSNR values of the test six images for the ISPA are obtained as 42.18, 42.12, 40.74, 42.98, 42.30, and 42.79 dB, respectively. The corresponding PSNR values for the SPA are 41.02, 43.11, 40.50, 42.16, 41.29, and 41.52 dB, respectively. And, the corresponding PSNR values for the AQIM are 41.23, 42.76, 40.91, 42.89, 41.25, and 42.03 dB, respectively. We can see that the PSNRs of the watermarked images exceed 40 dB for all of three schemes and the ISPA obtains the best objective quality of the watermarked images among the three compared schemes.

To evaluate the robustness performance of the proposed ISPA for image watermarking, the watermarked images used in testing are distorted by various attacks including AWGN, salt & pepper noise, rotation, scaling, Gaussian filter, median filter, and JPEG compression. And then we extract the messages from the attacked images to compute the SER by comparing the extracted messages with the original messages. The robustness of the three compared watermarking schemes are shown in Tables 2, 3, 4, and 5. In the following, we discuss the robustness against each type of attacks, respectively.

(1) **AWGN attack**: AWGN is the most commonly studied noise when considering the robustness of image watermarking. In this experiment, the AWGNs with standard deviation \( \sigma \in \{10, 20, 30\} \) (which is also restricted to the range of \([0, 255]\)) are added to the watermarked image. We can see from Tables 2 and 3 that the ISPA performs best in terms of the AWGN attacks. It can be also seen that the AWGN attack dramatically degrades the robustness of the SPA. The reason is that AWGN results in a significant perturbation to the short line segments used for messages embedding. This confirms our suggestion on constructing long line segments for watermarking.

(2) **Salt & pepper noise attack**: Salt & pepper noise is a kind of random impulse noises. We add the Salt & pepper noise with probability \( p = \{0.01, 0.02, 0.04\} \) to the watermarked images. The SERs of the extracted messages from the watermarked image are listed in Tables 2 and 3. We can see from Tables 2 and 3 that the ISPA is superior to both the AQIM and the SPA in resisting Salt & pepper noise attack.

(3) **Rotation attack**: The rotation attack is a kind of geometrical attacks and is a very severe attack to the direction-based embedding methods, such as the AQIM, the SPA, and the ISPA. From Tables 2 and 3, we can see that all of the three compared schemes do not perform well under rotation attack. Note that both the ISPA and the SPA are not designed for resisting geometrical attack. To resist the geometrical attack, the ISPA may be combined with other robustness techniques, such as the use of an additional template [20]. But, we can see from Tables 2 and 3 that the ISPA still performs best among the three schemes.

(4) **Amplitude scaling attack**: Like the AQIM, both the ISPA and the SPA are essentially invariant to amplitude scaling. As expected, the AQIM, the SPA, and the ISPA schemes are quite robust to the amplitude scaling attacks. Especially, it can be seen from the two columns in the right-most-side of Tables 2 and 3, the ISPA is almost invariant to this distortion. But it is not so good for the SPA. When the amplitude scale factor is 1.5 times, a number of image pixels will be saturated and then be truncated, which results in a non-linear distortion. This non-linear distortion likely changes the angles of the short line segments and so decreases the robustness of the SPA.

(5) **Gaussian and median filtering attack**: Gaussian low-pass filter has been commonly used for image de-noising. In our experiments, the watermarked images are denoised by the Gaussian filters with size \( W \times W \), where \( W \in \{3, 5, 7\} \) and standard deviation \( \sigma = 0.5 \). Since the Gaussian filter changes only the magnitudes of the sample vectors, all of the three methods are robust to this attack. The median filter is an effective tool to remove Salt & pepper noise. But it is non-linear and gives rise to a much larger distortion in the direction of an angle than the linear Gaussian filter. It can be seen from Tables 4 and 5 that the three compared schemes are more robust to Gaussian filtering attack than to median filtering attack.

(6) **Lossy JPEG compression attack**: JPEG compression is one of the most popular techniques for image compression and is widely applied in the internet. Thus, a watermarking scheme should be very robust to JPEG compression attack. It is known that the fidelity of a watermarked image decreases with the decrease of the quality factor (QF). In this experiment, JPEG compression with different QFs is performed on the watermarked images. The experimental results are given in Tables 4 and 5. We can see that both the ISPA and the AQIM are very robust to JPEG compression attack. While, the SPA performs not well enough. This is due to the fact the lengths of the line segments constructed by both the AQIM and the ISPA are far larger than that of the SPA. But we can observe that for "Baboon"
Fig. 10. Original test images (the first and third rows) and the watermarked images (the second and fourth rows). From left to right and top to bottom, the test images are “Lena”, “Baboon”, “Plane”, “Pirate”, “Boat”, and “Bridge” images.

Table 2
Comparison of SER (%) among the AQIM, the SPA, and the ISPA.

<table>
<thead>
<tr>
<th>Image</th>
<th>Method</th>
<th>AWGN (σ)</th>
<th>Salt &amp; pepper (p)</th>
<th>Rotation (θ)</th>
<th>Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10 20 30</td>
<td>0.01 0.02 0.04</td>
<td>0.5 1</td>
<td>0.75 1.5</td>
</tr>
<tr>
<td>Lena</td>
<td>AQIM</td>
<td>0.25 2.23 4.86</td>
<td>0.36 0.26 0.53</td>
<td>8.64 15.72</td>
<td>0.00 0.00</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
<td>13.50 18.31 19.62</td>
<td>5.97 7.82 9.85</td>
<td>19.37 29.30</td>
<td>0.00 0.10</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
<td>0.13 0.97 1.04</td>
<td>0.00 0.00 0.00</td>
<td>7.43 10.75</td>
<td>0.00 0.00</td>
</tr>
<tr>
<td>Baboon</td>
<td>AQIM</td>
<td>1.95 6.64 10.50</td>
<td>3.42 5.51 7.22</td>
<td>17.21 28.70</td>
<td>0.10 0.13</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
<td>12.90 16.40 23.40</td>
<td>8.23 10.37 11.43</td>
<td>15.65 27.20</td>
<td>0.10 0.11</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
<td>1.17 2.73 7.81</td>
<td>1.31 3.84 5.16</td>
<td>14.17 25.50</td>
<td>0.00 0.00</td>
</tr>
<tr>
<td>Plane</td>
<td>AQIM</td>
<td>0.39 2.73 5.47</td>
<td>0.39 0.58 0.73</td>
<td>10.16 16.03</td>
<td>0.00 0.00</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
<td>15.23 20.70 21.48</td>
<td>7.42 9.32 11.56</td>
<td>21.48 33.20</td>
<td>0.00 0.00</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
<td>0.39 0.78 1.17</td>
<td>0.00 0.35 0.52</td>
<td>8.98 12.44</td>
<td>0.00 0.00</td>
</tr>
</tbody>
</table>
and “Bridge” images, the robustness of the three schemes seems to be similar. This is in good agreement to the fact these two detailed images have large numbers of high-frequency components so that the lengths of the line segments constructed by the three schemes are approximately equal. However, for the relatively smooth images, such as “Lena”, “Plane”, “Pirate”, and “Boat”, the advantage of the line segments constructed by both the AQJM and the ISPA is apparent.

In order to further verify the effectiveness of the ISPA for various images, we employ a database of 2000 images to test the three compared methods. The test images are randomly chosen from BOWS2 dataset [21], which has 10,000 gray-scale images of 512 × 512 pixels and includes images of landscapes, people, plants, animals, buildings, and so on. The resulted PSNR and SER are averaged over 2000 test images. The average PSNRs of the database for the AQJM, the SPA, and the ISPA are 42.95, 42.29, and 43.03 dB, respectively. The ISPA still obtains the best quality of the watermarked images. From Tables 6 and 7, we can also see that the ISPA obtains the strongest robustness against various attacks among the three compared schemes.

### 6. Conclusions

In this paper, we have presented an improved sample projection approach (ISPA) for image copyright protection. The experiments conducted on both artificial Gaussian signals and the natural images demonstrate the superiority of the ISPA over the original SPA. The main contributions of this paper can be summarized as follows: 1) We have introduced the modified codelines by inverting the part of the codelines of the SPA. According to our analysis and experiments, the modified codelines can result in a lower embedding distortion than the SPA’s codelines; 2) We have also proposed a strategy to construct the long line segments, which is used for messages embedding. Our experiments show that the use of long line segments can significantly improve the robustness against various attacks; 3) We have provided the theoretical analysis of the DWRs for both the SPA and the ISPA, and have derived

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Comparison of SER (%) among the AQJM, the SPA, and the ISPA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Method</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Pirate</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Boat</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Bridge</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Comparison of SER (%) among the AQJM, the SPA, and the ISPA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Method</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Lena</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Baboon</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Plane</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5</th>
<th>Comparison of SER (%) among the AQJM, the SPA, and the ISPA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Method</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Pirate</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Boat</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
<tr>
<td>Bridge</td>
<td>AQJM</td>
</tr>
<tr>
<td></td>
<td>SPA</td>
</tr>
<tr>
<td></td>
<td>ISPA</td>
</tr>
</tbody>
</table>
the theoretical closed-form expression of the SER against AWGN attack for the ISPA. Our experimental results have validated the above theoretical analysis.

Acknowledgments

The authors would like to thank the anonymous reviewers for their comments. This work has been supported by 973 Program (2011CB302204), NSFC (U1135001, 61003297, 61272498), NSF of Guangdong Province (S2013010011806), the Knowledge Innovation Program of Shenzhen (JCYJ20130401170306848), and the Shenzhen Peacock Program (KQCX20120816160011790).

References


Yuan-Gen Wang is currently pursuing his Ph.D. degree in the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China. His current research interests include digital watermarking, digital forensics.

Guopu Zhu received the B.S. degree from Jilin University, China, in 2002, the M.S. and Ph.D. degrees from Harbin Institute of Technology, China, in 2004 and 2007, respectively. From 2007 to 2010, he was a post-doctoral researcher in Sun Yat-sen University, China. He is currently an Associate Professor in Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences. His main research areas are multimedia security and image processing. He has published more than 10 refereed international journal papers in these areas.

Jiwu Huang received the B.S. degree from Xidian University, Xi’an, China, the M.S. degree from Tsinghua University, Beijing, China, and the Ph.D. degree from the Institute of Automation, Chinese Academy of Science, Beijing, in 1982, 1987, and 1998, respectively. He is currently a Professor with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China. His current research interests include multimedia forensics and security. Dr. Huang serves as a member of the IEEE CASS Multimedia Systems and Applications Technical Committee, and the IEEE SPS Information Forensics and Security Technical Committee. He is an Associate Editor for a few international journals including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.