www.ietdl.org

Published in IET Image Processing
Received on 28th February 2013
Revised on 2nd August 2013
Accepted on 29th August 2013
doi: 10.1049/iet-ipr.2013.0386

ISSN 1751-9659

Geometric modelling of the wavelet coefficients for image watermarking using optimum detector

Mohammad Hamghalam[1], Sattar Mirzakuchaki[1], Mohammad Ali Akhaee[2]

[1]Department of Electrical Engineering, Iran University of Science and Technology, Tehran 16846–13114, Iran
[2]Department of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran 14588–89694, Iran
E-mail: m.hamghalam@gmail.com

Abstract: In this study, a robust image watermarking method based on geometric modelling is presented. Eight samples of wavelet approximation coefficients on each image block are utilised to construct two line segments in the two-dimensional space. The authors change the angle formed between these line segments for data embedding. Geometrical tools are used to solve the tradeoff between the transparency and robustness of the watermark data. They analytically determine the probability density function of the embedding angle for Gaussian samples. Maximum-likelihood decoder is implemented in the receiver side. Owing to embedding in the angle between two line segments, the proposed scheme has high robustness against the gain attacks. In addition, using the low frequency components of the image blocks for data embedding, high robustness against noise and compression attacks has been achieved. Experimental results confirm the validity of the theoretical analyses given in this study and show the superiority of the proposed method against common attacks, such as Gaussian filtering, median filtering and scaling attacks.

1 Introduction

Digital watermarking is the process of embedding some information called the watermark into a digital media (host signal) for the purposes of copyright protection, authentication, fingerprinting, copy protection etc. This embedding should not considerably degrade the perceptual quality of the host signal. The detectability of the watermark after manipulations occurring through channel either intentional or incidental is the main requirement of a digital watermarking system. Several watermarking techniques have been proposed so far. Watermarking techniques can be categorised into two classes [1]: quantisation index modulation (QIM)-based approaches [2–4] and spread spectrum (SS)-based [5–7] approaches. In SS-based watermarking, the copyright information is modulated using a pseudorandom sequence which corresponds to spreading the information in the frequency domain. The QIM-based schemes embed a watermark bit by quantising the host signal samples with one of a series of quantisation lattices.

The QIM-based algorithms have attracted extensive interest among many watermarking schemes presented so far. The robustness to additive white Gaussian noise (AWGN) and the high capacity are two advantages of these schemes. However, traditional quantisation-based schemes were not robust against simple volumetric attacks, which may happen because of the scanning process where light is not distributed uniformly over this paper in some multimedia applications. Robustness against volumetric attacks has been the subject of many papers over the last few years. Some researchers define an embedding domain invariant to the volumetric scaling [8, 9]. Oostveen *et al.* introduced a quantisation watermarking scheme with adaptive quantisation step size. The step size for a sample is taken proportional to the average value of the number of neighbouring samples. This approach leads to robustness against value scaling. Several studies [10, 11] have obtained improvement on the quantisation-based data-hiding method, called rational dither modulation (RDM). This method is based on using a gain-invariant adaptive quantisation step size at both transmitting and receiving ends. The high peak to average power ratio of RDM algorithm which happens because of its momentarily large quantisation step size is the main drawback of this method. Besides, the means of choosing its rational function is not optimal. This problem is demonstrated in [12], where the logarithmic homogenous RDM is proposed in either group or sample based. One study [13] reported a method for estimating amplitude modifications of watermarked data based on securely embedded scalar Costa scheme [14] pilot watermarks. However, embedding a pilot signal deterministically known to both transmitting and receiving ends reduces the available payload. It also decreases the security of the algorithm since the malicious attacker could simply focus on removing the pilot itself [15, 16]. In another work, Miller *et al.* [17] introduced an algorithm for image watermarking with large data payloads by means of informed embedding and coding techniques. A study by Conway *et al.* [18] has also shown that using spherical code words with correlator decoders improves the robustness on this scheme. However, their method results in a very complicated watermark embedding and decoding scheme.

Over the last few years, some methods have been proposed in frequency domain [19–24]. Nezhadarya *et al.* [24]

proposed an image embedding scheme that embedded the watermark using uniform quantisation of the direction of the significant gradient vectors obtained at multiple wavelet scales. Besides, a region-based QIM method that utilises quad-tree decomposition to find the visually significant image regions has been proposed in [25]. Kalantari and Ahadi [21] also proposed a logarithmic QIM (LQIM) scheme inspired by the μ-Law compression function. In their method, smaller step sizes are devoted to smaller amplitudes and larger step sizes are associated with larger amplitudes. In [26], angle quantisation index modulation (AQIM) works by quantising the angle formed by the host-signal vector with respect to the origin of a hyper-spherical coordinate system. The low robustness of AQIM against AWGN is the main drawback of this approach. This problem has been addressed in [22], where watermark embedding is performed by projection of the host samples on the specific coding lines. Although this method has a proper robustness against AWGN, it has low capacity and embeds 128 bits by preserving fidelity in 512 × 512 images.

Here, we propose a new watermarking method that embeds the hidden message in a domain invariant to the volumetric attack. In order to achieve higher robustness against AWGN and JPEG compression attacks, we embed the watermark bits into the wavelet approximation coefficients of the image blocks. Since human eyes sensitivity decreases in regions with spatial complexity, high entropy blocks have been employed for watermark embedding. Eight samples of each block are selected to this aim. Then the eight samples are modeled as four points in two-dimensional (2D) space. A straight line segment can be drawn joining the every two points. The angle between two line segments is considered for data hiding which is invariant to the gain attack. In the receiver side, to achieve optimum behaviour of the maximum-likelihood (ML) detector, the probability distribution function (pdf) which correctly models the distribution of the transform coefficients is required. The approximation coefficients of most of the image blocks after embedding can be modelled with the Gaussian distribution. We confirm the normality of these samples by applying the Kolmogorov–Smirnov test [27, 28]. The performance of the proposed method is analytically investigated and verified via simulations.

The remainder of this paper is organised as follows. In the next section, we describe the embedding method. Section 3, explains the watermark decoding. Section 4 is dedicated to analytical calculation of the bit error probability. Experimental results and comparison of the proposed method with some recent techniques are presented in Section 5. Finally, Section 6 concludes the paper.

2 Embedding method

In this section, we introduce our robust watermarking scheme. The proposed scheme embeds a watermark in the approximation coefficients of the image blocks by slightly modifying the eight coefficients of each block. In the first subsection, mode of one bit watermark insertion in eight samples of the host signal was explained. These samples correspond to four points in 2D space. Two line segments are defined using these points and the angles between two line segments are utilised for watermarking. Changing the points coordinates, the angle of these two line segments are altered in order to insert information bit. These manipulations must be as small as possible to let transparency condition be satisfied. In the following, we apply geometrical tools to minimise distortion imposed by watermarking. We first discuss the embedding details. Then, specific coding lines exploited for watermarking purpose will be introduced in the next subsection.

2.1 Proposed method

We assume to have eight samples of an independently and identically distributed (i.i.d) Gaussian random variable as the host signal. This host signal is denoted as $\boldsymbol{u} = [u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8]$ with mean and variance μ, σ_u^2, respectively. In the implementation of our watermarking system, this issue can be achieved by considering approximation coefficients of the image blocks. These eight samples are modelled as four points $p = [u_1, u_2]$, $q = [u_3, u_4]$, $r = [u_5, u_6]$ and $s = [u_7, u_8]$ in the 2D space. A straight line segment can be drawn between every two points. Thus, we have two line segments pq and rs. The angle between these lines is denoted as θ which is employed as our watermarking variable. The slopes of the two line segments are represented by m_1 and m_2; thus, θ, the angle between them can be calculated as

$$\tan\theta = \frac{m_1 - m_2}{1 + m_1 m_2}, \quad 0 < \theta < \pi$$

where

$$m_1 = \frac{u_4 - u_2}{u_3 - u_1} \text{ and } m_2 = \frac{u_8 - u_6}{u_7 - u_5}$$

In order to achieve a specified angle, displacement in the coordinates of points has to be applied. To preserve transparency criteria, we minimise the overall change in the coordinate of points. In Fig. 1, four arbitrary samples are depicted. Thus, the problem is to minimise (1) subject to $\theta = \theta_Q$

$$d = \min\left(\sum_{k=1}^{8}\left(u_k - u_k'\right)^2\right) \tag{1}$$

where u'_k are watermarked samples and θ_Q is the watermarked angle. The Euclidean distance required for each point to achieve

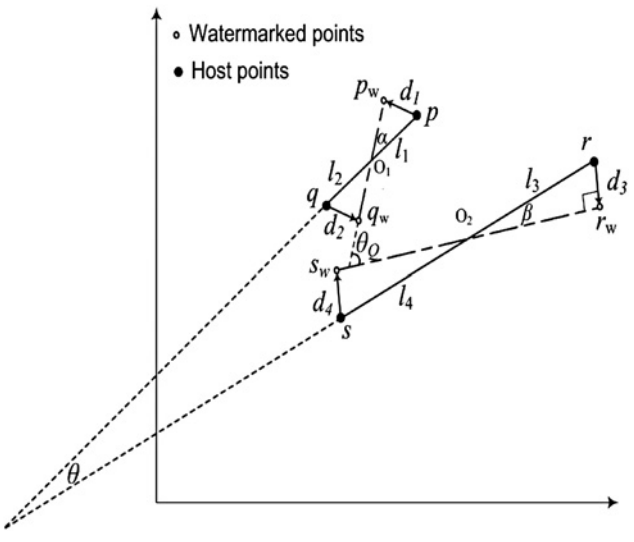

Fig. 1 *Illustrating eight typical samples in 2D space as the four points (p, q, r and s) and their corresponding watermarked points (p_w, q_w, r_w and s_w)*

the watermarked angle are denoted by d_1, d_2, d_3 and d_4, respectively. It can be expressed as

$$\begin{aligned} d_1 &= \sqrt{(u_1 - u_1')^2 + (u_2 - u_2')^2} \\ d_2 &= \sqrt{(u_3 - u_3')^2 + (u_4 - u_4')^2} \\ d_3 &= \sqrt{(u_5 - u_5')^2 + (u_6 - u_6')^2} \\ d_4 &= \sqrt{(u_7 - u_7')^2 + (u_8 - u_8')^2} \end{aligned} \tag{2}$$

Substituting (2) in (1) results in (3) as follows

$$d = \min\left(d_1^2 + d_2^2 + d_3^2 + d_4^2\right) \tag{3}$$

We define the angle between the line segment, pq, and the watermarked line segment, $p_w q_w$, as α. Moreover, we use β for the angle between rs and $r_w s_w$ line segments. In this way, d_i can be calculated as the following equation

$$\begin{aligned} d_i &= l_i \sin\alpha, \quad i = 1, 2 \\ d_i &= l_i \sin\beta, \quad i = 3, 4 \end{aligned} \tag{4}$$

where l_1, l_2, l_3 and l_4 are the length of half-lines as shown in Fig. 1. Using (4) we have

$$d = \min\left\{\left(l_1^2 + l_2^2\right)\sin^2\alpha + \left(l_3^2 + l_4^2\right)\sin^2\beta\right\} \tag{5}$$

It is noted that summation of l_1 and l_2 is a constant value which is equal to the length of the line segment $|pq|$. Accordingly, the summation of l_3 and l_4 is equal to $|rs|$. Suppose that the value of α and β are known, then (5) may be simplified as

$$d = \min\left\{(l_1 + l_2)^2 - 2l_1 l_2\right\}\sin^2\alpha + \min\left\{(l_3 + l_4)^2 - 2l_3 l_4\right\} \times \sin^2\beta$$

Therefore straightforward maximisation problem is given by

$$d = |pq|^2 - 2\max\left\{l_1 l_2\right\}\sin^2\alpha + |rs|^2 - 2\max\left\{l_3 l_4\right\} \times \sin^2\beta \tag{6}$$

for minimisation of (6), we have

$$l_1 = l_2 \text{ and } l_3 = l_4 \tag{7}$$

By combining (4) and (7), it is obtained $d_1 = d_2$ and $d_3 = d_4$. Assuming α and β are known, the relation (7) results. Putting this assumption away α and β values are calculated in order to minimise the overall change in host signal. According to Fig. 1, it is easy to show that $\alpha + \beta = |\theta - \theta_Q|$. Considering (7), (8) can be deduced

$$\min\left\{2l_1^2\sin^2\alpha + 2l_3^2\sin^2\beta\right\} \tag{8}$$

Applying the derivative function, we solve the minimisation problem of (8). After some simplifications, (9) can be achieved

$$\begin{aligned} \alpha_{\text{opt}} &= \frac{-i}{4} \times \log\left(\frac{l_3^2 e^{i4\left(|\theta - \theta_Q|\right)} - l_3^2}{l_1^2 e^{i2\left(|\theta - \theta_Q|\right)} + l_3^2} + 1\right) \\ \beta_{\text{opt}} &= |\theta - \theta_Q| - \alpha_{\text{opt}} \end{aligned} \tag{9}$$

where α_{opt} and β_{opt} are the optimum values to reach the watermarked angle of θ_Q. The watermarked angle can be attained by applying the optimum values to the line segments while minimising (8). The slope of the watermarked lines $p_w q_w$ and $r_w s_w$ can be computed as

$$\begin{aligned} k_1 &= \tan\left(\theta_1 \pm \alpha_{\text{opt}}\right) \\ k_2 &= \tan\left(\theta_2 \pm \beta_{\text{opt}}\right) \end{aligned}$$

Now, the imposed points, p, q, r and s, are projected on the watermarked lines. These watermarked points are depicted in Fig. 1 by p_w, q_w, r_w and s_w. The eight watermarked samples can be concluded by projection on the watermarked lines. The watermarked samples are represented as $\boldsymbol{u}' = \left[u_1', u_2', u_3', u_4', u_5', u_6', u_7', u_8'\right]$. As a consequence

$$\begin{aligned} k = \tan\theta_Q &= \frac{m_1' - m_2'}{1 + m_1' m_2'} \\ &= \frac{(u_8' - u_6')(u_2' - u_1') - (u_4' - u_3')(u_7' - u_5')}{(u_2' - u_1')(u_7' - u_5') + (u_4' - u_3')(u_8' - u_6')} \end{aligned} \tag{10}$$

where k is the tangent of the watermarked angle and $m_1' = \dfrac{u_4' - u_2'}{u_3' - u_1'}$ and $m_2' = \dfrac{u_8' - u_6'}{u_7' - u_5'}$.

2.2 Coding space

This subsection discusses about the proper choose of the watermarked angle, which is the angle formed by the coding line and the positive horizontal axis. These coding lines are shared between transmitter and receiver. Fig. 2 depicts the coding spaces in which the cl_i's are the indicators of the watermarked lines. The watermarking code is embedded by projecting the host points on one of these coding lines according to the message bits. In fact, the closest coding line to the angle formed by host lines is

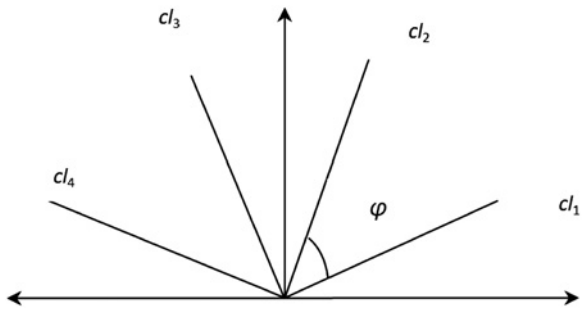

Fig. 2 *Illustration of the coding lines in 2D space*

Parameter ϕ is the angle between two coding lines, cl_1 and cl_2 as well as cl_3 and cl_4

doi: 10.1049/iet-ipr.2013.0386

selected to impose less distortion and thereby cause more invisibility of the watermarked signal. Note that, the more coding lines, the less quantisation distortion. We consider four typical coding lines as cl_1, cl_2, cl_3 and cl_4. By appropriately varying these line slopes and also the number of coding lines in the 2D space, a good trade-off between robustness and transparency would be achieved. On the other hand, by increasing the line numbers in the coding space, the imperceptibility of the watermark would be increased, whereas the robustness against attacks such as noise or lossy compression is decreased. Assuming four typical coding lines, a proper coding line according to the bit value can be found by (11). Here, in order to achieve an appropriate document-to-watermark ratio (DWR) and also to compare prior works in a fair condition, a number of different lines are utilised. This is fully covered in the experimental results section

$$\begin{cases} \text{bit} = 0, & \begin{cases} \theta_Q = \mathrm{cl}_2 & \theta < 90 \\ \theta_Q = \mathrm{cl}_3 & \theta \geq 90 \end{cases} \\ \text{bit} = 1, & \begin{cases} \theta_Q = \mathrm{cl}_1 & \theta < 90 \\ \theta_Q = \mathrm{cl}_4 & \theta \geq 90 \end{cases} \end{cases} \tag{11}$$

3 Watermark decoding

To extract the hidden bit in each block, we develop an optimum decoder based on the ML rule. To implement the decoder, the pdf of the host and watermarked samples are required. In [29], it is verified that the approximation coefficients of image blocks can be modeled with the Gaussian distribution. In the same way, we experimentally present that the watermarked approximation coefficients could be well approximated by a Gaussian distribution. Kolmogorov–Smirnov test is performed to compare the values of watermarked samples with the standard normal distribution. The test shows that for 90% of image blocks of various watermarked images, the approximation coefficients follow the Gaussian distribution at the significance level of 5%. Therefore this distribution has been used to develop our decoder. We also assume the host signal u and the watermarked signal u' to be i.i.d Gaussian coefficients, that is, $u \simeq u' \sim N(\mu_u, \sigma_u^2)$. Suppose that $\boldsymbol{y} = [y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8]$ represents the noisy watermarked approximation coefficients in the received block. In fact, the watermarked coefficients contaminated by zero mean AWGN $n \sim N(0, \sigma_n^2)$. That is, $\boldsymbol{y} = \boldsymbol{u}' + \boldsymbol{n}$.

Based on the assumptions made about the distribution of watermarked samples, we are able to estimate the distribution of the angle between the watermarked samples in the receiver side. By this distribution, the optimum detector can be designed. We model the eight coefficients in y as four points $p_r = [y_1, y_2]$, $q_r = [y_3, y_4]$, $r_r = [y_5, y_6]$ and $s_r = [y_7, y_8]$ in the 2D space. Thus, we have two lines $p_r q_r$ and $r_r s_r$ for each block. The angle between these two lines, θ_r, is computed as the following equation

$$\theta_r = \theta_2' - \theta_1' \tag{12}$$

where θ_2' and θ_1' can be calculated as the following equation

$$\begin{aligned} \theta_2' &= \arctan\left(\frac{y_8 - y_6}{y_7 - y_5}\right) \\ \theta_1' &= \arctan\left(\frac{y_4 - y_3}{y_2 - y_1}\right) \end{aligned} \tag{13}$$

Taking the tangent of both sides of (12), we have

$$\tan\theta_r = \frac{\tan\theta_2' - \tan\theta_1'}{1 + \tan\theta_2' \tan\theta_1'}$$

After some simplifications (14) is obtained as

$$\tan\theta_r = \frac{(y_8 - y_6)(y_2 - y_1) - (y_4 - y_3)(y_7 - y_5)}{(y_2 - y_1)(y_7 - y_5) + (y_4 - y_3)(y_8 - y_6)} \tag{14}$$

We define $c = \tan\theta_r$. Thus, exploiting (14), we can write (15) as (see eqn. (15))

To simplify the equations, (16) is defined as

$$\begin{aligned} a &= u_2' - u_1', \ b = u_4' - u_3' \\ g &= u_7' - u_5', \ h = u_8' - u_6' \\ a_n &= n_2' - n_1', \ b_n = n_4' - n_3' \\ g_n &= n_7' - n_5', \ h_n = n_8' - n_6' \end{aligned} \tag{16}$$

Substituting (16) and (10) in (15), (17) can be obtained

$$c = \frac{k(ag + bh) + a_n h + a h_n + a_n h_n - b g_n - b_n g - b_n g_n}{ag + bh + a g_n + a_n g + a_n g_n + h b_n + h_n b + h_n b_n} \tag{17}$$

To design the ML detector, the pdf which correctly models the distribution of the variable c is required. We propose the following assumption to implement our ML detector. Firstly, the approximation coefficients of the watermarked signal and noise are independent to each other. They are also independent and identically Gaussian distributed; therefore the distributions of the received coefficients can be computed as

$$\begin{aligned} a, b, g, h &\sim N(0, 2\sigma_u^2) \\ a_n, b_n, g_n, h_n &\sim N(0, 2\sigma_n^2) \end{aligned}$$

Secondly, as it is shown in [30], under some rational constrains, the multiplication of two Gaussian variables can be well approximated as Gaussian variable. In particular

$$N(\mu_f, \sigma_f^2) \times N(\mu_g, \sigma_g^2) \sim N(\mu_f \mu_g, \sigma_f^2 \sigma_g^2 + \mu_f^2 \sigma_g^2 + \mu_g^2 \sigma_f^2)$$

Thus, the distribution of the product terms in numerator and

$$c = \frac{(u_8' + n_8 - u_6' - n_6)(u_2' + n_2 - u_1' - n_1) - (u_4' + n_4 - u_3' - n_3)(u_7' + n_7 - u_5' - n_5)}{(u_2' + n_2 - u_1' - n_1)(u_7' + n_7 - u_5' - n_5) + (u_4' + n_4 - u_3' - n_3)(u_8' + n_8 - u_6' - n_6)} \tag{15}$$

denominator of (17) could be approximated in (18) as

$$\begin{aligned} &b_n g_n,\ h_n b_n,\ a_n g_n,\ a_n h_n \sim N\left(0,\ \sigma_{nn}^2\right) \\ &a g_n,\ a_n g,\ h b_n,\ h_n b,\ a h_n,\ a_n h,\ b g_n,\ b_n g \sim N\left(0,\ \sigma_{un}^2\right) \end{aligned} \tag{18}$$

where $\sigma_{nn}^2 = 4\sigma_n^4$ and $\sigma_{un}^2 = 4\sigma_u^2\sigma_n^2$.

Using (18), the pdf of the given numerator and denominator terms in (17) can be calculated as

$$c = \frac{N\left(0,\ 2\,k^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}^2\right)}{N\left(0,\ 2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}^2\right)} \tag{19}$$

Equation (19) gives the ratio of two correlated Gaussian random variable with zero mean and distinct variances. The pdf of the ratio $c = v/w$ of two zero-mean correlated Gaussian variables is Cauchy as

$$f_C(c) = \frac{1}{\pi}\frac{\sigma_v\sigma_w\sqrt{1-r^2}}{\sigma_w^2\left(c - \left(r\sigma_v/\sigma_w\right)\right)^2 + \sigma_v^2\left(1-r^2\right)} \tag{20}$$

where σ_a and σ_b are the variance of the numerator and denominator of the ratio, respectively; and r is the correlation coefficient calculated as the following equation

$$r = \frac{E\left[\left(v-\mu_v\right)\left(w-\mu_w\right)\right]}{\sigma_v\sigma_w} \tag{21}$$

Besides, its cumulative distribution function (cdf), can be given as

$$F_C(c) = \frac{1}{2} + \frac{1}{\pi}\tan^{-1}\frac{\sigma_w c - r\sigma_v}{\sigma_v\sqrt{1-r^2}} \tag{22}$$

According to (20), to compute the distribution of variable c, the estimation of the correlation coefficient is required. To this aim (21) is utilised. In (17), the terms with n indices represent the noise and since the watermarked signal and the noise are not correlated, the correlation coefficient of the noise terms with other terms is roughly equal to zero. Therefore it is sufficient to only show the correlation of the terms without noise such as ag and bh in the numerator and the denominator of (17). We investigated this correlation by the scatter plot and obtained the correlation coefficient equal to 0.02 which confirms implicitly the independency of the numerator from the denominator. Equation (23) presents the resulted correlation coefficient

$$r = \frac{2\,k\sigma_u^2}{\sqrt{\left(2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}^2\right)\left(2\,k^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}^2\right)}} \tag{23}$$

By substituting (23) in (20),the distribution function of c can be calculated. Using the pdf of c, the ML detector can be applied as

$$f_C(c|1) \underset{0}{\overset{1}{\gtrless}} f_C(c|0) \tag{24}$$

As discussed in Section 2, in order to embed each watermark bit, we fixed the angle between $p_w q_w$ and $r_w s_w$ line segments to the angle of θ_Q formed by the specified coding lines and the horizontal axis. We define k_0 and k_1 as the tangent of the watermarked angles subject to the bit zero or one is inserted. That is $k_0 = \tan(\theta_Q = \angle \mathrm{cl}_1)$ and $k_1 = \tan(\theta_Q = \angle \mathrm{cl}_2)$. Using these equations in (24), we have

$$\begin{aligned} &\frac{1}{\pi}\frac{\sigma_{v|1}\sigma_{w|1}\sqrt{1-r_{|1}^2}}{\sigma_{w|1}^2\left(c - \left(r_{|1}\sigma_{v|1}/\sigma_{w|1}\right)\right)^2 + \sigma_{v|1}^2\left(1-r_{|1}^2\right)} \underset{0}{\overset{1}{\gtrless}} \\ &\frac{1}{\pi}\frac{\sigma_{a|0}\sigma_{w|0}\sqrt{1-r_{|0}^2}}{\sigma_{w|0}^2\left(c - \left(r_{|0}\sigma_{v|0}/\sigma_{w|0}\right)\right)^2 + \sigma_{v|0}^2\left(1-r_{|0}^2\right)} \end{aligned} \tag{25}$$

where

$$\begin{aligned} \sigma_{v|1}^2 &= 2k_1^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un} \\ \sigma_{v|0}^2 &= 2k_0^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un} \\ \sigma_{w|1}^2 &= \sigma_{w|0}^2 = 2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un} \\ r_{|1} &= \frac{2k_1\sigma_u^2}{\sqrt{\left(2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}\right)\left(2k_1^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}\right)}} \\ r_{|0} &= \frac{2k_0\sigma_u^2}{\sqrt{\left(2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}\right)\left(2k_0^2\sigma_u^2 + 2\sigma_{nn}^2 + 4\sigma_{un}\right)}} \end{aligned}$$

As a consequence, (25) can be used as an optimum detector. The next section deals with the performance evaluation of the proposed algorithm.

4 Performance evaluation

In this section, the error probability of the proposed watermarking scheme in the presence of AWGN is analytically studied. The error occurs when the bit '0' is inserted while the bit '1' is detected and vice versa. Firstly, we compute the error probability when the detected angle between two lines is less than 90°. Then we extend the case for θ_r greater than 90°. In these calculations, d_1 is appointed as a decision boundary between two coding lines. With this assumption, the error probability P'_{e} can be written as

$$P'_{\mathrm{e}} = \frac{1}{2}\left\{P'(e|1) + P'(e|0)\right\} \tag{26}$$

According to d_1, decision boundary, (26) is rewritten as follows

$$\begin{aligned} P'_{\mathrm{e}} &= \frac{1}{2}\left\{P'\left(c < d_1|1\right) + P'\left(c > d_1|0\right)\right\} \\ P'_{\mathrm{e}} &= \frac{1}{2}\left\{F_{C|1}\left(d_1\right) + \left(1 - F_{C|0}\left(d_1\right)\right)\right\} \end{aligned} \tag{27}$$

Using the resulted cdf in (22) and by replacing it within (27), (28) is extracted as follows

$$\frac{1}{2}\left\{1 + \frac{1}{\pi}\tan^{-1}\frac{\sigma_{w|1}d_1 - r_{|1}\sigma_{v|1}}{\sigma_{v|1}\sqrt{1-r_{|1}^2}} - \frac{1}{\pi}\tan^{-1}\frac{\sigma_{w|0}d_1 - r_{|1}\sigma_{v|0}}{\sigma_{v|0}\sqrt{1-r_{|0}^2}}\right\} \tag{28}$$

doi: 10.1049/iet-ipr.2013.0386

Similarly, this equation is applicable when detected angle is larger than 90. In this case error probability is showed by P''_e.

Finally, the total error probability is the average of these two, as

$$P_e = \frac{1}{2}\left(P'_e + P''_e\right) \tag{29}$$

The comparison between theoretical and empirical error is made for Gaussian random variable with $\sigma = 40$. The coding lines whose angles are 22.5° and 67.5° are considered when θ is less than 90° for embedding the bits 0 and 1, respectively. Considering the existing symmetry, these values will be set to 112.5° and 157.5° when θ is more than 90°. Fig. 3 demonstrates the probability of error in the noisy environment with various noise power measured by the watermark-to-noise ratio. It confirms that the theoretical and experimental results are well matched.

5 Experimental results

Here, we conduct extensive simulations on both artificial and real signals to evaluate the performance of the proposed method and the validity of the analytical derivations. Initially, we present the experiment by simulation on artificial signals to show the performance of the proposed method for different situations. Following this, to show the advantages of the proposed method and to compare with previous quantisation-based methods, simulation on real images is performed.

5.1 Simulation on artificial signals

At this step, the host signal is produced by using random numbers from the normal distribution with mean parameter $\mu = 0$ and standard deviation parameter $\sigma = 40$. When this has been done, we evaluate the performance of the proposed method and verify the accuracy of our analysis. The results are reported by averaging over 100 different runs to ensure the accuracy of the empirical results.

Firstly, to compare the decoding performance of the proposed method with the AQIM [31], hyperbolic RDM [11] and sample projection method [22], the empirical probability of error against the DWR are shown in Fig. 4. The strength of the watermark, DWR, is fixed to 22 dB. It is clear that the proposed method consistently yields better decoding performance than these three methods under AWGN attack.

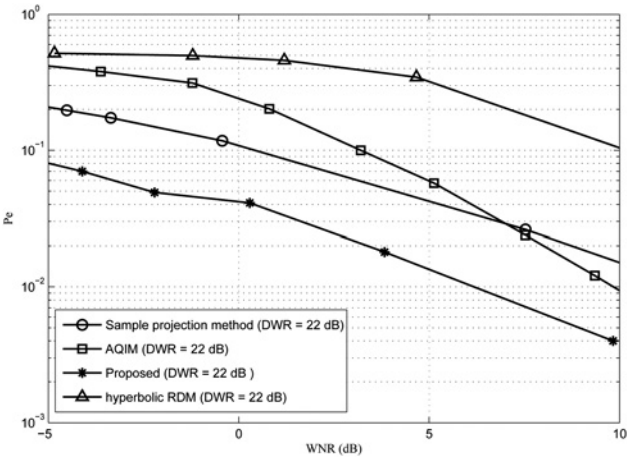

Fig. 4 *Comparison among the proposed watermarking method, AQIM [31], hyperbolic RDM [11] and sample projection method [22] on Gaussian host signals ($\sigma = 40$) of DWR = 22 dB*

Afterwards, we compare the capacity of the proposed scheme with the sample projection approach [22] for the same document-to-noise ratio (DNR) of 18 dB. In both methods, a fixed BER of 11% is considered as a typical value. It can be seen in Fig. 5 that the proposed methods outperform the sample projection method.

Finally, to examine the robustness of our method against non-linear distortions, power-law attack is utilised. The power-law attack consists of an exponentiation (γ) and gain scaling (λ) of the amplitudes of the watermarked signal, as $z = \lambda(y + n)^{\gamma}$, where y is the watermarked signal and n is the white Gaussian noise. The probability of error results of hyperbolic RDM [11], AQIM [31], sample projection method [22] and the proposed method with DWR = 25 dB, $(\lambda) = 0.7$ and $(\gamma) = 1.2$ is depicted in Fig. 6. It can be seen that the proposed method has better performance than the mentioned methods for the studied attack (Table 1).

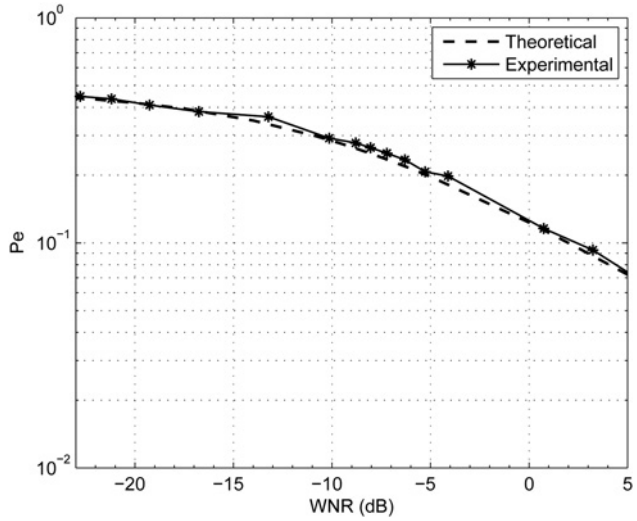

Fig. 3 *Comparison between the theoretical and experimental error probability for a Gaussian random variable with $\sigma_u = 40$*

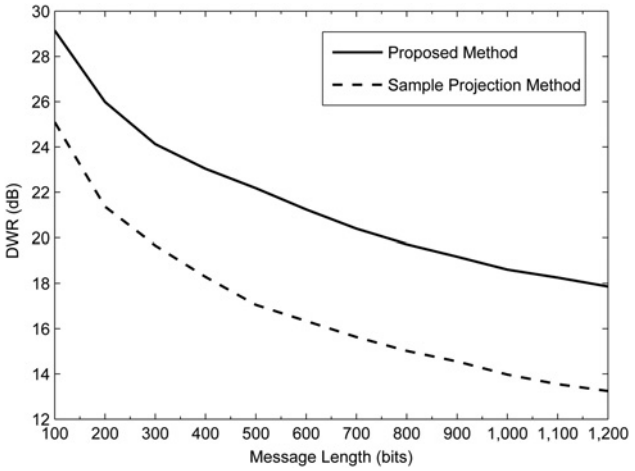

Fig. 5 *Comparing DWR for the proposed method and the sample projection approach [22] with the same condition [DNR = 18 dB and BER = 11(%)]*

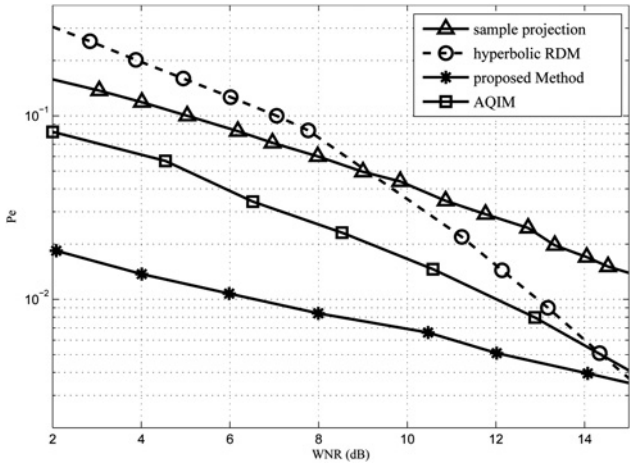

Fig. 6 *Empirical values of the error probability for a power-law attack with $\lambda = 0.7$ and $\gamma = 1.2$ (DWR = 25 dB)*

5.2 Simulation on real images

In this subsection, we present some experimental results on the grey-scale images. The results are reported for 512 × 512 pixel standard test images: Lena, Goldhill, Bridge and Peppers. In Table 1, peak signal to noise ratio (PSNR) and bit error rate (BER) (%) for AWGN with a 128-bit watermark for several well-known wavelet basis functions shown. We have used Symlets family which shows the best compromise between the imperceptibility and robustness. Moreover, we experimentally found that Daubechies length-8 Symlets (sym8) have the best results in this family which have the best results in our work with two levels of decomposition to compute the 2D DWT. These images are partitioned into 16 × 16 blocks, then the second level approximation coefficients of each block is considered for a watermark bit insertion. The results are also obtained by averaging over 100 runs with 100 different pseudo-random binary watermarks. The PSNR values for the proposed method are obtained as 43.45, 45.12, 43.20 and 42.71 dB, respectively, with a 128-bit watermark embedded. The original and watermarked images are shown in Fig. 7. Note that other image transforms which their coefficients can be well approximated by a Gaussian distribution can be used in our method. Here, we have not studied all the image filters

1. AWGN attack: Fig. 8 shows the robustness of the proposed method against AWGN attack. The BER (%) results are depicted against different noise standard deviations for four standard test images.
2. Lossy JPEG compression: We have studied robustness of the proposed method against JPEG lossy compression which is the most common compression scheme for image data. For this aim, the watermarked images are compressed by different quality factors. Then the watermarked data is extracted from the compressed watermarked images. As demonstrated in Fig. 9, the proposed method is robust to this attack. This is because of embedding the watermark in the low frequency components of the image blocks.
3. Cropping, scaling and rotation: In this experiment, we investigate the effect of editing attacks such as 5 and 10% cropping, scaling by factor 0.5, 0.75 and 1.5, and rotation where each test image is rotated by −10°, −5°, +5° and +10°. From Table 2, it can be seen that the proposed method is highly robust against these attacks.
4. The effect of the coding lines, block size and total capacity: In this part, we investigate the effect of changing the coding lines, block size and message length on the performance of the proposed algorithm. To this aim, we vary the block size from 8 to 32, and the number of blocks engaged; that is the message length from 128 to 1024. Also, we change the number of coding lines from 3 to 5. The results are summarised in Table 3 in terms of BER obtained by averaging over the four test images. The results on various modes indicating that while other block sizes and bit rates can be picked up based on the application, the case of 16 × 16 block size and 128 bit message length with three coding lines is the best compromise between the imperceptibility, capacity, and robustness.
5. Gain attack: Watermarking in the angle which is a gain-invariant domain makes the proposed method highly robust against the gain attack. To evaluate the proposed method against gain attack, we divide each watermarked image to non-overlapping segments. Then all the pixels in each block are multiplied by a variable gain factor $1 + w\delta$ where δ is a random variable uniformly distributed between 0 and 1, and w is a constant factor determining the strength of the attack. Table 4 shows performance of the proposed method compared with [22] for different segment sizes and strengths of the attack w. According to [22] the watermark length is 128 bits in both methods and results are averaged over 100 test images. It can be seen that the proposed method outperforms the [22], except for segment size of 4 × 4. Furthermore, the results confirm that our method is invariant to the fixed gain attack where the segment size is 16 × 16 in which the gain is constant in each embedding block.

Table 1 Effect of some well-known wavelet basis functions ON BER (%) UNDER AWGN with 128 bits watermark'

Wavelet filters	PSNR, dB	AWGN, ($\sigma = 10$)
Daubechies db1 or haar	45.10	16.95
Coiflets coif1	44.76	12.11
Symlets Sym2	43.51	8.67
Meyer	43.47	10.54
BiorSplines bior1.1	45.56	14.06
ReverseBior rbio1.1	45.12	14.45

5.3 Comparison with other watermarking methods

This section is dedicated to the comparisons with some of the well-known methods recently proposed. For a fair comparison, all the results are reported under the same condition. To this aim, the watermarked angle is adjusted such that the same PSNR values yield in the comparisons.

The first comparison is performed with Wang *et al.* [32] method and sample projection method [22]. The median and Gaussian filters are implemented using 3 × 3 windows. In Table 5, BER (%) results are reported for median filtering, Gaussian filtering, JPEG compression, rotation, scaling and AWGN attacks. To have a fair comparison, we decrease the angle between two consecutive coding lines in [22] to have approximately the same PSNR. As can be observed from the table, the proposed method outperforms [32] for all the studied attacks, except for the AWGN one. Despite having the same message length, 256 bits, in three

doi: 10.1049/iet-ipr.2013.0386

Fig. 7 *Original (left column) and watermarked (centre and right columns) test images*

Top–bottom: Lena, Goldhill, Bridge and Peppers, with a 128-bit watermark embedded (the image in the centre) and PSNR = 43.45, 45.12, 43.20 and 42.71 dB and with 1024-bit watermark embedded (right column) and PSNR = 40.17, 40.90, 36.87 and 38.79 dB top to bottom

methods, the PSNR of our method is slightly better than Wang *et al.*'s method and considerably better than [22]. Akhaee *et al.*'s method [22] is superior to the proposed scheme for the scaling attack.

Afterwards, we make a comparison with the vector LQIM [21] which uses non-uniform quantisation and sphere-hardening dither modulation (SHDM) [33] which utilises uniform quantisation levels. 'Lena' standard image of size 512 × 512 is used in the schemes. As was mentioned earlier, in order to have similar perceptual quality the parameters are set in a way that PSNR = 45.7 dB with 128 bits watermark. Table 6 gives the BER (%) results of the proposed method with [21, 33] against various noise variances after AWGN attack and median filtering. According to the table results, the proposed method has the best performance at high noise variances.

Then, we compared the mean structural similarity index (MSSIM) with [22, 32] for various message length from 128 to 1024. The results are summarised in Table 7 by averaging over ten test images for block size of 16 × 16.

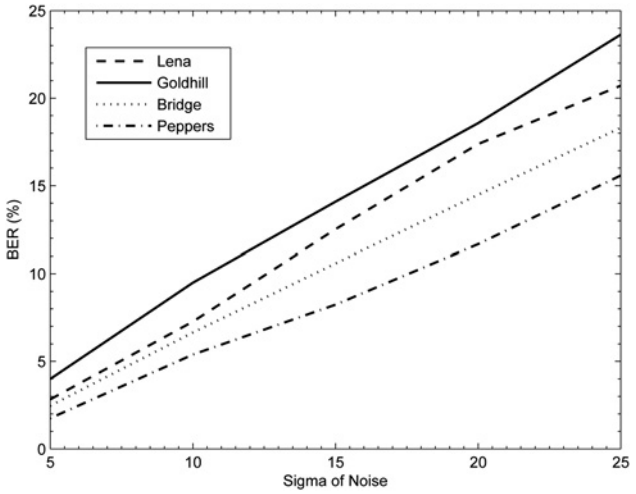

Fig. 8 *AWGN attack for various noise variances*

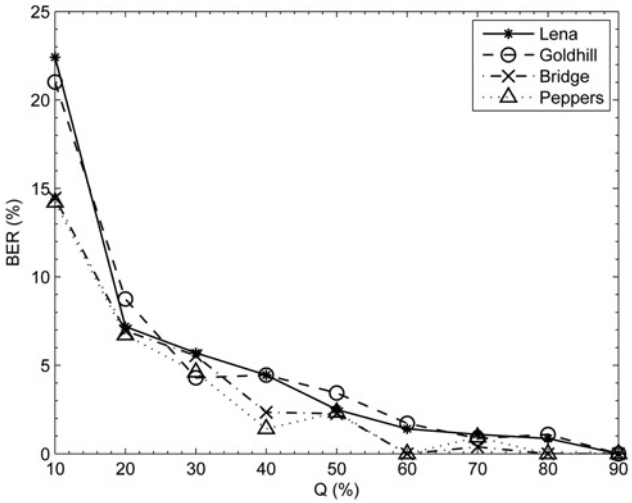

Fig. 9 *BER against various quality factors (Q) for JPEG compression*

Finally, we demonstrate the performance of the proposed method against improved multiplicative spread spectrum (IMSS) method [34], vector LQIM [21] and SHDM [33] under JPEG compression. As in [34], for each host image, we embed 4096 bits. In this regard, we have used real

Table 2 BER (%) results of extracted watermark under cropping, scaling and rotation attacks

Image	Cropping		Scaling			Rotation			
	5%	10%	0.5	0.75	1.5	– 10	– 5	5	10
Lena	1.83	5.92	4.81	2.06	0.44	6.16	5.39	4.38	4.78
Goldhill	2.84	6.53	4.59	0.86	0	4.16	4.50	3.04	4.06
Bridge	4.63	13.42	5.02	1.02	0.39	9.31	7.02	7.06	9.23
Peppers	6.58	10.48	1.78	0	0	5.64	4.72	5.84	6.55

Table 3 BER (%) results of extracted watermark under cropping, scaling and rotation attacks

Blk. size	Bits	PSNR, dB	JPEG 20%	AWGN 10	Gaus. 3 × 3	CROP 5%	Scale 0.75	Rot. + 5
Number of coding lines = 3								
16 × 16	128	43.21	8.01	7.97	4.72	4.06	0.88	4.77
16 × 16	256	40.21	10.31	9.53	4.87	4.76	0.67	5.40
16 × 16	512	37.41	14.98	13.31	6.31	4.82	0.79	6.62
16 × 16	1024	37.64	24.92	23.08	8.08	5.99	1.24	7.97
32 × 32	128	48.22	20.98	19.04	4.79	6.56	0.57	6.31
32 × 32	256	47.92	27.24	26.10	5.58	9.01	0.80	7.09
Number of coding lines = 5								
16 × 16	128	43.52	12.23	12.52	5.82	4.28	0.70	4.80
16 × 16	256	43.39	15.23	15.21	6.95	4.67	0.69	5.26
16 × 16	512	41.21	21.88	21.14	7.92	5.25	0.79	6.33
16 × 16	1024	40.42	30.75	30.13	10.69	6.23	1.12	7.97
32 × 32	128	48.11	26.88	26.47	6.95	7.17	0.25	6.05
32 × 32	256	48.34	33.49	34.01	7.54	8.54	0.27	7.41

Table 4 BER (%) comparison between the proposed method and Akhaee *et al.* [22] under variable gain attack (message length = 128 bits)

Segment Size	*w*							
	0.05		0.1		0.2		0.25	
	Pro	Akhaee *et al.* [22]	Pro	Akhaee *et al.* [22]	Pro	Akhaee *et al.* [22]	Pro	Akhaee *et al.* [22]
4 × 4	1.21	0.83	2.85	2.17	7.44	5.88	9.92	7.54
8 × 8	1.78	2.24	4.63	5.62	10.06	10.71	12.59	13.43
16 × 16	0	0	0	0	0	0	0	0

doi: 10.1049/iet-ipr.2013.0386

Table 5 BER comparison between the proposed method, [22, 32] under different types of attacks (message length = 256 bits)

Image	Method	PSNR	Median filter 3 × 3	Gaus. 3 × 3	JPEG $Q = 11$	AWGN $\delta^2 = 10$	Rot. + 5	Scale 0.75
Peppers	proposed	40.69	4.41	3.55	18.4	1.87	5.74	0.23
	Wang *et al.* [32]	42	29.35	27.21	26.10	1.25	9.45	1.12
	Akhaee *et al.* [22]	38.70	15.63	8.59	27.38	3.16	6.84	0.43
Baboon	proposed	43.75	15.14	9.80	15.08	1.09	10.58	1.25
	Wang *et al.* [32]	42	31.65	28.14	16.95	1.3	16.24	2.24
	Akhaee *et al.* [22]	43.90	33.63	17.58	30.27	6.25	12.11	1.13
Barbara	proposed	42.69	15.82	8.71	24.1	4.48	7.30	2.50
	Wang *et al.* [32]	42	24.95	22.74	16.45	1.45	13.18	3.56
	Akhaee *et al.* [22]	41.14	24.49	9.34	29.88	7.15	9.61	1.41
Lena	proposed	42	6.25	4.73	24.96	3.34	4.92	0.94
	Wang *et al.* [32]	42	30.80	25.26	29.80	1.45	10.12	1.52
	Akhaee *et al.* [22]	39.36	16.56	8.20	30.82	6.64	7.73	0.63

Table 6 BER (%) of watermark extraction under AWGN attack for various noise variances and median filtering attack

Method	AWGN(σ)							Median 3 × 3	PSNR, dB
	5	7.5	10	15	20	25	30		
Balado [33]	0	3.29	8.91	16.46	38.91	54.93	64.12	5.46	45.7
Vector LQIM [21]	0.27	6.03	8.50	14.27	29.20	40.58	52.08	5.39	45.7
proposed	3.34	5.87	8.23	13.84	18.45	23.58	27.52	4.12	45.7

128 bits have been embedded within *Lena* image in three methods where PSNR = 45.7 db.

Table 7 Comparison between our watermarking method, [22, 32]: MSSIM for different message length (bits)

Method	Message length, bits			
	128	256	512	1024
proposed (three coding lines)	0.9980	0.9962	0.9931	0.9899
proposed (five coding lines)	0.9994	0.9988	0.9978	0.9968
Akhaee *et al.* [22]	0.9983	0.9965	0.9932	0.9913
Wang *et al.* [32]	0.9979	0.9968	0.9922	0.9911

images of size 1024 × 1024 with block size of 16 × 16 where one bit is inserted in each block. Table 8 shows the BER (%) for different quality factors. It can be seen not only the performance of the proposed method is better than IMSS method, but also the proposed method has better PSNR about 1 dB from IMSS method. According to Table 8, [33, 21] outperform our method under the studied attack.

6 Conclusion

A robust watermarking technique in the wavelet domain is proposed. Each pair of samples is considered as points in 2D space and by defining a line segment for each two points, the angle between two line segments is regarded for data hiding. Thus, each eight samples of the approximation coefficients of image blocks provided us one bit watermark insertion. In order to embed the watermark, the angle between two lines is quantised to the specified angle. The quantisation is done by adjusting coordinates of the points. Then, by projection of samples on the specific code lines, watermarked samples are reproduced. To be robust against the noise and compression attacks, the algorithm is applied on the low frequency components of the image blocks. Our motivation to employ the angle between two line segments for data embedding is to be invariant to the gain attack. Moreover, we propose ML detector to extract the watermark in the noisy channel. To this aim, the distribution of the noisy watermarked samples is estimated in the receiver side. In comparison with other state-of-the-art watermarking techniques which is quantisation-based and invariant to the volumetric gain attack, the proposed method has higher robustness in most cases. This issue has been verified via extensive simulations. Our future work may be focused on performance of the proposed method on other image filters.

7 References

1 Wu, M., Liu, B.: 'Data hiding in image and video. i. Fundamental issues and solutions', *IEEE Trans. Image Process.*, 2003, **12**, (6), pp. 685–695

2 Moulin, P., Koetter, R.: 'Data hiding codes', *Proc. IEEE*, 2005, **93**, (12), pp. 2083–2126

Table 8 Average BER (%) for the IMSS [34], Vector LQIM [21], Balado[33] and the proposed schemes under JPEG compression with various quality factors when applied on 100 real images (message length = 4096 bits)

Method	Quality factor (Q)										PSNR, dB
	10	15	25	35	45	55	65	75	85	95	
IMSS [34]	52.22	48.17	38.41	29.73	17.65	10.12	8.69	6.5	4.5	2.3	37
Vector LQIM [21]	36.83	33.57	31.90	17.38	7.14	3.92	2.02	0.71	0.35	0.23	38
Balado [33]	39.24	35.76	32.41	22.66	10.11	7.06	5.33	2.15	1.98	0.44	38
proposed	46.74	41.52	32.20	17.44	13.48	9.83	8.23	5.13	3.76	1.52	38

3 Chen, B., Wornell, G.: 'Quantization index modulation: a class of provably good methods for digital watermarking and information embedding', *IEEE Trans. Inf. Theory*, 2001, **47**, (4), pp. 1423–1443
4 Kundur, D., Hatzinakos, D.: 'Diversity and attack characterization for improved robust watermarking', *IEEE Trans. Signal Process.*, 2001, **49**, (10), pp. 2383–2396
5 Cox, I., Kilian, J., Leighton, F., Shamoon, T.: 'Secure spread spectrum watermarking for multimedia', *IEEE Trans. Image Process.*, 1997, **6**, (12), pp. 1673–1687
6 Podilchuk, C.I., Zeng, W.: 'Image-adaptive watermarking using visual models', *IEEE J. Sel. Areas Commun.*, 1998, **16**, (4), pp. 525–539
7 Kuribayashi, M.: 'Interference removal operation for spread spectrum fingerprinting scheme', *IEEE Trans. Inf. Forensics Secur.*, 2012, **7**, (2), pp. 403–417
8 Oostveen, J.C., Kalker, T., Staring, M., Delp, E.J., Wong, E.P.W.: 'Adaptive quantization watermarking'. Proc. SPIE Security Watermarking Multimedia Contents, San Jose, CA, June 2004, vol. 5306, pp. 296–303
9 Li, Q., Cox, I.: 'Using perceptual models to improve fidelity and provide resistance to volumetric scaling for quantization index modulation watermarking', *IEEE Trans. Inf. Forensics Secur.*, 2007, **2**, (2), pp. 127–139
10 Perez-Gonzalez, F., Mosquera, C.: 'Quantization-based data hiding robust to linear-time-invariant filtering', *IEEE Trans. Inf. Forensics Secur.*, 2008, **3**, (2), pp. 137–152
11 Guccione, P., Scagliola, M.: 'Hyperbolic rdm for nonlinear valumetric distortions', *IEEE Trans. Inf. Forensics Secur.*, 2009, **4**, (1), pp. 25–35
12 Akhaee, M., Amini, A., Ghorbani, G., Marvasti, F.: 'A solution to gain attack on watermarking systems: logarithmic homogeneous rational dither modulation'. Proc. 2010 IEEE Int. Conf. Acoustics Speech and Signal Processing (ICASSP), March 2010, pp. 1746–1749
13 Eggers, J., Buml, R., Girod, B.: 'Estimation of amplitude modifications before scs watermark detection'. Proc. SPIE: Security Watermarking Multimedia Contents IV, January 2002, vol. 4675, pp. 387–398
14 Costa, M.: 'Writing on dirty paper (corresp.)', *IEEE Trans. Inf. Theory*, 1983, **29**, (3), pp. 439–441
15 Lee, K., Kim, D., Kim, T., *et al.*: 'Em estimation of scale factor for quantization-based audio watermarking'. Proc. Second Int. Workshop Digital Watermarking, Seoul, Korea, October 2003, pp. 316–327
16 Shterev, I., Lagendijk, R.: 'Amplitude scale estimation for quantization-based watermarking', *IEEE Trans. Signal Process.*, 2006, **54**, (11), pp. 4146–4155
17 Miller, M., Doerr, G., Cox, I.: 'Applying informed coding and embedding to design a robust high-capacity watermark', *IEEE Trans. Image Process.*, 2004, **13**, (6), pp. 792–807
18 Conway, J.H., Sloane, N.J.A., Bannai, E.: 'Sphere-packings, lattices, and groups' (New York, NY, USA, Springer-Verlag New York, Inc., 1998)
19 Ramanjaneyulu, K., Rajarajeswari, K.: 'Wavelet-based oblivious image watermarking scheme using genetic algorithm', *IET Image Process.*, 2012, **6**, (4), pp. 364–373
20 Bhatnagar, G., Raman, B., Wu, Q.M.J.: 'Robust watermarking using fractional wavelet packet transform', *IET Image Process.*, 2012, **6**, (4), pp. 386–397
21 Kalantari, N., Ahadi, S.: 'A logarithmic quantization index modulation for perceptually better data hiding', *IEEE Trans. Image Process.*, 2010, **19**, (6), pp. 1504–1517
22 Akhaee, M., Sahraeian, S., Jin, C.: 'Blind image watermarking using a sample projection approach', *IEEE Trans. Inf. Forensics Secur.*, 2011, **6**, (3), pp. 883–893
23 Nasir, I., Khelifi, F., Jiang, J., IPSON, S.: 'Robust image watermarking via geometrically invariant feature points and image normalisation', *IET Image Process.*, 2012, **6**, (4), pp. 354–363
24 Nezhadarya, E., Wang, Z.J., Ward, R.K.: 'Robust image watermarking based on multiscale gradient direction quantization', *IEEE Trans. Inf. Forensics Secur.*, 2011, **6**, (4), pp. 1200–1213
25 Phadikara, A., Maity, S.P., Verma, B.: 'Region based qim digital watermarking scheme for image database in dct domain', *Comput. Electr. Eng.*, 2011, **37**, (3), pp. 339–355
26 Perez-Gonzalez, F., Mosquera, C., Barni, M., Abrardo, A.: 'Rational dither modulation: a high-rate data-hiding method invariant to gain attacks', *IEEE Trans. Signal Process.*, 2005, **53**, (10), pp. 3960–3975
27 Massey, F.J.: 'The Kolmogorov-Smirnov test for goodness of fit', *J. Am. Stat. Assoc.*, 1951, **46**, (253), pp. 68–78
28 Marsaglia, G., Tsang, W., Wang, J.: 'Evaluating Kolmogorov's distribution', *J. Stat. Softw.*, 2003, **8**, (18), pp. 1–4
29 Akhaee, M., Sahraeian, S., Sankur, B., Marvasti, F.: 'Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor', *IEEE Trans. Multimed.*, 2009, **11**, (5), pp. 822–833
30 Ware, R., Lad, F.: 'Approximating the distribution for sum of product of normal variables', 2003. Available at: http://www.math.canterbury.ac.nz/research/ucdms2003n15.pdf = 0pt
31 Ourique, F., Licks, V., Jordan, R., Perez-Gonzalez, F.: 'Angle qim: a novel watermark embedding scheme robust against amplitude scaling distortions'. Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 2005 (ICASSP '05), March 2005, vol. 2, pp. 797–800
32 Wang, Y., Doherty, J., Van Dyck, R.: 'A wavelet-based watermarking algorithm for ownership verification of digital images', *IEEE Trans. Image Process.*, 2002, **11**, (2), pp. 77–88
33 Balado, F.: 'New geometric analysis of spread-spectrum data hiding with repetition coding, with implications for side-informed schemes'. Proc. IWDW, Siena, Italy, September 2005, vol. 4675, p. 336350
34 Valizadeh, A., Wang, Z.: 'An improved multiplicative spread spectrum embedding scheme for data hiding', *IEEE Trans. Inf. Forensics Secur.*, 2012, **7**, (4), pp. 1127–1143

doi: 10.1049/iet-ipr.2013.0386