Normalized blind STDM watermarking scheme for images and PDF documents robust against fixed gain attack

Makram Hatoum, Rony Darazi, Jean-François Couchot

Noname manuscript No.
(will be inserted by the editor)

Normalized Blind STDM Watermarking Scheme for Images and PDF Documents robust against Fixed Gain Attack

Makram W. Hatoum[1], **Rony Darazi**[2] **and**
Jean-François Couchot[1]

Received: date / Accepted: date

Abstract Spread Transform Dither Modulation (STDM), a special case of Quantization Index Modulation (QIM), has been widely used in digital watermarking. STDM has good performance in robustness against re-quantization and random noise attacks, but it is largely vulnerable to the Fixed Gain Attack (FGA). In addition to digital images and videos watermarking applications, copyright protection for digital text such as Portable Document Format (PDF) has received particular attention and interest. In this paper, we modify the STDM watermarking scheme by making the quantization step dependent on the original samples during the embedding process and on the watermarked samples during the decoding process to resist the FGA attack and enhance the robustness against the Additive White Gaussian Noise (AWGN) attack and JPEG compression attack in both the spatial domain and frequency domain regardless of the source of elements used as cover work. Experimentations have been conducted distinctly on digital images and text PDF documents. The tested images were watermarked with a uniform fidelity, where SSIM is fixed to 0.982 and 0.953. Our approach achieves significant robustness against the FGA attack with an improvement of 98% in terms of Bit Error Rates (BER) compared to traditional STDM. As for the AWGN attack, an improvement of 21% is shown. The proposed method also presents robustness against a variety of filtering and geometric attacks, while preserving a high level of transparency.

Keywords Digital watermarking, Data hiding, Portable Document Format, Robustness

M. W. Hatoum and J.F. Couchot
FEMTO-ST Institute, University of Bourgogne Franche-Comté, UMR 6174 CNRS, France. www.univ-fcomte.fr
E-mail: makram.hatoum@univ-fcomte.fr, jean-francois.couchot@univ-fcomte.fr

R. Darazi
TICKET Lab, Antonine University, Hadat-Baabda, Lebanon. www.ua.edu.lb
E-mail: rony.darazi@ua.edu.lb

1 Introduction

Nowadays, digital contents such as images, videos, and documents are getting more and more commonly distributed over the internet than before with increasing size and values. With the advancement of internet technologies, unauthorized users authenticate, duplicate and distribute digital contents in an illegal way. Therefore, digital watermarking was used for copyright protection, access control, authentication, and broadcast monitoring [6, 9, 20, 23, 31].
The watermarking schemes are categorized as a substitutive class known by Quantization Index Modulation (QIM) introduced by Chen and Wornell [8] and an additive class known by Spread Spectrum (SS) which was introduced by Cox et al. [10, 11, 28]. Part of the mentioned algorithms was performed in the spatial domain, where the watermark is embedded, for example, in the pixel intensity of an image or the character position in a text, while other watermarking algorithms were performed in the frequency domain using the DCT, DFT, DWT, and SVD [2, 18, 37], where the watermark is embedded in the frequency transform of the image.
Spread Transform Dither Modulation (STDM), a special case of Quantization Index Modulation (QIM), has been widely used for digital image watermarking, and in previous work we have applied the STDM watermarking scheme in PDF documents for copyright protection with a tradeoff between the transparency and robustness [4]. STDM achieves high robustness against additive noise attack, but it is largely vulnerable to the FGA attack [16]. In this type of attack, the received signal is indeed multiplied by a gain factor ρ, which scales the watermark vector and shifts it away from its original quantization cell. Therefore, the decoded watermark would be different from the embedded one. In this paper, we modify the STDM watermarking scheme to resist the FGA attack, to enhance the robustness against other types of attacks such as AWGN attack and JPEG compression, and improve its effectiveness for images and PDF documents.

2 Related Work

Below are a number of presented solutions that have been proposed using perceptual models based on Watson's model [36] to improve the fidelity and to provide robustness against the FGA attack. Watson provided a perceptual model for computing the slack associated with each DCT coefficient within an 8×8 block. These slacks are further used in watermarking schemes to determine the quantization step size during the embedding and decoding process.
Li *et al.* [25] have modified the QIM watermarking scheme based on Watson's perceptual model. They applied the DCT on the original image, in order to compute the quantization step size Δ based on the slacks, which are evaluated by:

$$s[i,j,k] = max(t_L[i,j,k], |C_0[i,j,k]|^{0.7} t_L[i,j,k]^{0.3}), \tag{1}$$

In the equation above, $C_0[i,j,k]$ is the coefficient at the position (i,j) of the k^{th} block of the cover work, and $t_L[i,j,k]$ is the luminance masked threshold given as:

$$t_L[i,j,k] = t[i,j](C_0[0,0,k]/C_{0,0})^{0.649}, \tag{2}$$

where $C_0[0,0,k]$ is the DC coefficient of the k^{th} block, $C_{0,0}$ is the average of all the DC coefficient in the image, and $t[i,j]$ is the smallest magnitude of the corresponding DCT coefficient in a block presented in a frequency sensitive table [9]. Δ is modified based on the slacks and a constant factor G, which can be adjusted to alter the watermark strength. This method ameliorates the robustness against the FGA attack, but still vulnerable against AWGN attack and misses the experiments against varieties of attacks such as JPEG compression.
Zhu, X. [39] introduced an image-adaptive STDM performed in the DCT domain in order to resist the FGA attack. In this method, Δ is computed based on Watson's model during the embedding process as:

$$\Delta = 2L^{-\frac{1}{4}} D \sum_{l=1}^{L} s_l. \tag{3}$$

D is the perceptual distance between the watermarked signal and the host signal, and the slack s_l is computed using the contrast making presented in (1) at the position (i,j) of the k^{th} block. The slacks s have been rearranged in a vector of length L to compute Δ. During the detection process, Δ is modified as:

$$\hat{\Delta} = \Delta \frac{C'_{0,0}}{C_{0,0}},$$

where $C_{0,0}$ and $C'_{0,0}$ are the mean of all the DC coefficients of the original and watermarked image. This method is not robust against JPEG compression and low-pass filtering as all the DCT coefficients were used to embed the watermark.
In [26], Li *et al.* proposed the STDM-MW-SS watermarking scheme in order to provide invariance to the FGA attack while improving the fidelity constraint. The DCT transform is applied to the original image, and the slacks of each 8×8 block are computed based on Watson's model to determine the projection vector and the quantization step size Δ. Given a length L vector of DCT coefficients and its corresponding vector of modified slacks, Δ is computed as follows:

$$\Delta = G_f \times \sum_{l=1}^{L} S_l^M. \tag{4}$$

G_f is a global factor used to adjust the watermarking strength, and S_l^M is the modified slack at the position (i,j) of the k^{th} block, computed as follows:

$$S^M[i,j,k] = max(t_L^M[i,j,k], |C_0[i,j,k]|^{0.7} t_L^M[i,j,k]^{0.3})$$

$$t_L^M[i,j,k] = t_L[i,j,k](C_{0,0}/128),$$

This method has been tested only against JPEG compression and FGA attack.
Yu *et al.* [38] presented an Adaptive STDM (ASTDM) based on Watson's model. The slacks are computed during the embedding process as in (1), and the luminance masking is modified during the extraction process as:

$$t_L[i,j,k] = t[i,j] \left(\frac{C_0[0,0,k]}{C_{0,0}} \right)^{0.7} \left(\frac{C_{0,0}}{C'_{0,0}} \right),$$

Δ_i is computed for the i^{th} bit of the watermark as:

$$\Delta_i = 2\lambda|\bar{s}_i|\|k_i\|^2/|\bar{k}_i|,$$

where k_i is a private subvector, s_i presents a vector containing the slacks of the i^{th} 8×8 block, $\lambda \in (0, 1)$ is used to adjust the embedding strength, $|\bar{s}_i|$ and $|\bar{k}_i|$ are the absolute mean values of s_i and k_i, and $\|k_i\|^2$ is the l^2-norm of k_i. An extra intensity sequence of the image must be transmitted to the detector to provide resistance to FGA attack.

In the STDM-Step projection (STDM-SP) scheme that was proposed by Li *et al*. [27], Δ is selected for each host vector based on Watson's model, and performed in the DCT domain. The slack vector s of the host signal is projected into a random vector p. Δ is given as:

$$\Delta = 2s^T p,$$

in which s presents the slack vector of the host signal, and p is the positive projection vector. In this sense, the original image is divided into 8×8 blocks, and the DCT is performed to each block to form the slack vector S_i, based on the position of the host vector elements in the 8×8 block. STDM-SP-wm selects the slack from the frequency sensitivity table [9] which has been modified as:

$$T_m = T \times \frac{C_{0,0}}{\mu},$$

where $C_{0,0}$ is the mean intensity of the image and μ=512. This method was not examined with related work.

Wan *et al*. [34] proposed a Logarithmic STDM (LSTDM-WM) watermarking scheme based on the perceptual model. According to a logarithmic function, the projection of the host signal x onto a random vector p is transformed as:

$$F(x^T p) = \frac{ln(1 + \mu \frac{x^T p}{C_{0,0}})}{ln(1 + \mu)},$$

in which the parameter μ is selected based on:

$$\mu < \frac{C_{0,0}}{|x^T p|}.$$

Δ is modified as:

$$\Delta = \frac{ln(1 + 2s^T p \times \frac{\mu}{C_{0,0}})}{ln(1 + \mu)},$$

where s presents the distortion visibility thresholds which is calculated based on Watson's perceptual model. This method is complex.

Jiang *et al*. [21] proposed an adaptive spread transform QIM (ST-QIM) watermarking algorithm based on improved perceptual models. They proposed four different implementations of perceptual modal and combined it with ST-QIM to form an adaptive quantization watermarking schemes. Those methods were not compared with related works.

Wang *et al.* [35] presented an improved AQIM watermarking method with minimum-distortion angle quantization and amplitude projection strategy. They proposed a new angle quantization function, which is given by:

$$Q(\theta) = \begin{cases} \Delta\left\lfloor \dfrac{\theta + \dfrac{\Delta}{2}}{\Delta} \right\rfloor & \text{if } m = 0 \\ \Delta\left(\left\lfloor \dfrac{\theta}{\Delta} \right\rfloor + \dfrac{\Delta}{2} \right) & \text{if } m = 1 \end{cases},$$

where $\Delta = 2\pi/k$, and k is a positive integer number. This method is implemented in the wavelet transform domain of grayscale images.
In [33], Wan *et al.* proposed an improved logarithmic spread transform dither modulation using a robust perceptual model. They introduced a new measurement of the edge, strength, and pixel intensity to calculate the slacks at the watermark embedder and watermark detector. They make a new quantization step size as:

$$\Delta = \frac{ln(1 + \frac{2s^T p}{128})}{ln(1+\gamma)},$$

where γ is a positive parameter defining the compression level.
Those modified watermarking schemes are applied in the frequency domain and could only be implemented on images to resist the FGA attack since they are dependent on the luminance and contrast making of images. Most of the proposed methods are studied based on the DCT transform, *i.e.* the DCT coefficients are quantized rather than the pixel values.
A different watermarking scheme, Rational Dither Modulation (RDM), has been proposed by Perez-Gonzalez *et al.* [29] in which the feature signal for quantization is constructed using the ratio of the previously generated watermarked sample and the current host sample as:

$$y_k = g(y_{k-L}^{k-1}) Q_m \left(\frac{x_k}{g(y_{k-L}^{k-1})} \right), \tag{5}$$

where Q_m represents the standard quantization operation, y_{k-L}^{k-1} denotes the set of past signals (y_{k-L} ... y_{k-1}), and the function $g()$ has the property that for any gain factor $\rho > 0$:

$$g(\rho y) = \rho g(y).$$

The function $g()$ include the L_p vector-norm:

$$g(y_{k-L}^{k-1}) = \left(\frac{1}{L} \sum_{i=1}^{L} |y_{k-i}|^p \right)^{\frac{1}{p}}.$$

The decoding is performed by using the minimum euclidean distance rule as:

$$\hat{m} = arg \min_{m \in \{-1,1\}} \left| \frac{z_k}{g(z_{k-L}^{k-1})} - Q_m \left(\frac{z_k}{g(z_{k-L}^{k-1})} \right) \right|. \tag{6}$$

Whereas RDM has proved to be robust against the FGA attack, it still limited against the additive noise attack due to the variation of the quantization step size.

Aside from digital images, electronic documents such as PDF files are widely exchanged over the internet, and they are subject to illegal copying and redistribution due to the effortless copying and distributing. Therefore, it has become more important to protect PDF files from any malicious user [17]. Few methods are proposed for hiding information in PDF files. Castiglione *et al.* [7] noted that PDF documents are not immune to some privacy issues. It is possible in PDF document to retrieve the previous version and display information not meant to be published, and it is also possible to trigger events when a PDF document is opened or printed. Therefore, the scientific communities have to consider such issues that might disclose the fairness of the review process of scientific papers. In [14], Feng *et al.* conducted a series of studies of the privacy leakage issues of PDF documents. The hidden private information is revealed with documents, and that will provoke privacy leakage. This methodology is helpful for users to check whether their PDF documents include privacy information prior to transmitting it via the Internet. Vellasques *et al.* [32] presented an intelligent watermarking technique based on particle swarm optimization for bi-tonal (or binary) images. They intended a watermarking application of streams of documents images. The performance remains to be tested. Por *et al.* [30] proposed an approach in information hiding using inter-paragraph and inter-word spacing. The main drawback of this method is that the embedded message can be easily destroyed. Lee *et al.* [24] presented an alternative space coding method to embed a secret message in a PDF file. An opponent could easily remove or modify the embedded message by replacing the ASCII codes. Alizadeh *et al.* [1] proposed two different algorithms using a TJ method. One of them has a lower security level, and the other one has a lower capacity level. Kuribayash *et al.* [22] used the space lengths between characters as watermarking space, and the watermark is embedded using the DM-QIM watermarking scheme. This method still missing the experimental tests of robustness. In previous work [5], we proposed a blind digital watermarking scheme for PDF documents. This method consists of embedding the watermark in the x-coordinates of a group of characters, taking into consideration the transparency and robustness trade-off.

2.1 Contribution

Except for the RDM, all the watermarking schemes mentioned above are based on Watson's perceptual model to resist the FGA attack. Therefore, those methods are dedicated for image watermarking and could not be applied on other types of signal. As for the RDM watermarking scheme, it achieves a good performance against the FGA attack with a certain limitation against the additive noise attack. RDM does not benefit from the property of the spreading vector, and the quantization step size is a variable step quantizer, whose size is a function of several past watermarked samples. For that, the attacking noise has more influence on the decoding quantization step size.
In this paper, we modified the traditional STDM watermarking scheme by making the quantization step dependent on the original samples during the embedding

process and the watermarked samples during the decoding process to resist the FGA attack and enhance the robustness against AWGN attack, JPEG compression attack, and variety of filtering and geometric attacks. Moreover, we affirm that this approach could also be used as a blind watermarking scheme for PDF documents. We have applied our approach on the grayscale images and PDF documents in the spatial domain and frequency domain and compared its performance with other proposed methods. Our approach is more flexible as it is not dependent on the perceptual model to achieve the robustness against the FGA attack, and any element can be used as support to embed the watermark.
The rest of this paper is organized as follows: Section 3 recalls some backgrounds on STDM. The proposed N-STDM method is presented in Section 4. Section 5 provides a theoretical analysis of STDM and N-STDM. Experiments on real images are shown in Section 6. Section 7 presents the experiments on PDF documents. The findings and discussion are shown in Section 8. Finally, Section 9 provides our conclusion and future work.

3 Background

STDM [8, 12, 13] is a special case of QIM where the quantization occurs entirely in the projection of the host signal x onto a normalized projection vector p. This way, the embedding-induced distortion spreads into a group of samples rather than one. The embedded function is as follows:

$$\begin{aligned} y &= x + (Q_m(x^T p, \Delta) - x^T p)p \\ &= x + \left(round\left(\frac{x^T p - d_m}{\Delta} \right) \Delta + d_m - x^T p \right) p, \end{aligned} \tag{7}$$

where Δ represents the quantization factor, $round()$ is the rounding value to the nearest integer, and d_m denotes the dither level based on the message bit $m \in \{0, 1\}$:

$$d_0 = -\frac{\Delta}{4} \text{ and } d_1 = \frac{\Delta}{4}. \tag{8}$$

The detection can be performed with a minimum distance decoder to extract the embedded message as follows:

$$\hat{m} = arg \min_{m \in \{0,1\}} \mid y^T p - Q_m(y^T p, \Delta) \mid . \tag{9}$$

Therefore, it achieves high robustness against re-quantization attack and additive noise attack, yet it is still unsafe against the FGA attack. In this type of attack, the received signal is indeed multiplied by a gain factor ρ, which scales the watermark vector and shifts it away from its original quantization cell; More formally, when the FGA attack is applied on the watermarked signal y, it becomes:

$$z = \rho \cdot y,$$

and $\hat{m}$ will be decoded as follows:

$$\hat{m} = arg \min_{m \in \{0,1\}} \mid \rho \cdot y^T p - Q_m(\rho \cdot y^T p, \Delta) \mid .$$

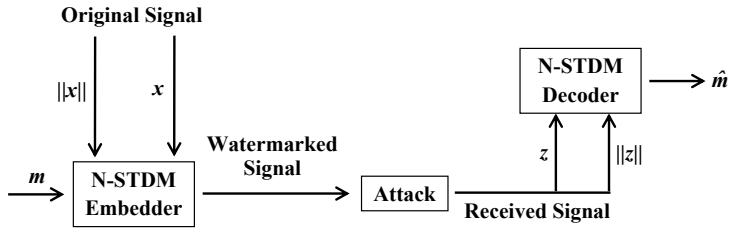


Fig. 1: Block diagram of the N-STDM watermarking scheme.

The quantification factor $Q_m(\rho \cdot y^T p, \Delta)$ is indeed equal to $round\left(\frac{\rho \cdot y^T p - d_m}{\Delta}\right)\Delta + d_m$ which may be different from $round\left(\frac{y^T p - d_m}{\Delta}\right)\rho \cdot \Delta + \rho \cdot dm$ and consequently not equal to $\rho \cdot Q_m(y^T p, \Delta)$. Therefore, as the decoded message can be different from the embedded one, the robustness against the FGA attack cannot be obtained. After analyzing the performance of STDM against the FGA attack and re-quantization attack, Bartolini *et al.* [3] concluded that STDM has more superior robustness against the re-quantization attack than the FGA attack. They argued that even though the values of gain factor ρ are close to 1, the error probability will still be excessively high.

4 Proposed N-STDM Method

The traditional STDM watermarking scheme has good performance in robustness against re-quantization and random noise attacks, but it is largely affected by the FGA attack. This is mainly due to the fact that when the host signal is scaled by the global factor ρ, the quantization step used for decoding is not scaled simultaneously. This problem will be solved if we scale the quantization step in the same way the watermarked signal is scaled. Obviously, it is difficult to straightforwardly estimate the global factor ρ, but if the quantization step size becomes dependent on the watermarked samples, it will be scaled concurrently with those samples. Therefore, in the proposed watermarking scheme, N-STDM, we have modified the embedding and decoding functions of the traditional STDM as illustrated in Fig. 1. We have computed the norm value $\|x\|$ based on the host signal to be used during the embedding process as:

$$y = x + \left(\|x\| Q_m\left(\frac{x^T p}{\|x\|}, \Delta\right) - x^T p\right) p \quad m \in \{0, 1\}. \tag{10}$$

$$\|x\| = (|x_1|^{\frac{1}{u}} + |x_2|^{\frac{1}{u}} + ... + |x_n|^{\frac{1}{u}})^u, \tag{11}$$

where n is the length of the extracted vector from the cover elements, $|x_n|$ is the absolute value of element x_n, and $\|x\|$ is a norm function that could be expressed as a l^2-norm when $u = 1/2$ and l^1-norm when $u = 1$ etc. (the influence of $\|x\|$ against the FGA attack while varying u is detailed in Section 6).

Algorithm 1 N-STDM Embedder

Input: I, m, p
I: Original image of size $n = N \times N$
m: Binary watermark of size $s = S \times S$
p: Normalized projection vector of length $L = n/s$

Choose Δ and u;
$j = 0$;
$X \leftarrow$ reshape $(I, n, 1)$;
$W \leftarrow$ reshape $(m, s, 1)$;

for $i = L + 1 : L : n + 1$ **do**
  j++;
  $w = W(j)$;
  $x = X(i - L : i - 1)$;
  $no =$ Power(Sum(Power$(x, 1/u)), u)$;
  q=Quantizer$(x^T p, w, \Delta)$;
  $y(i - L : i - 1) = x + (no * q - x^T p)p$;
end for
$Output = y^T$

The detection is performed with a minimum distance decoder to extract the embedded message as follows:

$$\hat{m} = \underset{m' \in \{0,1\}}{\arg\min} \left| \tilde{y} - \|y\| \, Q_{m'} \left(\frac{\tilde{y}}{\|y\|}, \Delta \right) \right|. \tag{12}$$

where

$$\tilde{y} = y^T p. \tag{13}$$

As a result, when performed, the FGA attack s.t. $z = \rho.y$ will not affect the minimum distance decoder :

$$\begin{aligned} \hat{m} &= arg \min_{m \in \{0,1\}} \mid \tilde{z} - \|z\| Q_m \left(\frac{\tilde{z}}{\|z\|}, \Delta \right) \mid \\ &= arg \min_{m \in \{0,1\}} \mid \rho \cdot \tilde{y} - \rho \cdot \|y\| Q_m \left(\frac{\rho \cdot \tilde{y}}{\rho \cdot \|y\|}, \Delta \right) \mid \\ &= arg \min_{m \in \{0,1\}} \mid \rho \left(\tilde{y} - \|y\| Q_m \left(\frac{\tilde{y}}{\|y\|}, \Delta \right) \right) \mid . \end{aligned} \tag{14}$$

Therefore, the non-linear impact of the ρ factor in the quantization is now linear and consequently will not affect the process of decoding the message.
Algorithm 1 details the embedding process of a watermark into an image using the proposed N-STDM. The complexity is directly proportional to n; order of growth is n. In a worst-case scenario, the statement will be executed n times. The time complexity is linear O(n).

5 Theoretical Analysis of STDM and N-STDM

This section provides a theoretical proof of the correction of the STDM and N-STDM watermarking schemes. In other words, we have verified that when a message is embedded into a host signal and when there is no attack, the message

would be extracted without any error.
The quantizer Q_m of the STDM watermarking scheme is given by:

$$Q_m(s, \Delta) = round\left(\frac{s - d_m}{\Delta}\right)\Delta + d_m, \tag{15}$$

where:

$$d_m = -\frac{\Delta}{4} + m.\frac{\Delta}{2}. \tag{16}$$

Let us first recall the definition of the rounding function.

$$round(x) = \begin{cases} \lfloor x + 0.5 \rfloor \text{ if } x \text{ is postive or null} \\ \lceil x - 0.5 \rceil \text{ otherwise} \end{cases}$$

In all what follows and without loss of generality, we consider $s - d_m$ to be positive. There exists $q_s \in \mathbb{N}$ and $r_s \in \mathbb{R}^+$, $0 \leq r_s < \Delta$ such that:

$$\begin{aligned} s - d_m + \frac{\Delta}{2} &= q_s\Delta + r_s, \text{ or equivalently} \\ s - r_s + \frac{\Delta}{2} &= q_s\Delta + d_m. \end{aligned} \tag{17}$$

In such a case,

$$\begin{aligned} Q_m(s, \Delta) = round\left(\frac{s - d_m}{\Delta}\right)\Delta + d_m &= q_s\Delta + d_m \\ &= s - r_s + \frac{\Delta}{2}. \end{aligned} \tag{18}$$

Let $m \in \{0, 1\}$ be the bit to be embedded into the host vector $x = (x_1, \ldots, x_n)$ with respect to the normalized projection vector $p = (p_1, \ldots, p_n)$ and a parameter Δ. Let y be the vector that contains the watermark.

5.1 Correction Proof of STDM

In the original STDM algorithm:

$$y = x + \left(Q_m(x^T p, \Delta) - x^T p\right) p$$

$$\hat{m} = \underset{m' \in \{0,1\}}{\arg\min} \left| y^T p - Q_{m'}\left(y^T p, \Delta\right)\right|,$$

thanks to eq. (18), $Q_m(x^T p, \Delta) = x^T p - r_{x^T p} + \frac{\Delta}{2}$ so that

$$y = x - (r_{x^T p})p + \frac{\Delta}{2}p,$$

this allows deducing

$$y^T p = x^T p - r_{x^T p} + \frac{\Delta}{2}.$$

Let us then evaluate $Q_{m'}\left(y^T p, \Delta\right) = Q_{m'}\left(x^T p - r_{x^T p} + \frac{\Delta}{2}, \Delta\right)$.
First of all:

$$\begin{aligned} Q_{m'}\left(x^T p - r_{x^T p} + \frac{\Delta}{2}, \Delta\right) &= Q_{m'}\left(q_{x^T p}\Delta + d_m, \Delta\right) \text{thanks to eq. (17)} \\ &= round\left(\frac{q_{x^T p}\Delta + d_m - d_{m'}}{\Delta}\right)\Delta + d_{m'} \\ &= round\left(\frac{q_{x^T p}\Delta + \frac{\Delta}{2}(m - m')}{\Delta}\right)\Delta + d_{m'} \\ &= round\left(q_{x^T p} + \frac{m - m'}{2}\right)\Delta + d_{m'} \end{aligned}$$

We then have

$$\begin{aligned} \hat{m} &= \underset{m' \in \{0,1\}}{\arg\min} \left| y^T p - Q_{m'}\left(y^T p, \Delta\right)\right| \\ &= \underset{m' \in \{0,1\}}{\arg\min} \left| x^T p - r_{x^T p} + \frac{\Delta}{2} - round\left(q_{x^T p} + \frac{m - m'}{2}\right)\Delta - d_{m'})\right| \\ &= \underset{m' \in \{0,1\}}{\arg\min} \left| q_{x^T p}\Delta + d_m - round\left(q_{x^T p} + \frac{m - m'}{2}\right)\Delta - d_{m'}\right| \\ &= \underset{m' \in \{0,1\}}{\arg\min} \left| \left(q_{x^T p} + \frac{m - m'}{2}\right)\Delta - round\left(q_{x^T p} + \frac{m - m'}{2}\right)\Delta\right| \\ &= \underset{m' \in \{0,1\}}{\arg\min} \left| \left(q_{x^T p} + \frac{m - m'}{2}\right) - round\left(q_{x^T p} + \frac{m - m'}{2}\right)\right| \end{aligned} \tag{19}$$

Therefore, we conclude that the extracted message $\hat{m}$ depends on m and m'. Obviously, if $m = m'$, we have to evaluate $q_{x^T p} - round(q_{x^T p})$ which is null since $q_{x^T p}$ is a natural number. Otherwise, *i.e.*, when m and m' are distinct, let us first suppose that $\frac{m - m'}{2} = 0.5$. In this case, $\left|q_{x^T p} + 0.5 - round(q_{x^T p} + 0.5)\right| = \left|q_{x^T p} + 0.5 - (q_{x^T p} + 1)\right| = 0.5$. The last case, *i.e*, when $\frac{m - m'}{2} = -0.5$ is similar and is thus omitted. The minimum value is thus obtained when $m = m'$. Without any attack, $\hat{m}$ is thus m.

5.2 Correction Proof of N-STDM

In the following equations, $\|.\|$ is consider as the norm of elements.

Theorem 1 *Let y be the watermarked host:*

$$y = x + \left(\|x\| Q_m\left(\frac{x^T p}{\|x\|}, \Delta\right) - x^T p\right) p.$$

Let $\hat{m}$ be the retrieved watermark bit, which is defined by:

$$\hat{m} = \underset{m' \in \{0,1\}}{\arg\min} \left| y^T p - \|y\| \, Q_{m'} \left(\frac{y^T p}{\|y\|}, \Delta \right) \right|. \tag{20}$$

Without any attack, $\hat{m}$ is the same as m.

Proof: First of all, let us identify $y^T p$:

$$\begin{aligned} y^T p &= \left(x + \left(\|x\| \, Q_m \left(\frac{x^T p}{\|x\|}, \Delta \right) - x^T p \right) p \right)^T p \\ &= x^T p + \left(\|x\| \, Q_m \left(\frac{x^T p}{\|x\|}, \Delta \right) - x^T p \right) p^T p. \end{aligned}$$

Since p is a normalized vector, $p^T p$ is 1. Thus,

$$\begin{aligned} y^T p &= \|x\| \, Q_m \left(\frac{x^T p}{\|x\|}, \Delta \right) \\ &= \|x\| \left(\frac{x^T p}{\|x\|} - r_{\frac{x^T p}{\|x\|}} + \frac{\Delta}{2} \right) \text{ thanks to eq. (18)} \\ &= \|x\| \left(q_{\frac{x^T p}{\|x\|}} \Delta + d_m \right) \\ &= x^T p - \|x\| \, . r_{\frac{x^T p}{\|x\|}} + \frac{\Delta}{2} \|x\| \end{aligned}$$

Hence,

$$y = x - \|x\| \, . r_{\frac{x^T p}{\|x\|}} . p + \frac{\Delta}{2} \|x\| \, . \tag{21}$$

Let us now evaluate $Q_{m'} \left(\frac{y^T p}{\|y\|}, \Delta \right)$.

$$Q_{m'} \left(\frac{y^T p}{\|y\|}, \Delta \right) = round \left(\frac{\frac{y^T p}{\|y\|} - d_{m'}}{\Delta} \right) \Delta + d_{m'}$$

$$= round\left(\frac{x^T p - \|x\| \cdot r_{\frac{x^T p}{\|x\|}} + \frac{\Delta}{2}\|x\|}{\frac{\frac{x^T p}{\|x\|}}{\|y\|} - d_{m'}}{\Delta}\right)\Delta + d_{m'}$$

$$= round\left(\frac{\|x\|\,(q_{\frac{x^T p}{\|x\|}}\Delta + d_m)}{\frac{\frac{x^T p}{\|x\|}}{\|y\|} - d_{m'}}{\Delta}\right)\Delta + d_{m'}$$

$$= round\left(\frac{\|x\|\, q_{\frac{x^T p}{\|x\|}}\Delta + \|x\|\, d_m - \|y\|\, d_{m'}}{\Delta\,\|y\|}\right)\Delta + d_{m'}$$

$$= round\left(\frac{\|x\|\, q_{\frac{x^T p}{\|x\|}}\Delta + \|x\|\,\frac{\Delta}{4}(2m-1) - \|y\|\,\frac{\Delta}{4}(2m'-1)}{\Delta\,\|y\|}\right)\Delta + \frac{\Delta}{4}(2m'-1)$$

$$= round\left(\frac{\|x\|\, q_{\frac{x^T p}{\|x\|}} + \|x\|\,\frac{2m-1}{4} - \|y\|\,\frac{2m'-1}{4}}{\|y\|}\right)\Delta + \frac{\Delta}{4}(2m'-1)$$

$$= round\left(\frac{\|x\|}{\|y\|} q_{\frac{x^T p}{\|x\|}} + \frac{\|x\|}{\|y\|}\,\frac{2m-1}{4} - \frac{2m'-1}{4}\right)\Delta + \frac{\Delta}{4}(2m'-1).$$

Let's go back to the definition (20) of $\hat{m}$ which becomes:

$$\begin{aligned}
\hat{m} = \underset{m' \in \{0,1\}}{\arg\min} \Bigg| & \|x\| \left(q_{\frac{x^T p}{\|x\|}} \Delta + \frac{\Delta}{4}(2m-1) \right) \\
& - \|y\| \left(round \left(\frac{\|x\|}{\|y\|} q_{\frac{x^T p}{\|x\|}} + \frac{\|x\|}{\|y\|} \frac{2m-1}{4} - \frac{2m'-1}{4} \right) \Delta + \frac{\Delta}{4}(2m'-1) \right) \Bigg| \\
= \underset{m' \in \{0,1\}}{\arg\min} \Bigg| & \|x\| \left(q_{\frac{x^T p}{\|x\|}} + \frac{2m-1}{4} \right) \\
& - \|y\| \left(round \left(\frac{\|x\|}{\|y\|} q_{\frac{x^T p}{\|x\|}} + \frac{\|x\|}{\|y\|} \frac{2m-1}{4} - \frac{2m'-1}{4} \right) + \frac{2m'-1}{4} \right) \Bigg| \\
= \underset{m' \in \{0,1\}}{\arg\min} \Bigg| & \frac{\|x\|}{\|y\|} . q_{\frac{x^T p}{\|x\|}} + \frac{\|x\|}{\|y\|} . \frac{2m-1}{4} - \frac{2m'-1}{4} \\
& - round \left(\frac{\|x\|}{\|y\|} q_{\frac{x^T p}{\|x\|}} + \frac{\|x\|}{\|y\|} \frac{2m-1}{4} - \frac{2m'-1}{4} \right) \Bigg| .
\end{aligned}$$

One can first notice that what is inside the absolute value is close to 0 since it has the form $X - round(X)$, where $X \in \mathbb{R}$.

Let us now evaluate $\frac{\|x\|}{\|y\|}$. Thanks to (21), we have:

$$\begin{aligned}
\|y\| &\leq \|x\| + \|x\| . r_{\frac{x^T p}{\|x\|}} . \|p\| + \frac{\Delta}{2} \|x\| \\
&\leq \|x\| \left(1 + r_{\frac{x^T p}{\|x\|}} + \frac{\Delta}{2} \right) \\
&\leq \|x\| \left(1 + \frac{3\Delta}{2} \right) .
\end{aligned}$$

In all what follows, x and p are supposed to only have postive or null values and Δ is assumed to be less than 2.
Again, thanks to (21),

$$y_i = x_i - \|x\| . r_{\frac{x^T p}{\|x\|}} . p_i + \frac{\Delta}{2} \|x\| . p_i$$

$$y_i > x_i - \|x\| .\Delta.p_i + \frac{\Delta}{2} \|x\| .p_i \text{ since } r < \Delta$$

$$y_i > x_i - \frac{\Delta}{2} \|x\| .p_i \text{ which is postive if } \Delta \text{ is sufficently small.}$$

Thus

$$\begin{aligned} \|y\| &\geq \left\| x - \frac{\Delta}{2} \|x\| .p \right\| \\ &\geq \|x\| \left(1 - \frac{\Delta}{2}\right). \end{aligned}$$

Finally,

$$\frac{2}{2+3\Delta} \leq \frac{\|x\|}{\|y\|} \leq \frac{2}{2-\Delta}, \text{ for } \Delta < 2 \text{ sufficiently small.} \tag{22}$$

Next, if Δ is tiny, then r_s is too; consequently, q_s will have a very large value. Equation (21) implies that y (resp. $\|y\|$) is close to x (resp. $\|x\|$). In this context, $\frac{\|x\|}{\|y\|} . q_{\frac{x^T p}{\|x\|}}$ is significantly larger than $\frac{\|x\|}{\|y\|} . \frac{2m-1}{4} - \frac{2m'-1}{4}$.

In this sense, when m and m' are equal, $\frac{\|x\|}{\|y\|} . \frac{2m-1}{4} - \frac{2m'-1}{4}$ is close to 0; therefore, the $round()$ value will be close to the $round()$ value of $\frac{\|x\|}{\|y\|} . q_{\frac{x^T p}{\|x\|}}$ and the global result will be close to 0, but when m and m' are distinct, $\frac{\|x\|}{\|y\|} . \frac{2m-1}{4} - \frac{2m'-1}{4}$ is close to ± 0.5. In this situation, the $round()$ value may be significantly different.

As shown in subsections 5.1 and 5.2, the extracted message $\hat{m}$ depends on m and m'; without any attack, $\hat{m}$ will be the same as m.

If we perform the FGA attack s.t. $z = \rho.y$ on the tradional STDM watermarking scheme, $\hat{m}$ will be decoded as follows:

$$\hat{m} = arg \min_{m \in \{0,1\}} \mid \rho \cdot y^T p - Q_m(\rho \cdot y^T p, \Delta) \mid .$$

The quantification factor $Q_m(\rho \cdot y^T p, \Delta)$ is indeed equal to $round\left(\frac{\rho \cdot y^T p - d_m}{\Delta}\right) \Delta + d_m$ which may be different from $round\left(\frac{y^T p - d_m}{\Delta}\right) \rho \cdot \Delta + \rho \cdot dm$ and consequently not equal to $\rho \cdot Q_m(y^T p, \Delta)$. Therefore, as the decoded message can be different from the embedded one, the robustness against the FGA attack cannot be obtained. But with the N-STDM watermarking scheme, $\hat{m}$ will be decoded as follows:

$$\begin{aligned} \hat{m} &= arg \min_{m \in \{0,1\}} \left| \rho \cdot \tilde{y} - \rho \cdot \|y\| Q_m\left(\frac{\rho \cdot \tilde{y}}{\rho \cdot \|y\|}, \Delta\right) \right| \\ &= arg \min_{m \in \{0,1\}} \left| \rho \cdot \left(\tilde{y} - \|y\| Q_m\left(\frac{\tilde{y}}{\|y\|}, \Delta\right)\right) \right|. \end{aligned}$$

Thus, the non-linear impact of the ρ factor in the quantization will not affect the process of decoding the message; as a result, the N-STDM has stronger resistance to the FGA attack.

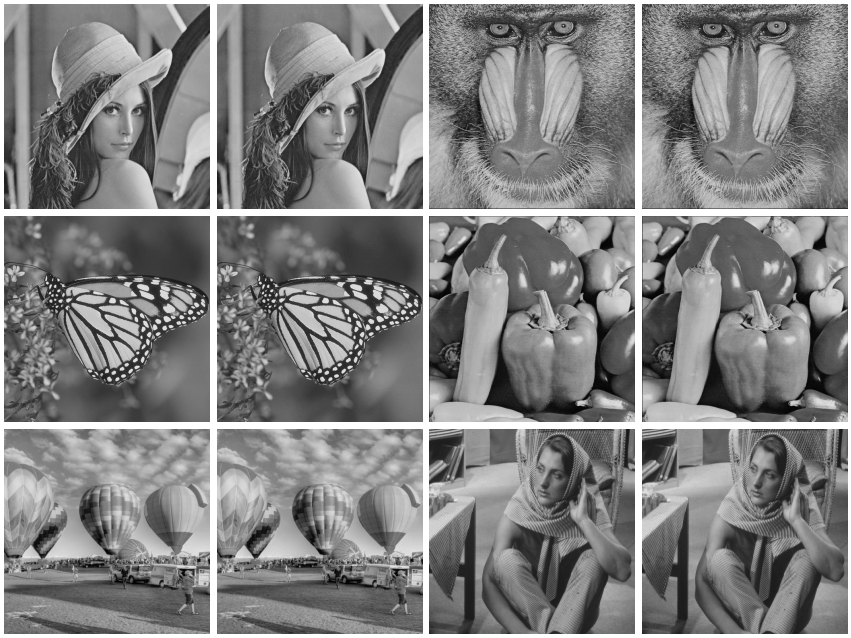
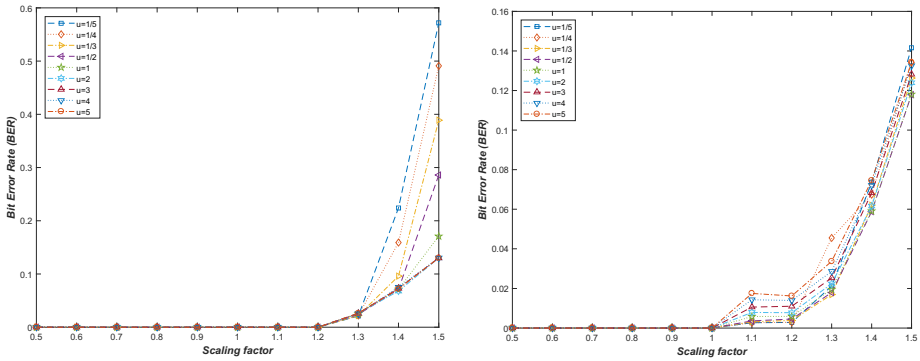


Fig. 2: The original images (first and third columns) and corresponding watermarked images (second and fourth columns) using the N-STDM method for u=2 with a 4096-bit message embedded and SSIM=0.982.

6 Experiments on Real Images

The algorithm is parameterized by two variables, which are the u factor, presented in (11), and the elements that are considered to compute the norm. The first part of the experiment aimed at finding optimal values for these parameters with respect to the results against the FGA attack. We compared our proposed method against the FGA attack while varying u using two forms. In the first one (Global form), we compute the norm value $\|x\|$ of the whole pixels of the cover image which will be used to embed all the watermark bits. In the second one (Local form), we extract the pixels values from the cover image and arrange them into several vectors. After that, we compute the norm value $\|x\|$ of each vector, in which we will embed the i^{th} bit of the watermark; hence, each bit will have a specific norm value, and each vector will have the same length as the projection vector. In this experiment, grayscale images with size 512×512, such as the images presented in Fig. 2, have been used as a host signal, the length of the projection vector is set to 64, which allows a 4096-bit message to be embedded into each image, and Δ is adjusted to have watermarked images with same level of fidelity by using a fixed SSIM of 0.982 (PSNR around 45 dB). The robustness of N-STDM method against FGA attack when varying u between 1/5 and 5 using the global form is shown in Fig. 3a. The BER decrease when u increases, with preferable results when u is higher than 1.



(a) Global form. (b) Local form.

Fig. 3: Robustness of N-STDM against FGA attack in term of BER while varying u with SSIM=0.982.

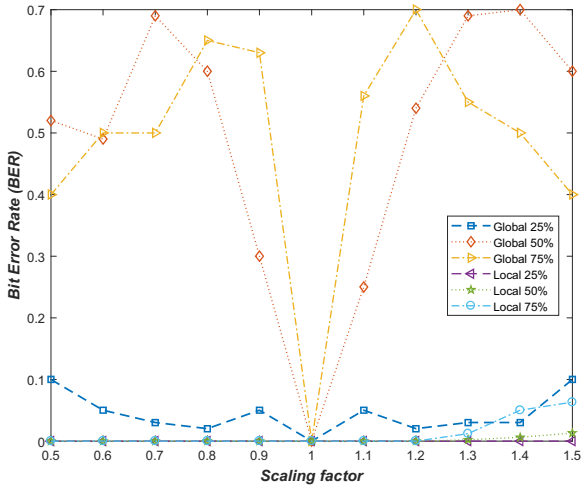


Fig. 4: Robustness of N-STDM (Local form vs Global form) against FGA attack applied to a given area of the watermarked image (between 25% and 75%) with u=2.

Fig. 3b shows the robustness of N-STDM against FGA attack using the local form. In this situation, the N-STDM has a good performance regardless of the value of u. The BER increase a little bit when multiplying the pixels of the grayscale images by a gain factor higher than 1.2 due to the clipping error; when the pixels values are beyond 255, it will be clipped to 255. The maximum allowed value is 255. Besides, the robustness of the global form and the local form was tested against the FGA attack, when applied to a given area of the watermarked image (between 25% and 75%). As shown in Fig. 4, the local form has better robustness comparing to the global form. The global form is affected when the FGA attack is applied

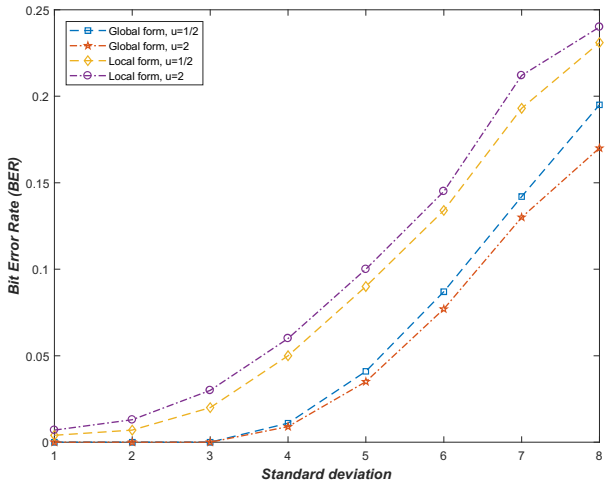


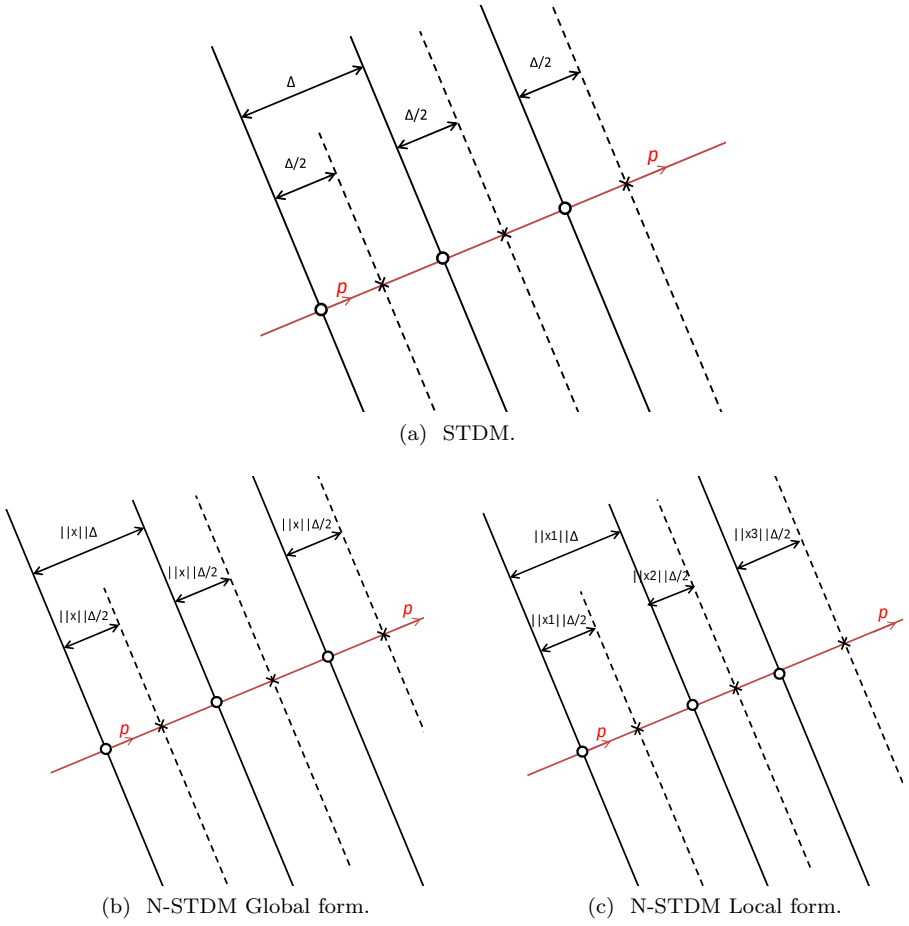
Fig. 5: Robustness of N-STDM (Local form vs Global form) against AWGN attack in term of BER while varying u with SSIM=0.982.

to 50% or 75% of the area of the watermarked images. The problem of the global form is solved in the frequency domain when the DCT transform is applied to the cover images. The detailed results are presented in Section 6.2.

Moreover, we have compared the robustness of global form and local form against the AWGN attack while varying the standard deviation between 1 and 8. As shown in Fig. 5, the N-STDM watermarking scheme has better robustness using the global form comparing to the local form. Fig. 6 shows the sets of reconstruction points of the quantizers for embedding each bit in each vector, where the projection of the vector is done before quantization. The signal is quantized to the nearest point on a $\circ$-line to embed a 0-*bit* and on a $\times$-line to embed a 1-*bit*. The minimum distance d_{min} between the sets of reconstruction points of different quantizers in the ensemble effectively determines the robustness of the embedding. With STDM [8], as shown in Fig. 6, $d_{min} = \Delta/2$. In N-STDM global form, the same norm value is used uniformly to embed each bit of the watermark. For that, $d_{min}=\|x\|\Delta/2$. In the local form, the quantization step size can be seen as a variable step quantizer; each vector has a specific quantization step size. Therefore, d_{min} of the first bit will be different from d_{min} of the second bit, and so on. This variation increases the influence of additive noise attacks on the decoding quantization step size. In the global form, a uniform gain invariant adaptive quantization is obtained at both the embedder and decoder, which improves the robustness against the additive noise attacks. It still better to use the global form since the same norm value $\|x\|$ is used to embed all the bits of the watermark; accordingly, all the watermarked vectors in the image will have an identical imperceptibility and better robustness.

In conclusion, the parameter value that provides the results with the lowest errors is u=2 using a global form of the norm, which will be applied in the subsequent experiments.

In the second part of the experiment, we have practically evaluated the correction of the N-STDM watermarking scheme. In other words, we have verified that when



(a) STDM.

(b) N-STDM Global form.

(c) N-STDM Local form.

Fig. 6: Geometrical representation of STDM, N-STDM Global form, and N-STDM Local form. Points on solid-lines represent embedding for m=1, whereas dashed-lines are for m=0.

a message is embedded into a host signal, prior to applying any attacks, it will be extracted without any error. Practically speaking, 1000 grayscale images with size 512×512 extracted from Boss image database [15] are used as a host signal. The length of the projection vector is set to 64, which allows a 4096-bit message to be embedded into each image. The quantization step size Δ is adjusted in order to have watermarked images with uniform fidelity, a fixed SSIM of 0.982. For all the images, the BER of the extracted watermark are equal to 0, which leads to a conviction that any embedded message could be retrieved without errors prior to applying any attacks.

In the third part of the experiment, the visual aspect of the presented approach has been studied. The length of the projection vector is set to 64, which allows a 4096-bit message to be embedded into each image. We used the Structural Similarity Index Measurement (SSIM) to evaluate the quality performance of N-STDM.

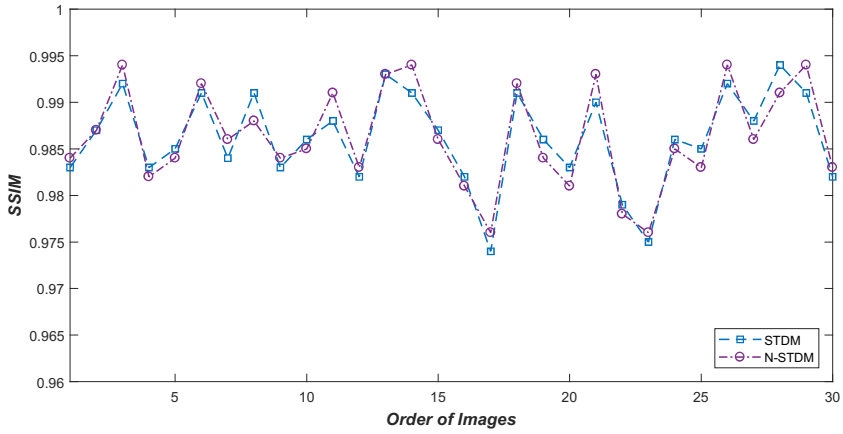


Fig. 7: SSIM comparison between N-STDM and STDM.

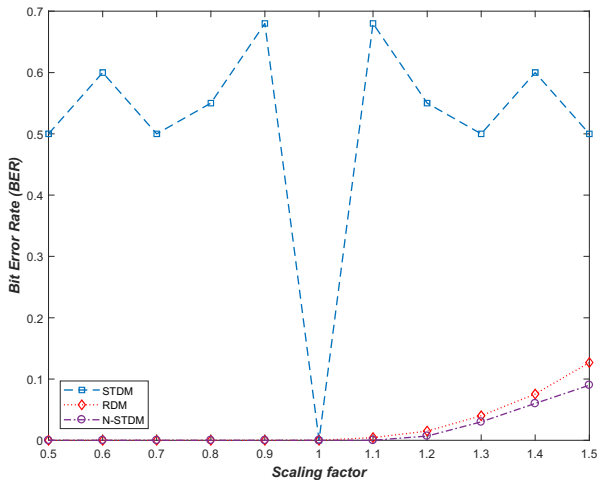


Fig. 8: Robustness against FGA attack in term of BER with SSIM=0.982.

Fig. 7 shows the comparison between N-STDM and STDM on 30 standard watermarked images in term of SSIM. N-STDM produces watermarked images that yield nearly the same SSIM performance as that of the traditional STDM. Fig.2 shows a part of grayscale images. The second and fourth columns display the obtained watermarked images using the N-STDM method with a SSIM=0.982. These watermarked images appear identical to the original ones, to a far extent that they cannot be told differently with the naked eye.

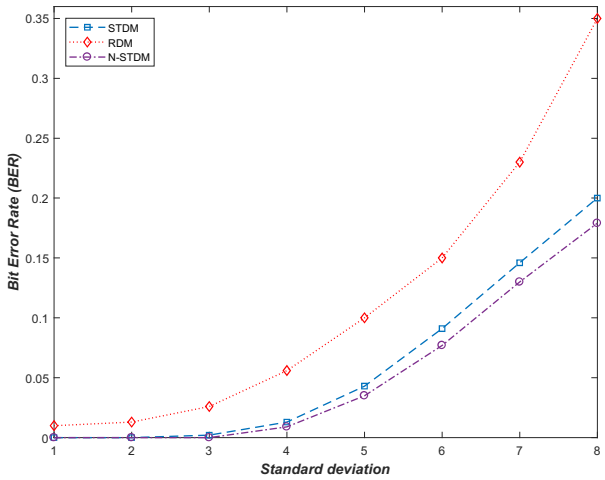


Fig. 9: Robustness against AWGN attack in term of BER with SSIM=0.982.

6.1 Comparison in the Spatial Domain

In this section, we compare the robustness in the spatial domain of our proposed approach with the traditional STDM watermarking scheme and RDM [29] against the FGA attack and AWGN attack. The comparison is conducted using the grayscale images of size 512×512. The length of the projection vector is set to 64 which allows a 4096-bit message to be embedded into each image, and the tested images were watermarked with a uniform fidelity, where SSIM is fixed to 0.982 (PSNR around 45 dB).

As shown in Fig. 8, N-STDM and RDM have good robustness against the FGA attack, while STDM has low robustness against the FGA attack; even when the values of a gain factor are close to 1, such as 1.1 or 0.9, the BER are excessively high.

As to the RDM, the feature signal for quantization is constructed using the ratio of the previously generated watermarked sample and the current host sample. As a result, it resists the FGA attack but will be affected by the AWGN attack as shown in Fig. 9. The quantization step size in RDM is a variable step quantizer, whose size is a function of several past watermarked samples, and does not benefit from the randomness property of the spreading vector. Therefore, the attacking noise has more influence on the decoding quantization step size. Concerning the N-STDM, the quantization step size depends on the watermarked samples during the decoding process which will scale linearly with the FGA attack, and based on the global form, a uniform gain invariant adaptive quantization is obtained at both the embedder and decoder. However, since the proposed N-STDM keep on using the spreading vector in the embedding process, it withstands AWGN attack. This is due to the randomness property of the spreading vector, which affects the embedding of the watermark and hence makes it randomly distributed in the host signal samples. Therefore, the proposed N-STDM sustain the robustness against various noise attacks.

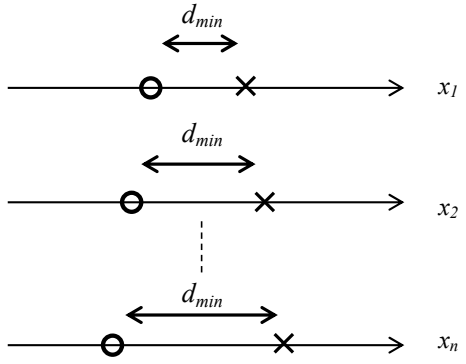
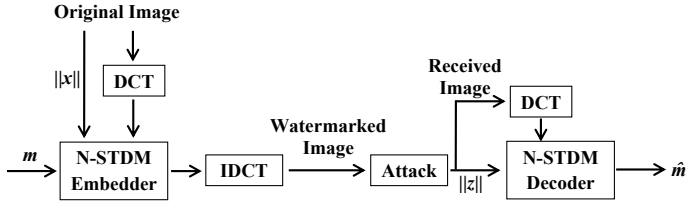


Fig. 10: Geometrical representation of RDM in term of d_{min}. The signal is quantized to the nearest point on a $\circ$-line to embed a 0-*bit* and on a $\times$-line to embed a 1-*bit*.

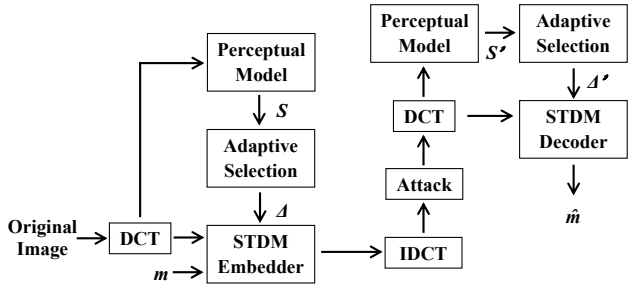
Also, the quantization step size Δ in RDM depends on $g(y_{k-L}^{k-1})$, which is not uniform for all the samples. Therefore, as shown in Fig. 10, each sample will have a specific minimum distance d_{min}. By this way, each watermarked sample will have a specific level of robustness. Comparing to N-STDM global form, as shown in Fig. 6, d_{min} is uniform for all the sets of reconstruction points of different quantizers. Therefore, the trade-off between robustness and transparency is achieved. The watermark bit is spread into a group of samples instead of one sample, which also increase the level of robustness. Each time the watermarking space increases, the probability of accurate decoding is higher. This is mainly because of the spreading property of the watermark using the spreading vector. Our approach achieves significant robustness against the FGA attack with an improvement of 98% in terms of BER compared to traditional STDM and 24% compared to RDM. As for the AWGN attack, an improvement of 21% is shown compared to STDM and 50% compared to RDM.

6.2 Comparison in the Frequency Domain

To test the performance of N-STDM in the frequency domain, we have implemented the DCT transform on the grayscale images of size 512×512 as shown in the block diagram in Fig. 11a. First of all, we have computed the norm value $\|x\|$ of the original image to be used during the embedding process. After that, we have divided the image into 8×8 blocks of pixels, upon which the DCT transform was later performed to get the DCT coefficients. A part of these coefficients was used as a host vector of length L, in which we have later embedded the i^{th} bit of the watermark message m. Then, we have performed the inverse DCT transform at each block to get the watermarked image.
To assure a fair comparison, we compared the proposed N-STDM watermarking scheme with I-ASTDM [39], STDM-MW-SS [26] and STDM-SP-wm [27]; family methods based on the perceptual model. The block diagram of those family methods is shown in Fig. 11b, where the quantization step size Δ is modified based on



(a) Block diagram of the N-STDM method.



(b) Block diagram of the family methods based on Watson's model.

Fig. 11: Block diagrams of the N-STDM method (a) and the family methods based on Watson's model (b).

the slacks vectors S which are computed using Watson's model.
The FGA attack, AWGN attack, JPEG compression, and a variety of common signal processing attacks are used to verify the performance of our proposed scheme. The 2nd-21st DCT coefficients have been used for all the algorithms. These coefficients have been selected based on the zig-zag-scanned order of each 8×8 block, in which we embed 1 bit of the watermark. The embedding rate is 1/64, *i.e.* one bit in each 8×8 block, which allows the embedding of a 4096-bit message into each image. The tested images were watermarked using a uniform fidelity, with a fixed SSIM of 0.982 (PSNR around 45 dB) for the first part of comparisons, and a fixed SSIM of 0.953 (PSNR around 40 dB) for the second part of comparisons by regulating the quantization step size and the factors that adjust the watermarking strength. All of the experimental results are obtained by averaging over 100 runs.

In the first part of the experiments, the global form of the N-STDM watermarking scheme was examined facing the FGA attack, when applied to a given area of the watermarked image (between 25% and 100%). As shown in Fig. 12, the robustness is highly improved comparing to the global form in the spatial domain presented in Fig. 4, especially when the FGA attack is applied to 50% or 75% of the area of the watermarked image.
Moreover, the proposed N-STDM is compared with the family methods based on Watson's model against the FGA attack. As expected, the results of the posted comparison have met the suggestions of the proposed method. According to Fig. 13, the proposed N-STDM watermarking scheme has a slightly better level of robustness than the family methods, varying from 5% comparing to STDM-MW-SS

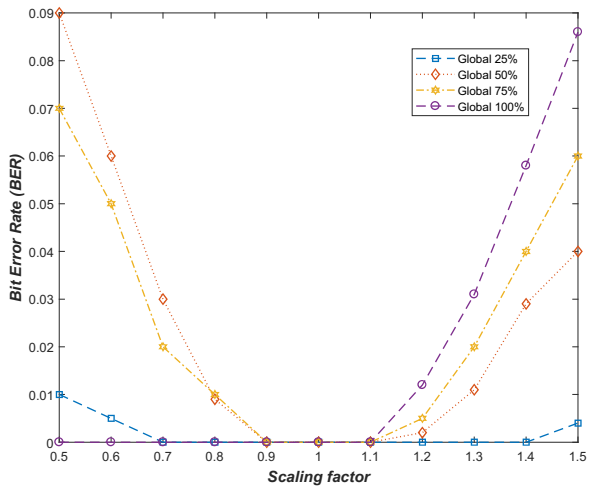
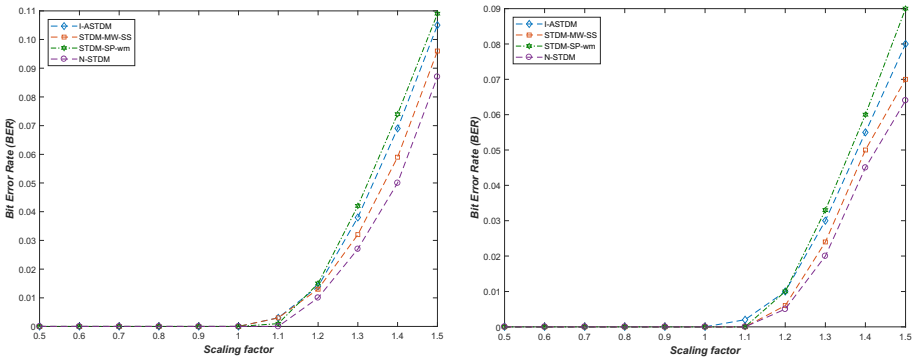


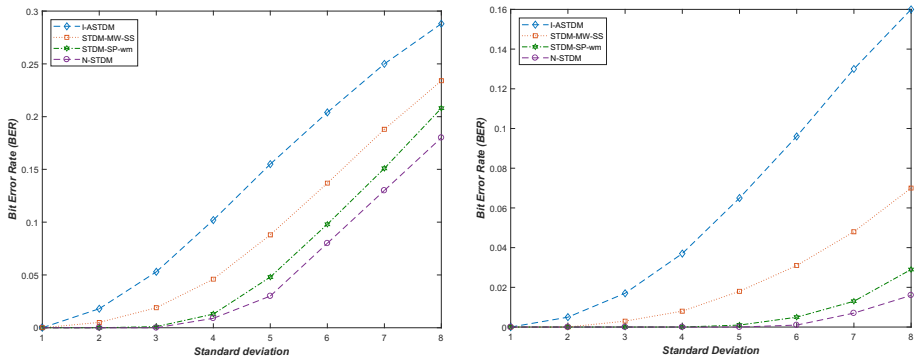
Fig. 12: Robustness of N-STDM against FGA attack applied to a given area of the watermarked image (between 25% and 100%) with SSIM=0.982.



(a) SSIM=0.982. (b) SSIM=0.953.

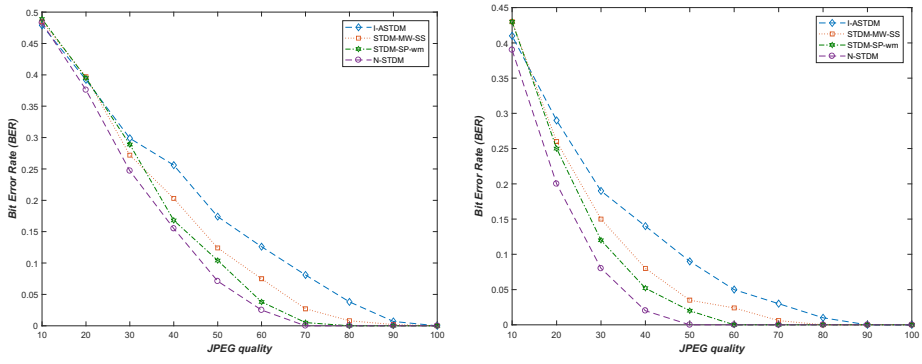
Fig. 13: Robustness against FGA attack in term of BER.

to 22% comparing to STDM-SP-wm for SSIM = 0.982, while proved to have better to more superior robustness against the AWGN attack and JPEG compression.
The robustness against AWGN attack has been tested in terms of BER while varying the standard deviation between 1 and 8. As shown in Fig. 14, the proposed N-STDM watermarking scheme achieves better performance than the STDM-SP-wm (improvement of 14%) and notably superior performance to the I-ASTDM (improvement of 38%) and STDM-MW-SS (improvement of 56%).
Fig. 15 illustrates the robustness to JPEG compression in term of BER while varying the JPEG quality between 10 and 100. The JPEG quality denotes the compressibility of the JPEG compressor; lower numbers mean lower quality. The N-STDM has better performance than STDM-SP-wm (improvement of 13%) with



(a) SSIM=0.982. (b) SSIM=0.953.

Fig. 14: Robustness against AWGN attack in term of BER.



SSIM=0.982. SSIM=0.953.

Fig. 15: Robustness against JPEG compression in term of BER.

more notable variations comparing to STDM-MW-SS (improvement of 18%) and I-ASTDM (improvement of 27%) against the JPEG compression.

To further evaluate the performance of N-STDM watermarking scheme, we have compared the robustness against noise addition attacks, image filtering attacks, and geometric attacks. All the watermarked images were exposed to many different attacks such as Salt&Pepper with noise densities $\in \{0.005, 0.01\}$, Gaussian filtering, Median filtering, Wiener filtering, Average filtering, Cropping, Rotation, and Resizing. The detailed experimental results are shown in Table 1 with SSIM=0.982 and Table 2 with SSIM=0.953. The experiments have verified that our proposed scheme is not only robust against the FGA attack but also robust to common signal processing attacks. N-STDM has achieved good robustness against Salt&Pepper attack and image filtering attacks comparing to the family methods based on Watson's model. As for the geometric attacks, N-STDM achieved good robustness against the cropping attack when we cropped 10% of the image, but the BER slightly increased when we increased the cropping dimension of the image to 20%.

Table 1: BER comparison under noise addition, image filtering, and geometric attacks with SSIM=0.982.

Attacks	I-ASTDM	STDM-MW-SS	STDM-SP-wm	N-STDM
Salt&Pepper (d=0.005)	0.12	0.11	0.12	**0.09**
Salt&Pepper (d=0.01)	0.21	0.19	0.22	**0.17**
Gaussian filtering (3 × 3)	0.016	0.024	0.035	**0.014**
Median filtering (3 × 3)	0.25	0.21	0.22	**0.16**
Wiener filtering (3 × 3)	0.26	0.2	0.22	**0.16**
Average filtering (3 × 3)	0.35	0.31	0.29	**0.24**
Crop (10%)	0.0064	0.0063	0.0066	**0.0061**
Crop (20%)	0.023	0.022	0.024	0.08
Rotation (1°)	0.48	0.46	0.47	0.46
Re-Rotation (-1°)	0.18	0.09	0.1	**0.07**
Resizing (1024 × 1024)	0.025	0.003	0.008	**0**
Resizing (256 × 256)	0.31	0.28	0.24	**0.21**

Table 2: BER comparison under noise addition, image filtering, and geometric attacks with SSIM=0.953.

Attacks	I-ASTDM	STDM-MW-SS	STDM-SP-wm	N-STDM
Salt&Pepper (d=0.005)	0.09	0.07	0.08	**0.06**
Salt&Pepper (d=0.01)	0.16	0.14	0.14	**0.1**
Gaussian filtering (3 × 3)	0.004	0.002	0.01	**0**
Median filtering (3 × 3)	0.17	0.14	0.15	**0.11**
Wiener filtering (3 × 3)	0.16	0.13	0.12	**0.07**
Average filtering (3 × 3)	0.26	0.22	0.21	**0.16**
Crop (10%)	0.0053	0.0051	0.0052	**0.0041**
Crop (20%)	0.019	0.017	0.018	0.06
Rotation 1°	0.47	0.48	0.46	0.45
Re-Rotation 1°	0.05	0.05	0.06	**0.04**
Resizing (1024 × 1024)	0.001	0.001	0.001	**0**
Resizing (256 × 256)	0.23	0.21	0.19	**0.12**

Concerning the rotation attack, all the compared methods were vulnerable to the rotation of 1° of the image, though the BER highly decrease if we re-rotate the image by -1°. As for the resizing attack, N-STDM achieved better robustness comparing to the family methods, noting that the robustness improved as well while adjusting the watermarking strength based on Δ.

7 Experiments and Comparisons on PDF Documents

Portable Document Format (PDF) has been invented by Adobe [19] and maintained by the International Organization for Standardization (ISO). PDF is a digital form and an imaging model derived from PostScript language, with more structured format for representing documents, which enable users to view and exchange the electronic documents reliably and easily. PDF users around the world include important information while using PDF. Therefore, the protection of those documents against unauthorized users has become essential and necessary. PDF functions vary from text to images and other multimedia elements.
The general text-based structure of PDF is composed of 4 parts:

1. Header: contains the version number of the PDF document.
2. Body: consists of a series of objects, representing the contents of a document.

Digital networks become an essential communication mechanism. They are used to transmit any sort of information like text, audio and image. Due to the rapid growth of the Internet, access to multimedia data has become much easier, but authors and data providers are reluctant to allow the distribution of their data in a network environment due to a significant number of problems such as illegal distribution, duplication, authentication and malicious tampering of digital data.

(a) $\Delta = 1 \times 10^{-3}$, $MSE = 7 \times 10^{-3}$.

Digital networks become an essential communication mechanism. They are used to transmit any sort of information like text, audio and image. Due to the rapid growth of the Internet, access to multimedia data has become much easier, but authors and data providers are reluctant to allow the distribution of their data in a network environment due to a significant number of problems such as illegal distribution, duplication, authentication and malicious tampering of digital data.

(b) $\Delta = 2 \times 10^{-3}$, $MSE = 0.03$.

Digital networks become an essential communication mechanism. They are used to transmit any sort of information like text, audio and image. Due to the rapid growth of the Internet, access to multimedia data has become much easier, but authors and data providers are reluctant to allow the distribution of their data in a network environment due to a significant number of problems such as illegal distribution, duplication, authentication and malicious tampering of digital data.

(c) $\Delta = 3 \times 10^{-3}$, $MSE = 0.07$.

Digital networks become an essential communication mechanism. They are used to transmit any sort of information like text, audio and image. Due to the rapid growth of the Internet, access to multimedia data has become much easier, but authors and data providers are reluctant to allow the distribution of their data in a network environment due to a significant number of problems such as illegal distribution, duplication, authentication and malicious tampering of digital data.

(d) $\Delta = 4 \times 10^{-3}$, $MSE = 0.13$.

Digital networks become an essential communication mechanism. They are used to transmit any sort of information like text, audio and image. Due to the rapid growth of the Internet, access to multimedia data has become much easier, but authors and data providers are reluctant to allow the distribution of their data in a network environment due to a significant number of problems such as illegal distribution, duplication, authentication and malicious tampering of digital data.

(e) $\Delta = 5 \times 10^{-3}$, $MSE = 0.17$.

Fig. 16: Perceptual visualization of the watermarked document using the N-STDM for $\Delta = 1 \times 10^{-3}$ to 5×10^{-3} gradually from top to bottom.

3. Cross-reference table: contains one-line entry for each indirect object and has a fixed format in order to access randomly the entries in the table.
4. Trailer: enables a conforming reader to quickly find the cross-reference table and other special objects.

In a PDF file, coordinate systems determine the position, orientation, and size of the text, images, and graphics that appear on a page. Each character has a coordinate pair, x and y, that locates the character horizontally and vertically within two-dimensional coordinate space. The x-coordinates values are non-constant. Therefore, they have been used as the watermarking space in order to embed the watermark.

Each character of the watermark has been encoded into 8 bits in order to form a total of N bits. Each bit message is then embedded into L characters' x-coordinates extracted from the original document. Accordingly, a total of $N \times L$ characters are used from the document to embed the whole bits of the message. Fig. 16 presents a part of a watermarked paragraph extracted from the watermarked document, which has been watermarked using the N-STDM watermarking scheme with several values of Δ. When Δ increases, the error values increase as well, especially when $\Delta \geq 4 \times 10^{-3}$. 24 lines have been extracted from a PDF document with 84 characters each (n=84), totalling 2016 characters.

To assure a wider comparison between the proposed N-STDM watermarking scheme and the traditional STDM and RDM watermarking schemes against FGA and AWGN attacks, two scenarios have been applied through which the number of bits N and the length of the projection vector L have been variably used: In the first scenario, we embedded $k = 1$ bit per line (N=24 and L=84), and in the second one, we embedded $k = 4$ bits per line (N=96 and L=21). Same embedding parameters have been used such as the length of the host signal, the secret message, and dither level. All the experiments were conducted while varying Δ. Several values of Δ have been used taking into account the Mean Squared Error (MSE) values; the Δ value has been adjusted in order to have the same MSE values (0.03 and 0.13)

7.1 Comparison Against FGA and AWGN Attacks

In order to prove the superiority of N-STDM in terms of robustness constraint, a comparison between the proposed scheme (N-STDM) and the traditional schemes (RDM and STDM) was performed while varying the parameters N and L. The comparison mainly tackles the robustness against FGA and the robustness against AWGN attacks.

The N-STDM robustness against the FGA attack, to start with, has achieved a great superiority over STDM. Fig. 17 and Fig. 18 show that the traditional STDM is affected by the FGA attack even when the Δ value is high (MSE=0.13) and regardless of the length of projection vector and the number of the embedded bits. On the contrary, N-STDM, along with RDM, surpass the FGA attack for MSE = 0.03 and 0.13.

As to the robustness against AWGN attack, the strength is evaluated by mean of the Watermark to Noise Ratio (WNR):

$$WNR = 10 \log_{10}\left(\frac{\sigma_w^2}{\sigma_n^2}\right). \tag{23}$$

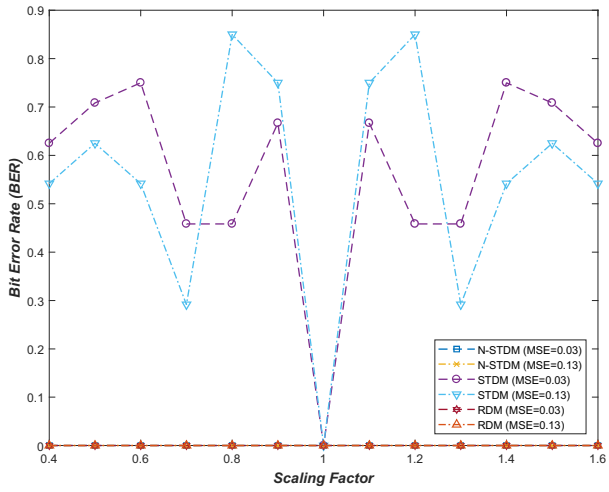


Fig. 17: Robustness against FGA for N=24 and L=84.

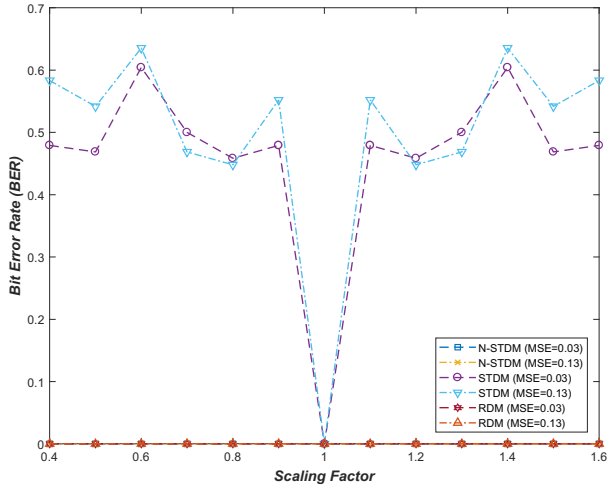


Fig. 18: Robustness against FGA for N=96 and L=21.

Only the digits after the decimal point are modified. Fig. 19 and Fig. 20 show that RDM is noticeably affected by the AWGN attack even when the Δ value is high whereas the proposed N-STDM achieves great performance against this attack. STDM preserves good performance against AWGN, yet the proposed N-STDM could perform even better noting that the BER of STDM and N-STDM are close to each other with an advantage of N-STDM over STDM.

As shown in Fig. 19 and Fig. 20, RDM is affected by the AWGN attack even with a higher value of Δ. In contrast, our proposed N-STDM watermarking scheme preserves superior robustness against the AWGN attack. The robustness increases while Δ and L increase, with a BER close to 0 when WNR $>$ 0. The BER of

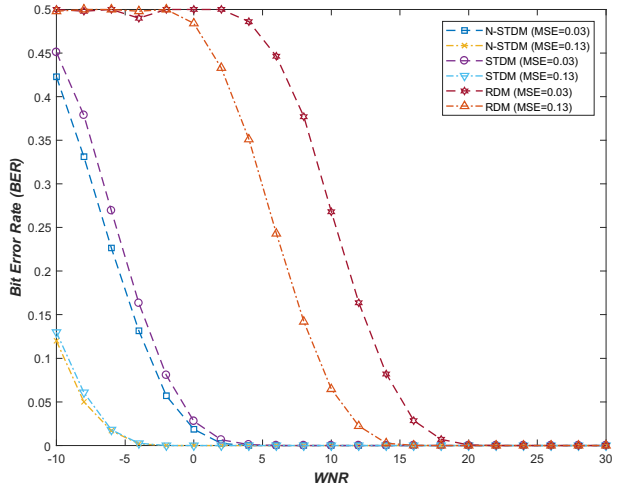


Fig. 19: Robustness against AWGN for N=24 and L=84.

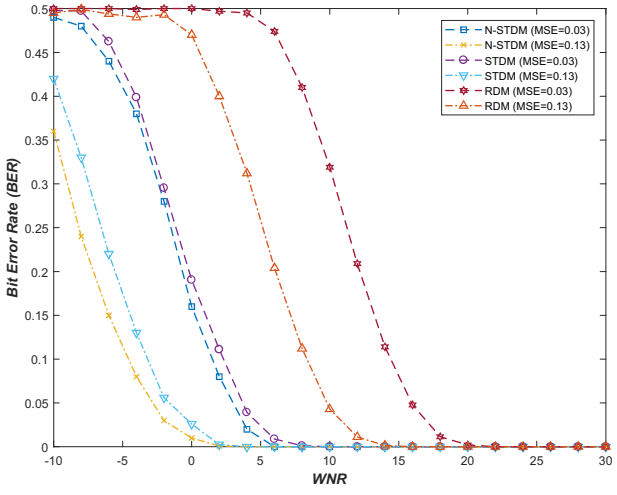


Fig. 20: Robustness against AWGN for N=96 and L=21.

STDM and N-STDM watermarking schemes are close to each other, with better performance for N-STDM.
N.B. Based on Watsons model, the family methods could not be applied to PDF documents because they are dependent on the perceptual model of images.

8 Findings and Discussion

We have studied the performance of the proposed N-STDM watermarking scheme in the spatial domain and the frequency domain using the grayscale images and

Table 3: Summary of the findings.

Watermarking scheme	**Findings**
STDM	*Strong against the AWGN attack *Week against the FGA attack
RDM	*Strong against the FGA attack *Week against the AWGN attack
Family methods based on Watson's model	*Robust against FGA, AWGN, JPEG compression, Image filtering, and Cropping attacks *Weak against Rotation attack *Dedicated for images *Could only be applied in the frequency domain
N-STDM	*More flexible *Could be applied in the spatial domain and frequency domain *Any element can be used as support to embed the watermark (such as images and PDF documents) *High level of robustness against FGA, AWGN, JPEG compression, and Image filtering attacks *Robust against Copping, and Resizing attacks *Weak against Rotation attack

PDF documents. As for the experiments on real images in the spatial domain, the proposed N-STDM has achieved high robustness against FGA and AWGN attacks comparing to STDM and RDM. STDM has good robustness against AWGN attack, but it is highly affected by the FGA attack. RDM achieves good robustness against FGA attack but has a weak performance against the AWGN attack.
With respect to the experiments on real images in the frequency domain, the family methods (I-ASTDM, STDM-MW-SS, and STDM-SP-wm) have good robustness against the FGA attack, and an accepted robustness against AWGN attack and JPEG compression. The proposed watermarking scheme, N-STDM, on the other hand, achieves a superior performance comparing to the family methods varying from little different against FGA attack to a greater one against AWGN, JPEG compression, and image filtering attacks. As for the geometric attacks, N-STDM has achieved good robustness against the cropping attack, but the BER slightly increased while increasing the cropping dimension of the image. N-STDM and the family methods are vulnerable to the rotation attack, though the BER highly decrease if we re-rotate the image. Concerning the resizing attack, N-STDM has achieved better robustness comparing to the family methods, noting that the robustness improved as well while adjusting the watermarking strength based on Δ. Moreover, we proved that our approach could also be used as a blind watermarking scheme for PDF documents under a sufficient transparency-robustness tradeoff. We exploited the x-coordinates values of characters as real cover elements to embed the watermark. The comparison between N-STDM and the traditional STDM

and RDM against FGA and AWGN attacks shows that the proposed N-STDM achieves better performance than the mentioned watermarking schemes.

9 Conclusion and Future Work

In this paper, we have proposed an improved version of STDM watermarking scheme, which is essentially invariant to FGA attack. In this method, called N-STDM, we scaled the quantization step size in the same way the watermarked signal is scaled as an invariant adaptive size based on the global form. Experiments on real images in the spatial domain and frequency domain have verified that our method is not only robust to the FGA attack but also robust to common signals processing attacks such as AWGN attack, JPEG compression, and Image filtering attacks comparing to STDM, RDM, and the family methods based on Watson's model. As for the geometric attacks, N-STDM has achieved good robustness against the resizing and cropping attacks, but the BER slightly increased while increasing the cropping dimension of the image. N-STDM and the family methods are vulnerable to the rotation attack, though the BER highly decrease if we re-rotate the image.
Moreover, we have verified that our approach could also be used as a blind watermarking scheme for PDF documents with a perceptual advantage and better robustness over STDM and RDM.
As for future enhancements, we plan to include further improvement of the N-STDM watermarking scheme against the geometric attacks, by applying other types of frequency transform such as DWT and SVD.

Acknowledgements This work is partially funded with support from the National Council for Scientific Research in Lebanon CNRS-L, the Hubert Curien CEDRE programme, the Agence Universitaire de la Francophonie AUF-PCSI programme, and the Labex ACTION program (contract ANR-11-LABX-01-01).

References

1. Alizadeh-Fahimeh, F., Canceill-Nicolas, N., Dabkiewicz-Sebastian, S., Vandevenne-Diederik, D.: Using steganography to hide messages inside PDF files. SSN Project Report (2012)
2. Barni, M., Bartolini, F., Cappellini, V., Piva, A.: A DCT-domain system for robust image watermarking. Signal processing **66**(3), 357–372 (1998)
3. Bartolini, F., Barni, M., Piva, A.: Performance analysis of ST-DM watermarking in presence of nonadditive attacks. IEEE Transactions on Signal Processing **52**(10), 2965–2974 (2004)
4. Bitar, A.W., Darazi, R., Couchot, J.F., Couturier, R.: Blind digital watermarking in PDF documents using Spread Transform Dither Modulation. Multimedia Tools and Applications **76**(1), 143–161 (2017)
5. Bitar, A.W., Darazi, R., Couchot, J.F., Couturier, R.: Blind digital watermarking in PDF documents using Spread Transform Dither Modulation. Multimedia Tools and Applications **76**(1), 143–161 (2017)
6. Boney, L., Tewfik, A.H., Hamdy, K.N.: Digital watermarks for audio signals. In: Multimedia Computing and Systems, 1996., Proceedings of the Third IEEE International Conference on, pp. 473–480. IEEE (1996)
7. Castiglione, A., Santis, A.D., Soriente, C.: Security and privacy issues in the Portable Document Format. Journal of Systems and Software **83**(10), 1813 – 1822 (2010).

DOI https://doi.org/10.1016/j.jss.2010.04.062. URL http://www.sciencedirect.com/science/article/pii/S0164121210001287
8. Chen, B., Wornell, G.W.: Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory **47**(4), 1423–1443 (2001). DOI 10.1109/18.923725
9. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital watermarking and steganography. Morgan Kaufmann (2007)
10. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE transactions on image processing **6**(12), 1673–1687 (1997)
11. Cox, I.J., Kilian, J., Leighton, T., Shamoon, T.: Secure spread spectrum watermarking for images, audio and video. In: Image Processing, 1996. Proceedings., International Conference on, vol. 3, pp. 243–246. IEEE (1996)
12. Darazi, R., Callau, P., Macq, B.: Secure and HVS-adaptive exhibition Spread Transform Dither Modulation watermarking for Digital cinema. In: 2009 First IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–5 (2009). DOI 10.1109/WIFS.2009.5386493
13. Darazi, R., Hu, R., Macq, B.: Applying Spread Transform Dither Modulation for 3D-mesh watermarking by using perceptual models. In: 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1742–1745 (2010). DOI 10.1109/ICASSP.2010.5495455
14. Feng, Y., Liu, B., Cui, X., Liu, C., Kang, X., Su, J.: A Systematic Method on PDF Privacy Leakage Issues. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1020–1029 (2018). DOI 10.1109/TrustCom/BigDataSE.2018.00144
15. Filler, T., Pevný, T., Craver, S., Ker, A.D. (eds.): Information Hiding - 13th International Conference, IH 2011, Prague, Czech Republic, May 18-20, 2011, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 6958. Springer (2011). DOI 10.1007/978-3-642-24178-9. URL https://doi.org/10.1007/978-3-642-24178-9
16. Hatoum, M.W., Darazi, R., Couchot, J.: Blind Image Watermarking using Normalized STDM robust against Fixed Gain Attack. In: 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1–6 (2018). DOI 10.1109/IMCET.2018.8603038
17. Hatoum., M.W., Darazi., R., Couchot., J.: Blind PDF Document Watermarking Robust Against PCA and ICA Attacks. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT,, pp. 420–427. INSTICC, SciTePress (2018). DOI 10.5220/0006899605860593
18. Hsu, C.T., Wu, J.L.: Hidden digital watermarks in images. IEEE Transactions on image processing **8**(1), 58–68 (1999)
19. Iso, T.: 171/sc 2: Iso 32000–1: 2008 document management-portable document format-part 1: Pdf 1.7
20. Jalil, Z., Mirza, A.M.: A review of digital watermarking techniques for text documents. In: Information and Multimedia Technology, 2009. ICIMT'09. International Conference on, pp. 230–234. IEEE (2009)
21. Jiang, Y., Zhang, Y., Pei, W., Wang, K.: Adaptive spread transform QIM watermarking algorithm based on improved perceptual models. AEU - International Journal of Electronics and Communications **67**(8), 690 – 696 (2013). DOI https://doi.org/10.1016/j.aeue.2013.02.005. URL http://www.sciencedirect.com/science/article/pii/S1434841113000587
22. Kuribayashi, M., Fukushima, T., Funabiki, N.: Data Hiding for Text Document in PDF File. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 390–398. Springer (2017)
23. Langelaar, G.C., Setyawan, I., Lagendijk, R.L.: Watermarking digital image and video data. A state-of-the-art overview. IEEE Signal processing magazine **17**(5), 20–46 (2000)
24. Lee, I.S., Tsai, W.H.: A new approach to covert communication via PDF files. Signal processing **90**(2), 557–565 (2010)
25. Li, Q., Cox, I.J.: Using perceptual models to improve fidelity and provide invariance to valumetric scaling for quantization index modulation watermarking. In: Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on, vol. 2, pp. ii–1. IEEE (2005)
26. Li, Q., Cox, I.J.: Improved spread transform dither modulation using a perceptual model: robustness to amplitude scaling and JPEG compression. In: Acoustics, Speech and Signal

Processing, 2007. ICASSP 2007. IEEE International Conference on, vol. 2, pp. II–185. IEEE (2007)

27. Li, X., Liu, J., Sun, J., Yang, X., Liu, W.: Step-projection-based spread transform dither modulation. IET information security **5**(3), 170–180 (2011)
28. Malvar, H.S., Florêncio, D.A.: Improved spread spectrum: A new modulation technique for robust watermarking. IEEE transactions on signal processing **51**(4), 898–905 (2003)
29. Pérez-González, F., Mosquera, C., Barni, M., Abrardo, A.: Rational dither modulation: A high-rate data-hiding method invariant to gain attacks. IEEE Transactions on Signal Processing **53**(10), 3960–3975 (2005)
30. Por, L.Y., Delina, B.: Information hiding: A new approach in text steganography. In: WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering, 7. World Scientific and Engineering Academy and Society (2008)
31. Potdar, V.M., Han, S., Chang, E.: A survey of digital image watermarking techniques. In: Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on, pp. 709–716. IEEE (2005)
32. Vellasques, E., Sabourin, R., Granger, E.: A high throughput system for intelligent watermarking of bi-tonal images. Applied Soft Computing **11**(8), 5215–5229 (2011)
33. Wan, W., Liu, J., Sun, J., Gao, D.: Improved logarithmic spread transform dither modulation using a robust perceptual model. Multimedia Tools and Applications **75**(21), 13,481–13,502 (2016)
34. Wan, W., Liu, J., Sun, J., Yang, X., Nie, X., Wang, F.: Logarithmic spread-transform dither modulation watermarking based on perceptual model. In: Image Processing (ICIP), 2013 20th IEEE International Conference on, pp. 4522–4526. IEEE (2013)
35. Wang, Y.G., Zhu, G.: An improved AQIM watermarking method with minimum-distortion angle quantization and amplitude projection strategy. Information Sciences **316**, 40–53 (2015)
36. Watson, A.B.: DCT quantization matrices visually optimized for individual images. In: Human vision, visual processing, and digital display IV, vol. 1913, pp. 202–217. International Society for Optics and Photonics (1993)
37. Xia, X.G., Boncelet, C.G., Arce, G.R.: A multiresolution watermark for digital images. In: Image Processing, 1997. Proceedings., International Conference on, vol. 1, pp. 548–551. IEEE (1997)
38. Yu, D., Ma, L., Wang, G., Lu, H.: Adaptive spread-transform dither modulation using an improved luminance-masked threshold. In: Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on, pp. 449–452. IEEE (2008)
39. Zhu, X.: Image-adaptive spread transform dither modulation using human visual model. In: Computational Intelligence and Security, 2006 International Conference on, vol. 2, pp. 1571–1574. IEEE (2006)

Makram W. HATOUM received his M.S degree in computer science and telecommunication engineering from Antonine University (UA), Hadat-Baabda, Lebanon in 2013. He is a Telecom and Network Engineer at GlobalCom Data Service (GDS) since 2013, and his research focuses on digital watermarking.

Rony DARAZI (SM'16) received the M.S. degree in Computer and Telecommunications engineering from Antonine Univerity (UA), Lebanon in 2005, and the Ph.D. degree in engineering sciences from the Universit catholique de Louvain (UCL), Louvain-la-Neuve, Belgium, in 2011. His PhD was entitled "Towards a combining scheme for compression and watermarking for 3D stereo images". He is currently an Associate Professor at UA. He was a Researcher in the ICTEAM Institute at UCL from 2006 until 2012, and is a Member of the TICKET Lab at UA since 2010. His research interests include information security and digital watermarking, digital 2D and 3D image processing, sensor networks, and e-health. Dr. Darazi is an IEEE senior member, he received a grant research project from the National Council for Scientific Research in Lebanon (CNRS-L) in 2016. In 2017, he received a research fund from the Hubert Curien CEDRE programme n°40283YK, and another fund from the Agence Universitaire de la Francophonie AUF-PCSI programme. In 2018, Dr. Darazi received a research award from the research council at the Antonine University. He co-chaired the International Conference on Applied Research in Computer Science & Engineering (ICAR'15), sponsored by IEEE in 2015, and has been actively involved as a Reviewer in several conferences and journals. In 2009, he received the Best Paper Award, second prize by the Digital Watermarking Alliance and the IS&T/SPIE International Conference on Media Forensics and Security XII.

Jean-François COUCHOT is an Associate Professor of the FEMTO-ST institute (CNRS) at the university of Bourgogne Franche-Comté. He received a Ph.D. in Computer Science in 2006 in the FEMTO-ST institute.
He has applied for a postdoctoral position at INRIA Saclay Ile de France in 2006. His research focuses on discrete dynamic systems (with applications into data hiding, watermarking, pseudorandom number generators, hash function) and on bioinformatics, especially in gene evolution prediction. He has written more than 40 scientific articles in these areas.