Two Dual Watermarking Based on DCT and Krawtchouk Moments for Handwritten Document Images: A Comparative Analysis

Ernesto Avila-Domenech[1][0000−0002−4797−289X] and Alberto Taboada-Crispi[2][0000−0002−7797−1441]

[1] Universidad de Granma, Carretera Central vía Holguín Km $\frac{1}{2}$, Granma, Cuba
eadomenech@gmail.com
[2] Universidad Central de Las Villas, Villa Clara, Cuba
ataboada@uclv.edu.cu

Abstract. Digital image watermarking is a powerful tool to secure digital image. In the present work, two dual digital image watermarking techniques based on DCT and Krawtchouk moments for handwritten document images have been elaborated and compared. In the proposed schemes, we adopt the YCbCr color space for watermark embedding. The comparative study is based on the values of the PSNR and BER. Simulation results demonstrate that the embedded watermarks can be almost fully extracted from the JPEG-compressed images with high compression ratios for both methods.

Keywords: Digital Watermarking · DCT · Handwritten Document Images · Krawtchouk moments.

1 Introduction

Handwritten documents hoarded in historical archives, libraries and museums are an important source of knowledge and research for historians and the general public. Many of these manuscripts are being digitized with the aim of preserving their physical integrity and providing access to a greater number of people. In the digitization process, it is important to take into account security, as they can be modified and adjudicated to people illegally.

Digital watermarking is an important research branch of information hiding, which can be used for protect the multimedia digital data for example copyright protection, content verification and tamper detection.

Watermarking methods have been proposed for various image content and since the various types of content each have their own characteristics, a watermarking technique should be designed that takes account of their characteristics [9]. That is why we are motivated to investigate a dual watermarking method taking into account the characteristics of the images corresponding to handwritten documents.

Digital watermarking schemes can be divided according to working domain into spatial domain and frequency domain.

Spatial image watermarking techniques are commonly used in steganographic contexts because, hiding data into the least significant bits of an image can allow to embed a large quantity of data. Either it is useful in fragile schemes to determine the ownership integrity. However, the watermark will not be robust to common manipulations, e.g., JPEG compression [3].

The frequency domain schemes are generally considered more robust than the spatial domain schemes; this schemes consist in to transform an image from spatial domain to frequency domain. Some authors have made proposals based on Discrete Cosine Transform (DCT) [12, 16], this is because it has good energy compaction property that is widely used in image compression. Others have been based on Discrete Wavelet Transform (DWT) [3] because assures good robustness against the most popular image manipulations such that rotation, translation and image cropping; and others, have been based on Krawtchouk moments [2, 11, 13, 18] because local image features can be located and described.

On the other hand, for digitized images to be safely and efficiently transmitted on the Internet, watermarked images should be particularly robust to JPEG compression because is the image standard compression which is popularly used in Internet.

In this work, two dual digital image watermarking techniques based on DCT and Krawtchouk moments have been elaborated and compared. Both schemes used Dither Modulation Quantization (QIM-DM) and are optimized for handwritten document images.

The rest of the paper is organized as follow; Section 2 summarize a preliminaries. Section 3 describes the proposed methods including robust watermarking and fragile watermarking. Our experimental results and discussion, especially on JPEG compression with high compression ratios are given in Section 4 and Section 5 concludes the paper.

2 Preliminaries

2.1 Arnold transform

The Arnold transform is a invertible method that can be used for pixel scrambling, and has been adopted in various watermarking schemes. By using the Arnold transform, the high pixel correlation can be disrupted. The Arnold transform is shown in Eq. 1, where p and q are positive integers, $det(A) = 1$, and (x', y') are the new coordinates of the pixel after Arnold transform is applied to a pixel at position (x, y) [5].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N. \tag{1}$$

2.2 Dither modulation quantization

Dither modulation is an extension of traditional QIM algorithm proposed in [4]. It has good performance on following requirements of watermarking: perceptibility ratio, data payload, robustness, and blind extraction. The combination

of dither modulation quantization with different transformation domain watermarking methods also improves watermark extraction capability. The scheme has been applied successfully in watermarking algorithms [2, 6, 13, 19].

One bit of the watermark can be embedded as

$$|C_0^{'}(k_1,k_2)| = \begin{cases} 2\Delta \times round(\frac{|C_0(k_1,k_2)|}{2\Delta}) + \frac{\Delta}{2}, & if\ W(i,j) = 1 \\ 2\Delta \times round(\frac{|C_0(k_1,k_2)|}{2\Delta}) - \frac{\Delta}{2} & if\ W(i,j) = 0 \end{cases}, \tag{2}$$

where Δ is the quantization step controlling the embedding strength of the watermark bit, $|\cdot|$ is the absolute operator, $round(\cdot)$ denotes the rounding operation to the nearest integer, $W(i,j)$ is the watermark bit at the position (i,j) and $C_0^{'}(k_1,k_2)$ is the modified block. In general, a smaller Δ results in less visibility and poorer robustness while a larger Δ leads to higher visibility and better robustness.

To extract the watermark it is used

$$W^*(i,j) = arg_{\sigma\in\{0,1\}} min(|C_0^{''}(k_1,k_2)|_\sigma - |C_0^*(k_1,k_2)|), \tag{3}$$

where $W^*(i,j)$ is the extracted watermark, $C_0^*(k_1,k_2)$ the element (k_1,k_2) of modified block and $|C_0^{''}(k_1,k_2)|_\sigma$ is defined as

$$|C_0^{''}(k_1,k_2)|_\sigma = \begin{cases} 2\Delta \times round(\frac{|C_0^*(k_1,k_2)|}{2\Delta}) + \frac{\Delta}{2}, & if\ \sigma = 1 \\ 2\Delta \times round(\frac{|C_0^*(k_1,k_2)|}{2\Delta}) - \frac{\Delta}{2} & if\ \sigma = 0 \end{cases}. \tag{4}$$

2.3 Discrete Cosine Transform (DCT)

The DCT [1] is a transform based on the Discrete Fourier Transform (DFT), but using only real numbers. Generally it is not applied to the image directly, but first that image is divided into blocks and then the transformation is applied to each block, resulting in a matrix divided into bands of low, medium and high frequencies. For an image of size $N \times N$ the equations used to calculate the DCT and its inverse (IDCT) are the following:

$$D(u,v) = b(u)b(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{(2x+1)\,u\pi}{2N}\right] \cos\left[\frac{(2y+1)\,v\pi}{2N}\right] \tag{5}$$

$$f(x,y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} b(u)b(v)D(u,v) \cos\left[\frac{(2x+1)\,u\pi}{2N}\right] \cos\left[\frac{(2y+1)\,v\pi}{2N}\right] \tag{6}$$

where D represents the coefficients of the DCT of the image and f represents the function obtained when applying the IDCT. It is also defined that:

$$b(u) = \begin{cases} \frac{1}{\sqrt{N}} & , u = 0 \\ \sqrt{\frac{2}{N}} & , 1 \le u \le N-1 \end{cases} \tag{7}$$

$$b(v) = \begin{cases} \frac{1}{\sqrt{N}} & , v = 0 \\ \sqrt{\frac{2}{N}} & , 1 \leq v \leq N-1 \end{cases} \tag{8}$$

The first coefficient of the matrix obtained when applying the DCT to a block (DC coefficient) is simply the average of the remaining coefficients of the block. The remaining coefficients represent successively increasing frequencies.

2.4 Krawtchouk moments

Yap in [17] introduced the Krawtchouk transform (also known as Krawtchouk moments). These orthogonal moments satisfy the following recurrence relation

$$\alpha_n(Np - 2np + n - x)\overline{K}_n^{p,N}(x) \\ = p(n-N)\overline{K}_{n+1}^{p,N}(x) + \beta_n n(1-p)\overline{K}_{n-1}^{p,N}(x), \quad n \geq 1,$$

with initial conditions

$$\overline{K}_0^{p,N}(x) = \sqrt{w^{p,N}(x)p^{-1}},$$

and

$$\overline{K}_1^{p,N}(x) = (Np - x)(Np)^{-1}\sqrt{w^{p,N}(x)(1-p)(Np)^{-1}},$$

where $\alpha_n = \sqrt{\frac{(1-p)(n+1)}{p(N-n)}}$, $\beta_n = \sqrt{\frac{(1-p)^2(n+1)n}{p^2(N-n)_2}}$, $w^{p,N}(x) = \binom{N}{x}p^x(1-p)^{N-x}$ and $0 < p < 1$.

The Krawtchouk moment of order $(m+n)$ of an image $f(x,y)$ with $M \times N$ pixels is defined as

$$K_{mn} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\overline{K}_m^{p,M}(x)\overline{K}_n^{q,N}(y), \tag{9}$$

where $m \in [0, M-1]$ and $n \in [0, N-1]$.

The image $f(x,y)$ can be reconstructed using

$$f(x,y) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} K_{mn}\overline{K}_m^{p,M}(x)\overline{K}_n^{q,N}(y), \tag{10}$$

where $x \in [0, M-1]$ and $y \in [0, N-1]$.

The lower order Krawtchouk moments store information of a specific region-of-interest of an image, the higher order moments store information of the rest of the image. Therefore, by reconstructing the image from the lower order moments and discarding the higher order moments, a sub-image can be extracted from the subject image. For each additional moment used in reconstructing the image, the square error of the reconstructed image is reduced [17].

The set of lower order Krawtchouk moments is generally the set of perceptually significant components of the image. This choice ensures that the watermark is robust to attacks [18].

3 Dual watermarking techniques

Dual watermarking implies embedding of fragile as well as robust watermarks into the same cover image. It facilitates integration of image authentication and copyright protection into the same scheme. First robust watermarking and then the fragile watermarking should be done because the fragile watermarking is sensitive to small changes. Unlike the fragile watermarking, the robust one resists changes caused by performing the fragile watermarking.

3.1 Common scheme

The robust watermarking method proposed is similar to the one proposed in [2]. The difference consists of considering any binary image as a watermark. In the previous work only a QR code was considered as a watermark, so it was possible a restructuring of the extracted watermark making use of the characteristics related to the QR codes.

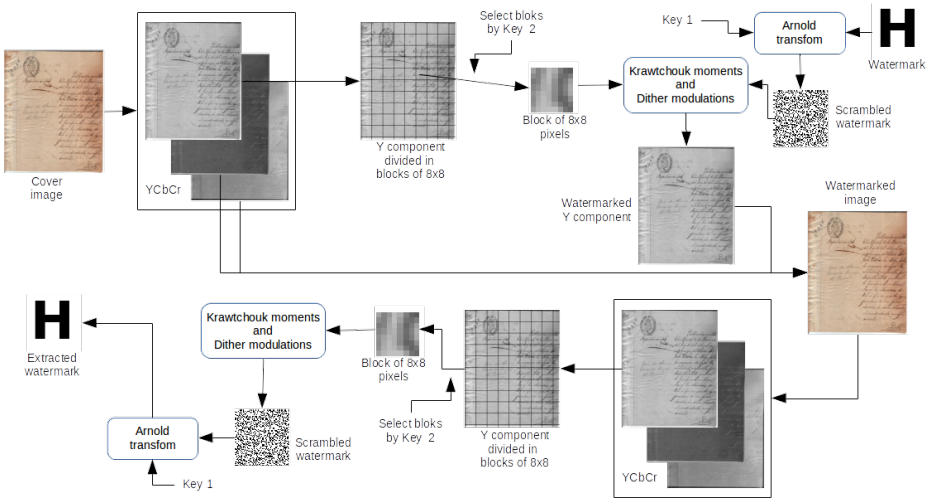

Fig. 1. Watermark embedding and extraction scheme. (Modified from [2])

The following steps are taken during the embedding process:

Step 1: The binary watermark image is scrambled using Eq. 1.
Step 2: The cover image is transformed from RGB to YCbCr color space because RGB color space is highly correlated and is not suitable for robust watermarking applications.
Step 3: The Y component, corresponding to the luminance information in YCbCr color space, is divided into non-overlapping image blocks of 8×8 pixels. We

select the Y component because human visual system is more sensitive to luminance than to the other two chrominance components and the JPEG standard typically use higher density for Y than for the other two components.

Step 4: A number of blocks equal to the number of bits to be inserted is selected from a given key.

Step 5: Each selected blocks are transform from spatial domain to frequency domain. The coefficients $p(u, v)$ of the 2-D 8×8 transformed matrix are zigzag-scanned into 1-D sequence of 64 coefficients $p(k)$, where $k \in [0, 63]$ indicates the zigzag position.

Step 6: Watermark bit is embedded in the $p(c)$ coefficient using Eq. 2. The value of c will be in correspondence with the transform to be used.

Step 7: The YCbCr to RGB color space is transformed to obtain RGB watermarked image.

For watermark extraction:

Step 1: The watermarked image is transformed from the RGB to the YCbCr color space and the Y component is divided into non-overlapping blocks of 8×8 pixels.

Step 2: Some blocks are selected from which they will be extracted from the key used in the embedding process.

Step 3: Each selected blocks are transform from spatial domain to frequency domain and are zigzag-scanned into 1-D sequence of 64 coefficients.

Step 4: Scrambled watermark bits are obtained using Eq. 3.

Step 5: Finally, a watermark is constructed with the scrambled bits using Arnold transform.

For the process of embedding the fragile watermark for tampered small changes, the following steps are performed for each RGB component:

Step 1: The component is divided into 32×32 non-overlapped blocks.

Step 2: 128 pixels of each block are selected by a given key.

Step 3: The least significant bit (LSB) of each selected pixel is assigned the value 0.

Step 4: The MD5 hash value of the modified block is generated as a watermark.

Step 5: The watermark is embedded into the LSB of the selected pixels and a watermarked block image is obtained.

Detecting a fragile watermark is the reverse process of embedding watermark, which is used to detect whether the watermarked image has been tampered and what the precise position of the tampered parts is. For this:

Step 1: The RGB image is divided into 32×32 non-overlapped blocks.

Step 2: 128 pixels of each block are selected by a given key.

Step 3: Three binary series are formed from the LSBs of the selected pixels.

Step 4: The LSBs of each selected pixel are assigned the value 0.

Step 5: The MD5 hash value of the modified block is generated and compared with obtained series.

3.2 DCT-based dual watermarking

In the DCT-based scheme is used the coefficient $p(1)$ in zigzag order, corresponding to the position $(0, 1)$ in the block, because the most number of blocks are concentrated in said coefficient (see Fig. 2); partly because low frequencies hold the most significant information of the image and not affected by the quantitative method of JPEG algorithm.

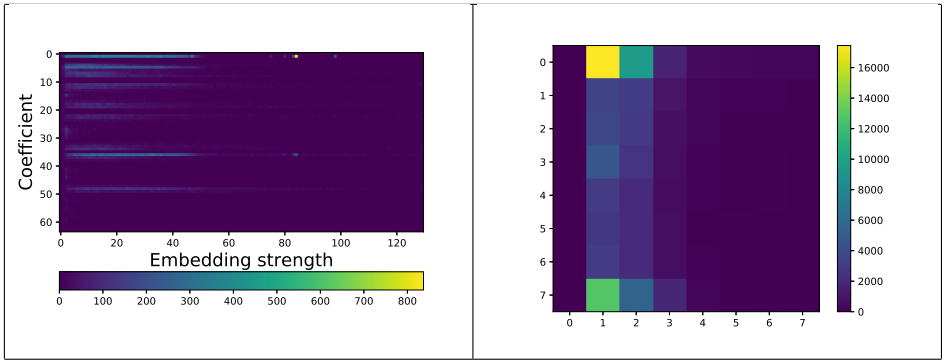

Fig. 2. Quantity of blocks by coefficients where better quality parameters are obtained.

3.3 Krawtchouk moments-based dual watermarking

Unlike DCT-based scheme, in Krawtchouk moments-based watermarking we used $p(19)$, corresponding to the position $(4, 1)$ in the block.

The p and q parameters used in Eq. 9 and Eq. 10 are the parameters of the Krawtchouk polynomials that control their locality behaviour, that define the specific host areas control the horizontal and vertical direction of the watermark localization, respectively. In this work, it was taken $p = q = 0.7$.

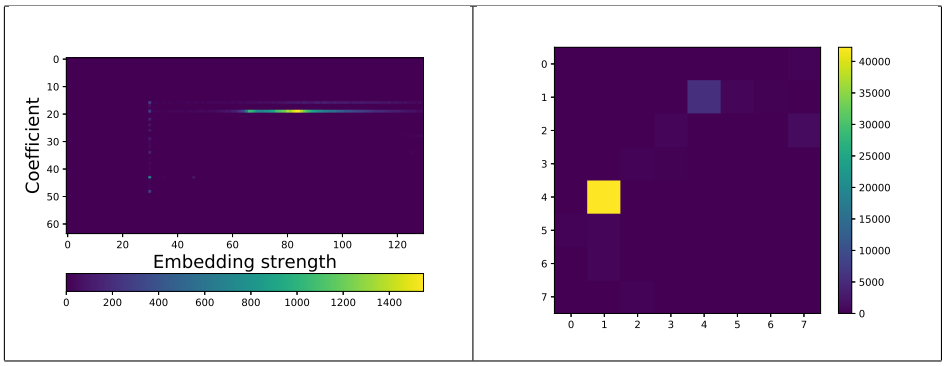

Fig. 3. Quantity of blocks by coefficients where better quality parameters are obtained.

4 Experiments and Results

To verify the performance of the proposed algorithm, the imperceptibility, robustness and tamper detection are tested in Python 3.7.1 using Anaconda 4.6.14. We used two handwriten document image databases: Saint Gall [7] and Parzival [8] database and compressed into JPEG images with the quality factor (QF) of 75, 50 and 25. The first one contains manuscripts from the 9th century using Carolingian scripts by a single writer, while the Parzival is compiled from 13th century Gothic scripts [14].

4.1 Imperceptibility

We calculated the larger peak signal-to-noise ratio (PSNR) which compares the similarity between the original image I, and the watermarked image I_w. A higher PSNR indicates that the watermarked image more closely resembles the original image meaning that the watermark is more imperceptible.

By comparing with the algorithms proposed by [10] and [15], the imperceptibility of the proposed algorithms are verified.

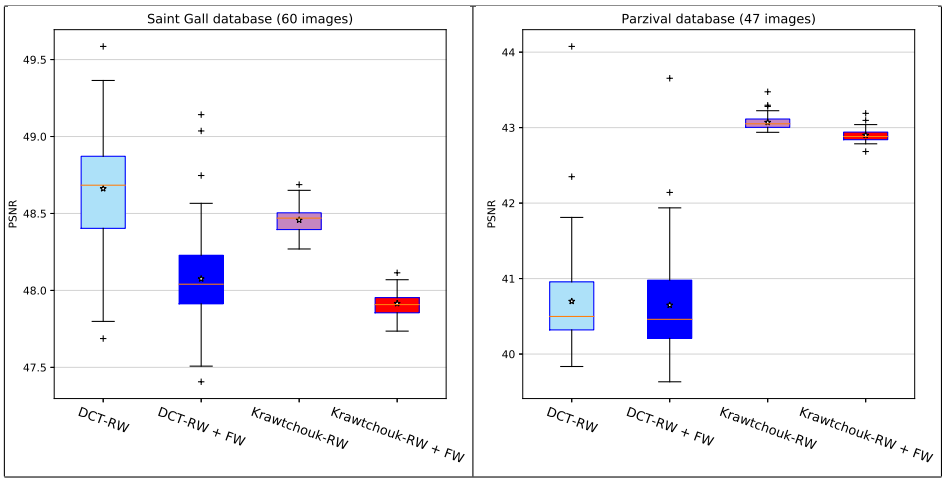

Fig. 4. PSNR values for Saint Gall and Parzival database watermarked images.

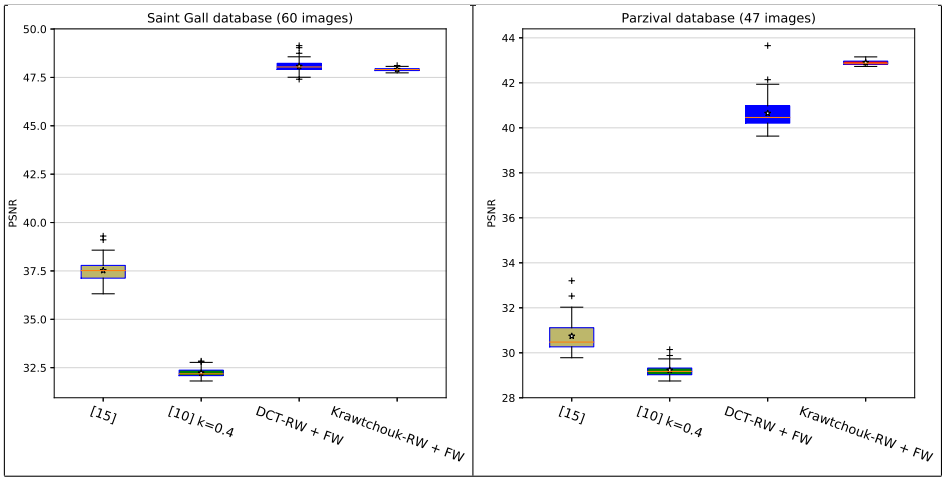

Fig. 5. Comparison with two generic dual watermarking schemes.

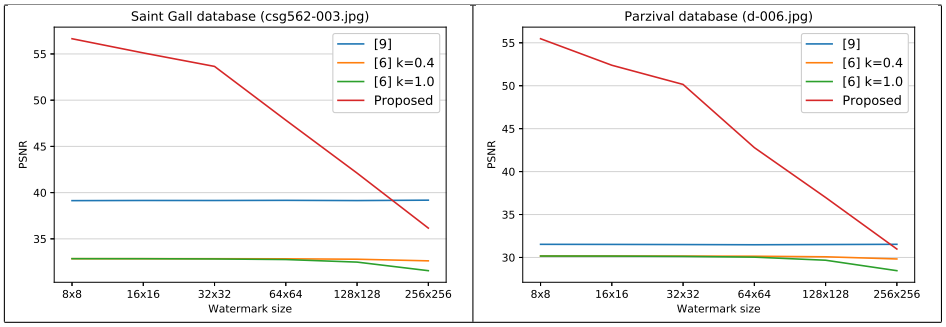

Fig. 6. PSNR behavior to mark the "csg562-003.jpg" image of Saint Gall database and "d-006.jpg" image of Perzival database with watermarks of different sizes.

4.2 Robustness

The robustness is measured as the bit error rate (BER) corresponding to incorrectly formed binary values of the watermark image.

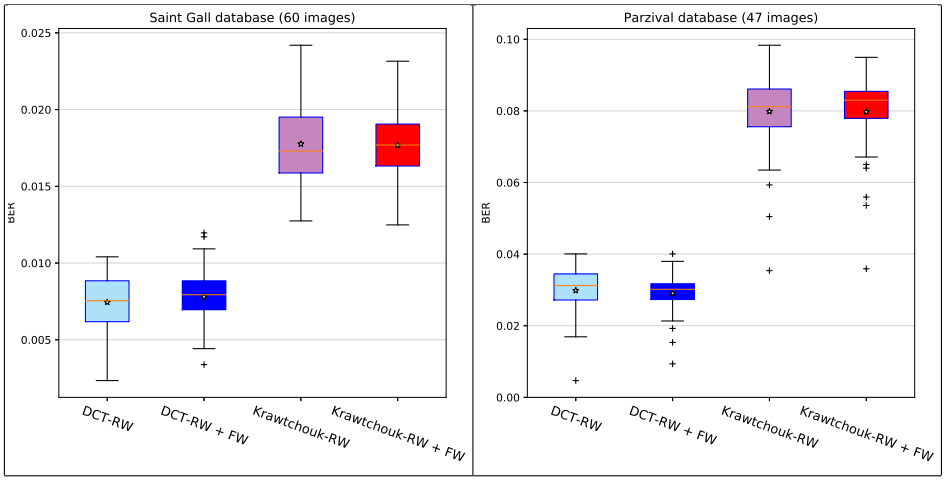

Fig. 7. BER values for watermarked images with JPEG compression (QF=75).

The main contributions of this paper are of twofold. First is the obtaining of better values of imperceptibility, and the second is the remarkable improvement in the strength when JPEG compression attacks with QF 75, 50 and 25 are applied (see Figs. 7-9). Similar to the PSNR, a preliminary experiment, using the same two images, was performed to obtain the corresponding BER by varying the size of the watermark.

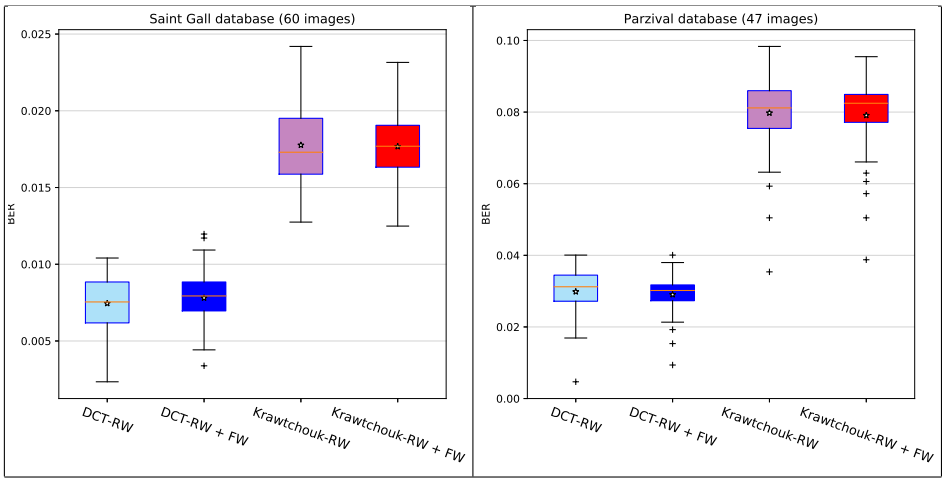

Fig. 8. BER values for watermarked images with JPEG compression (QF=50).

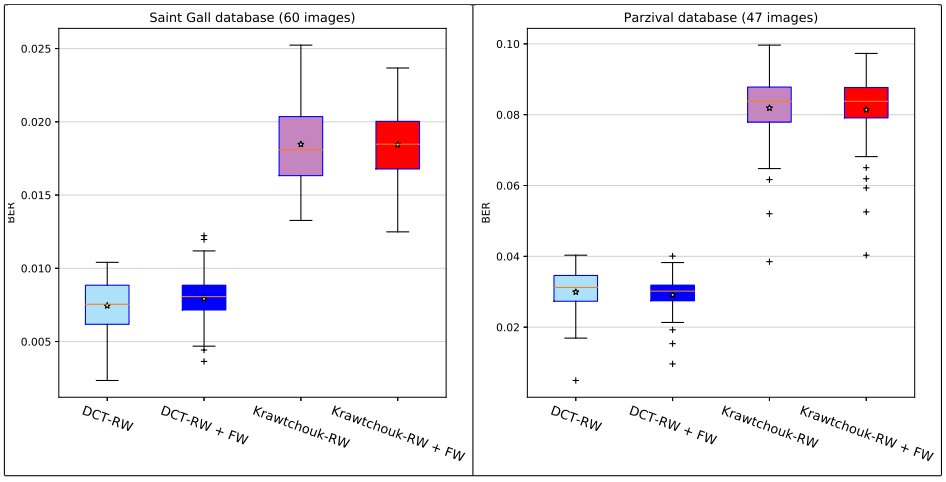

Fig. 9. BER values for watermarked images with JPEG compression (QF=25).

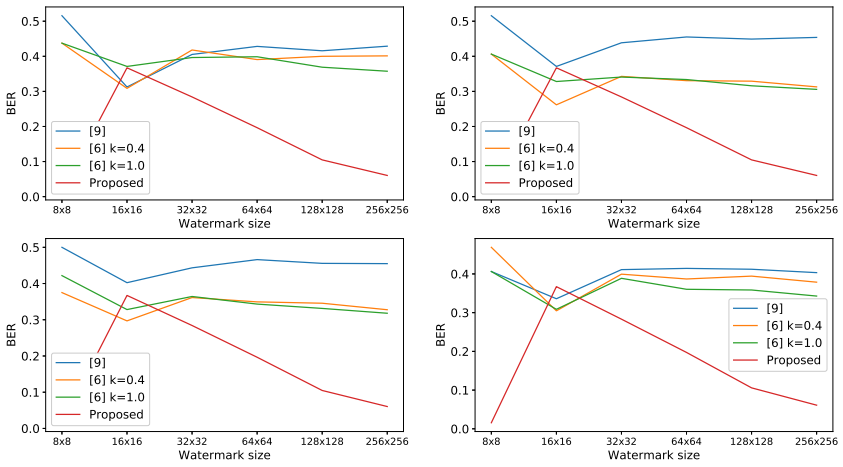

Fig. 10. BER behavior to mark the image "csg562-003.jpg" of Saint Gall database with watermarks of different sizes when no attack is applied, a JPEG compression is performed with QF = 75, 50 and 25 respectively.

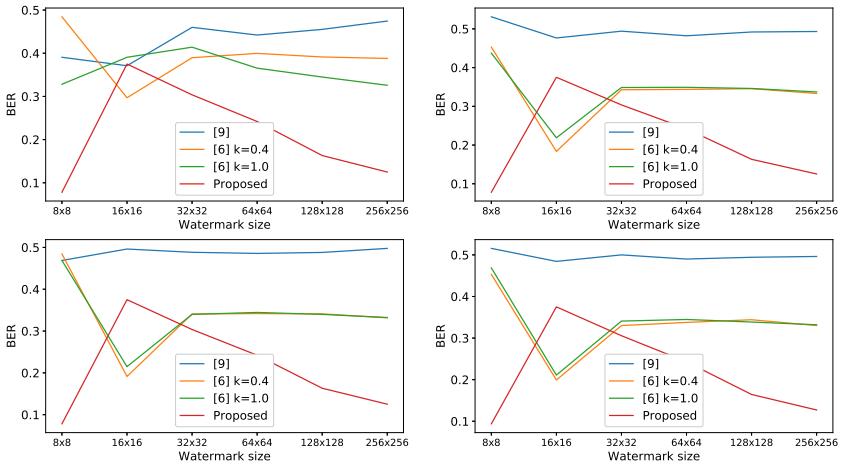

Fig. 11. BER behavior to mark the image "d-006.jpg" of the Parzival database with watermarks of different sizes when no attack is applied, a JPEG compression is performed with QF = 75, 50 and 25 respectively.

4.3 Tamper detection

Fig. 12. Watermarked image, modified watermarked, tamper zone and tamper detection corresponding to [15], [10] and proposed scheme.

Tamper area detection capability is evaluated, by modifying the contents of images. We developed our proposed fragile watermarking particularly for integrity images and locating tampered areas. Fig. 12 shows the modified watermarked

image by text addition, word substitution, underline words, content removal, and their corresponding tamper detection results.

5 Conclusions

In this paper, two dual watermarking techniques based on DCT and Krawtchouk moments for handwritten document images have been proposed and compared. Both transforms are good enough. The experimental results show that the proposed algorithms are robust to JPEG compression.

References

1. Ahmed, N., Natarajan, T., Rao, K.R.: Discrete Cosine Transform. IEEE Transactions on Computers **100**(1), 90–93 (1974)
2. Avila-Domenech, E., Soria-Lorente, A.: Watermarking Based on Krawtchouk Moments for Handwritten Document Images. In: International Workshop on Artificial Intelligence and Pattern Recognition. pp. 122–129. Springer (2018)
3. Cardamone, N., dAmore, F.: DWT and QR Code Based Watermarking for Document DRM. In: International Workshop on Digital Watermarking. pp. 137–150. Springer (2018)
4. 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)
5. Chow, Y.W., Susilo, W., Tonien, J., Zong, W.: A QR Code Watermarking Approach Based on the DWT-DCT Technique. In: ACISP 2017. pp. 314–331 (2017). https://doi.org/10.1007/978-3-319-59870-3
6. Deng, C., Gao, X., Li, X., Tao, D.: A local Tchebichef moments-based robust image watermarking. Signal Processing **89**(8), 1531–1539 (2009)
7. Fischer, A., Frinken, V., Fornés, A., Bunke, H.: Transcription alignment of latin manuscripts using hidden Markov models. In: Proceedings of the 2011 Workshop on Historical Document Imaging and Processing. pp. 29–36. ACM (2011)
8. Fischer, A., Wuthrich, M., Liwicki, M., Frinken, V., Bunke, H., Viehhauser, G., Stolz, M.: Automatic transcription of handwritten medieval documents. In: 2009 15th International Conference on Virtual Systems and Multimedia. pp. 137–142. IEEE (2009)
9. Kang, J., Ji, S.K., Lee, H.K.: Spherical Panorama Image Watermarking Using Viewpoint Detection. In: International Workshop on Digital Watermarking. pp. 95–109. Springer (2018)
10. Liu, X.L., Lin, C.C., Yuan, S.M.: Blind dual watermarking for color images authentication and copyright protection. IEEE Transactions on Circuits and Systems for Video Technology **28**(5), 1047–1055 (2018)
11. Liu, X., Han, G., Wu, J., Shao, Z., Coatrieux, G., Shu, H.: Fractional Krawtchouk transform with an application to image watermarking. IEEE Transactions on Signal Processing **65**(7), 1894–1908 (2017)
12. Muñoz-Ramirez, D.O., Ponomaryov, V., Reyes-Reyes, R., Kyrychenko, V., Pechenin, O., Totsky, A.: A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 619–624. IEEE (2018)

13. Papakostas, G.A., Tsougenis, E., Koulouriotis, D.E.: Moment-based local image watermarking via genetic optimization. Applied Mathematics and Computation **227**, 222–236 (2014)
14. Pastor-Pellicer, J., Afzal, M.Z., Liwicki, M., Castro-Bleda, M.J.: Complete system for text line extraction using convolutional neural networks and watershed transform. In: 2016 12th IAPR Workshop on Document Analysis Systems (DAS). pp. 30–35. IEEE (2016)
15. Shivani, S., Singh, P., Agarwal, S.: A dual watermarking scheme for ownership verification and pixel level authentication. In: Proceedings of the 9th International Conference on Computer and Automation Engineering. pp. 131–135. ACM (2017)
16. Wang, J., Wan, W., Zhang, M., Zou, L., Sun, J.: A blind quantization watermarking scheme for screen content image. In: International Conference on Cloud Computing and Security. pp. 61–71. Springer (2018)
17. Yap, P., Paramesran, R., Ong, S.H.: Image Analysis by Krawtchouk Moments. IEEE Trans. Image Process. **12**(11), 1367–1377 (2003)
18. Yap, P.T., Paramesran, R.: Local watermarks based on Krawtchouk moments. In: TENCON 2004. 2004 IEEE Region 10 Conference. pp. 73–76. IEEE (2004)
19. Zhu, X.S., Sun, Y., Meng, Q.H., Sun, B., Wang, P., Yang, T.: Optimal watermark embedding combining spread spectrum and quantization. EURASIP Journal on Advances in Signal Processing **2016**(1), 74 (2016)