Dual watermarking for handwritten document image authentication, tamper detection and copyright protection for JPEG compression attacks

Ernesto Avila-Domenech[1] [0000−0002−4797−289X], Anier Soria-Lorente[1] [0000−0003−3488−3094], and Alberto Taboada-Crispi[2] [0000−0002−7797−1441]

[1] Universidad de Granma, Carretera Central vía Holguín Km $\frac{1}{2}$, Granma, Cuba
{eadomenech, asorial1983}@gmail.com
[2] Universidad Central de Las Villas, Villa Clara, Cuba
{ataboada}@uclv.edu.cu

Abstract. For authentication, tamper detection and copyright protection of handwritten document images, a dual watermarking algorithm that connects the robust watermarking algorithm based on Krawtchouk moments with a fragile watermarking algorithm based on MD5 hash function is presented. Hence, the robust watermarking algorithm is used to guarantee robustness by modifying frequency coefficients in Krawtchouk moments. Thus, this study proposes a fragile watermarking algorithm, which can perceive in time when the protected image is tampered. Experimental results show that the proposed algorithm can be used for copyright protection for JPEG compression attacks and tampering detection of this images.

Keywords: Handwritten · Image · Watermarking.

1 Introduction

The explosive growth of digital multimedia techniques, together with the rapid development of digital network communication has created a pressing demand for techniques that can be used for content authentication and copyright protection. Due to these needs, digital rights management (DRM) is gaining importance; it refers to a range of access control technologies used to limit or restrict the use of digital content. Digital watermarking is useful in DRM systems as it can hide information within the digital content like images, audio and video.

Watermarking technique is effectively applied to content authentication and copyright protection. In accordance with the desired robustness of the embedded watermark, digital watermarking techniques are divided into fragile watermarking and robust watermarking. The first ones is designed to detect slight changes to the watermarked image with high probability and the second ones is typically used for copyright protection, thus it is designed to resist attacks that attempt to remove or destroy the watermark without significantly degrading the visual quality of the watermarked image.

When users want to detect illegal tampering and protect the copyright at the same time, the single watermarking algorithm cannot meet the needs of users. Therefore, a dual watermarking algorithm is developed, as it can effectively combine the advantages and functions of the two watermarks [12].

Numerous dual watermarking algorithms have been proposed. In [7] is presented a dual watermarking technique which attempts to establish the owners right to the image and detect the intentional and unintentional tampering of the image. However, this early research is simply a combination of visible and invisible watermarking algorithms. In [12] is presented a dual watermarking algorithm that connects the robust watermarking algorithm based on singular value decomposition (SVD) with a fragile watermarking algorithm based on compressive sensing (CS). In [11] use cryptography and QR Code in combined approach of LSB and DCT, the authors combines the LSB and DCT approach because LSB contain spatial domain property and DCT contain frequency domain property.

[9] provides dual functionalities of ownership assertion and authentication. In [6] is presented a blind dual watermarking mechanism for digital color images. The first watermark is embedded by using the discrete wavelet transform (DWT) in YCbCr color space, and it can be extracted blindly without access to the host image. However, fragile watermarking is based on an improved least significant bits (LSB) replacement approach in RGB components for image authentication. In [10] is presented a lifting wavelet transform (LWT) and discrete cosine transform (DCT) based robust watermarking approach for tele-health applications. They are based on LWT requires less memory, reduced aliasing effects and distortion, fast and it is a good choice for low computational complexity than conventional DWT.

The rest of the paper is organized as follow; Section 2 describes the proposed method including robust watermarking and fragile watermarking. Experimental results are given in Section 3 and Section 4 concludes the paper.

2 Proposed method

Dual watermarking implies embedding of robust as well as fragile watermarks into the same cover image. It facilitates integration of copyright protection and integrity verification 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, robust watermarking resists changes caused by performing the marked fragile.

2.1 Robust watermarking

The robust watermarking method proposed is similar to the one proposed in [2]. The difference consists in considering any binary image as a watermark. In the previous work only a QR code was considered as a watermark.

The following steps are taken to embedding process:

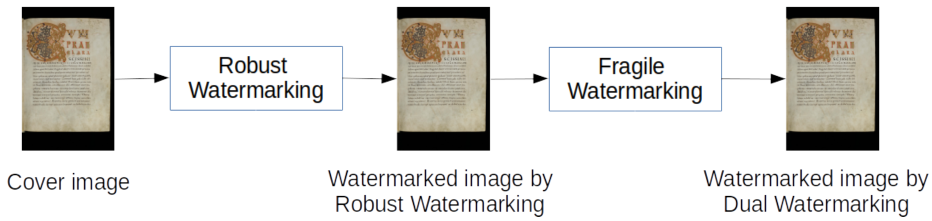

Fig. 1. Dual watermarking scheme.

1. The binary watermark image is scrambled using Arnold transform [1].
2. The cover image is transformed from RGB to YCbCr color space, and the Y component, corresponding to the luminance information, is divided into small image blocks of 8×8 pixels.
3. A number of blocks equal to the number of bits to be inserted is selected from a given key.
4. The Krawtchouk moments [13] of selected blocks are determined.
5. Watermark bit is embedded in the selected block moments using Dither modulation [3]. The values 19 and 128 are used as the coefficient and embedding strength values respectively. Watermarked blocks can be obtained.
6. Conversion from YCbCr to RGB is performed to obtain RGB watermarked image.

For watermark extraction:

1. The watermarked image is transformed from the RGB to the YCbCr color space and the Y component is divided into 8×8 pixels blocks.
2. Some blocks are selected from which they will be extracted from the key used in the embedding process.
3. The Krawtchouk moments of selected blocks are determined.
4. Scrambled watermark bits are obtained with the selected blocks moments using Dither modulations.
5. Finally, a watermark is constructed with the scrambled bits using Arnold transform.

2.2 Fragile watermarking

As we know, hash function, such as MD5 or SHA-256, can be utilized to authenticate the data. If the hash value of original message is exactly equal to the re-calculated hash value of the received message, the received data can be regarded as integrated, otherwise as false.

For the process of embedding the following steps are performed each RGB component:

1. The component is divided into 32×32 non-overlapped blocks.
2. 128 pixels of each block are selected by a given key.

3. The least significant bit (LSB) of each selected pixel is assigned the value 0.
4. The MD5 hash value of the modified block is generated as a watermark.
5. The watermark is embedded into the LSB of the selected pixels and watermarked block image is obtained.

Detecting a fragile watermark water 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:

1. The RGB image is divided into 32×32 non-overlapped blocks.
2. 128 pixels of each block are selected by a given key.
3. Three binary series are formed from the LSBs of the selected pixels.
4. The LSBs of each selected pixel are assigned the value 0.
5. The MD5 hash value of the modified block is generated and compareted with obtained series.

3 Experiments and Results

The watermarking algorithm is evaluated through imperceptibility, tamper detection and robustness, and the following experiments are introduced.

We used two handwriten document image databases: Saint Gall [4] and Parzival [5] database. 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 [8].

3.1 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 PSNR indicates that the watermarked image more closely resembles the original image meaning that the watermark is more imperceptible.

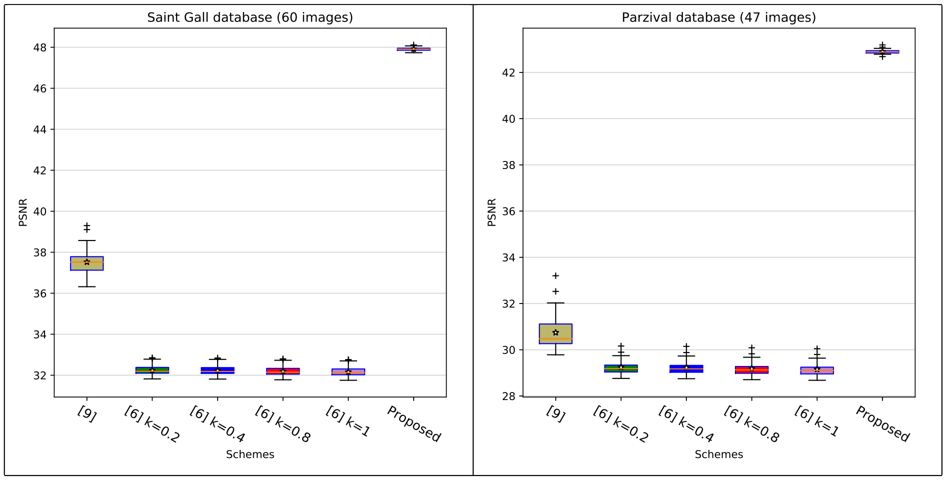

Fig. 2. PSNR values for Saint Gall and Parzival database watermarked images.

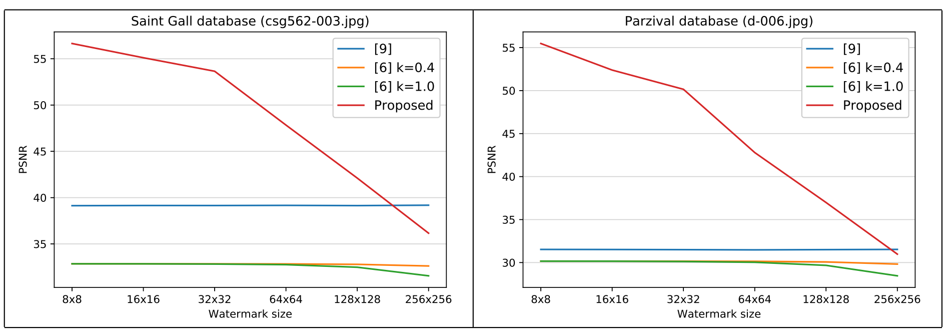

Fig. 3. PSNR behavior to mark the “csg562-003.jpg” image of Saint Gall database and “d-006.jpg” image of Perzival database with watermarks of different sizes.

3.2 Tamper detection

Tamper area detection capability is evaluated, by modifying the contents of images, adding and removing content. We developed our proposed fragile watermarking particularly for integrity images and locating tampered areas. Fig. 2 shows the attacked images and their corresponding tamper detection results.

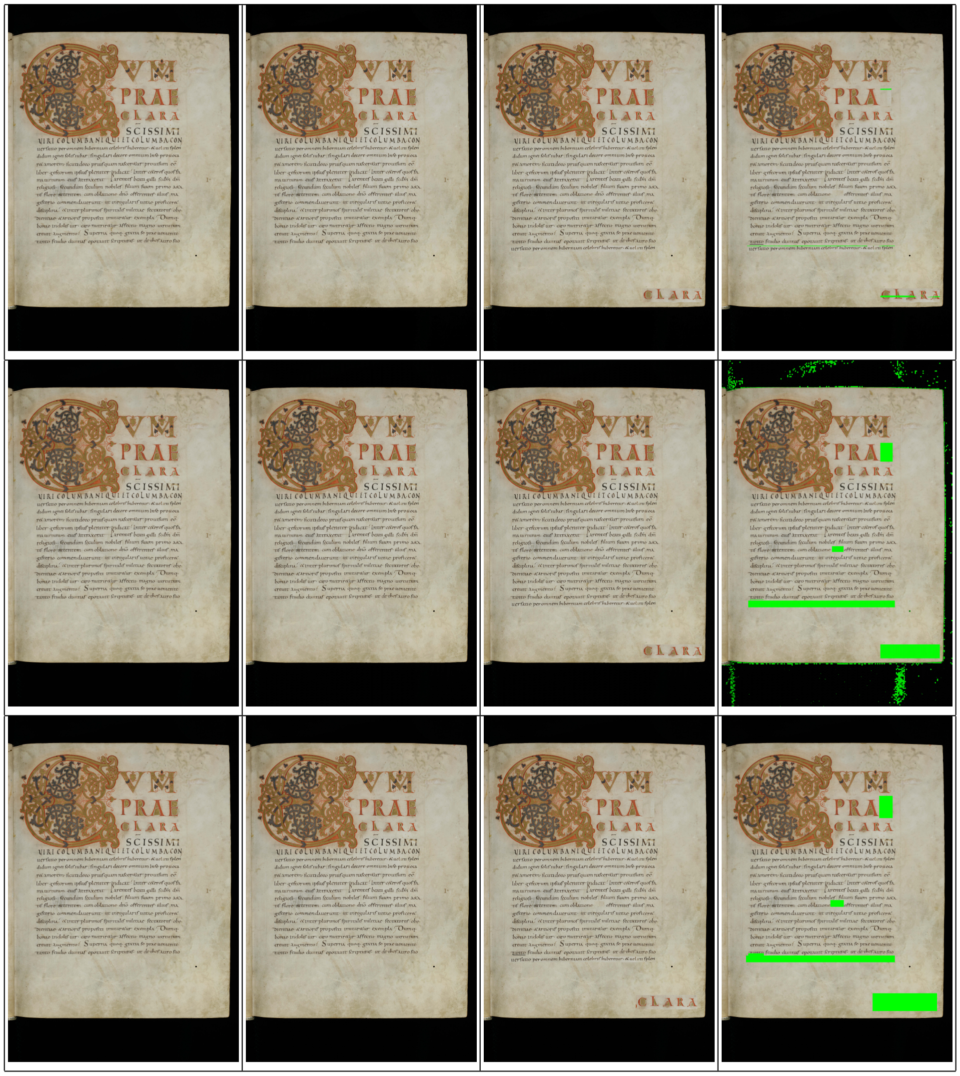

Fig. 4. Cover image, watermarked image, modified watermarked image by text addition and content removal, and tamper detection.

3.3 Robustness

The bit error rate (BER) is defined as ratio between number of incorrectly decoded bits and total number of bits.

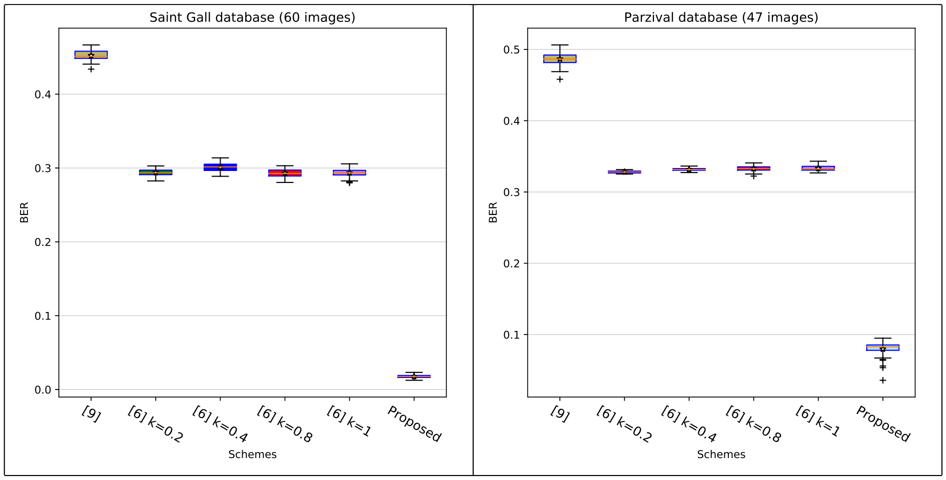

Fig. 5. BER values for watermarked images with JPEG compression (QF=75%).

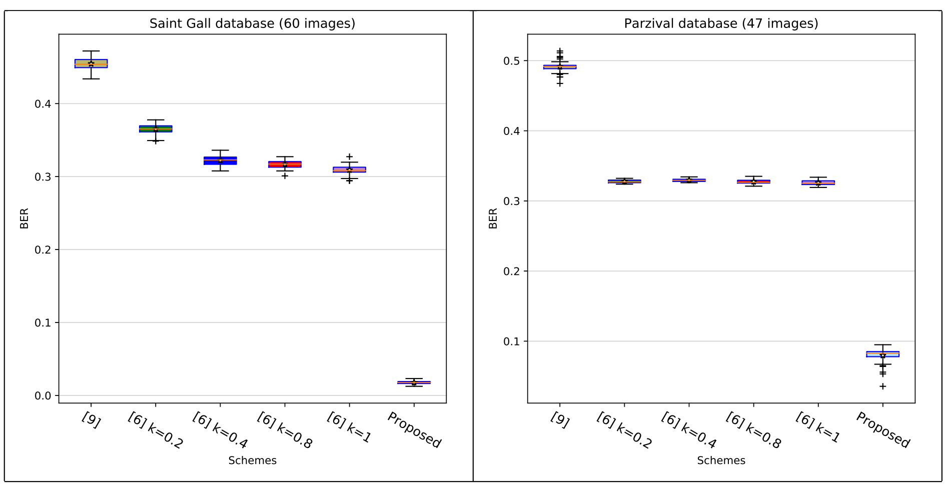

Fig. 6. BER values for watermarked images with JPEG compression (QF=50%).

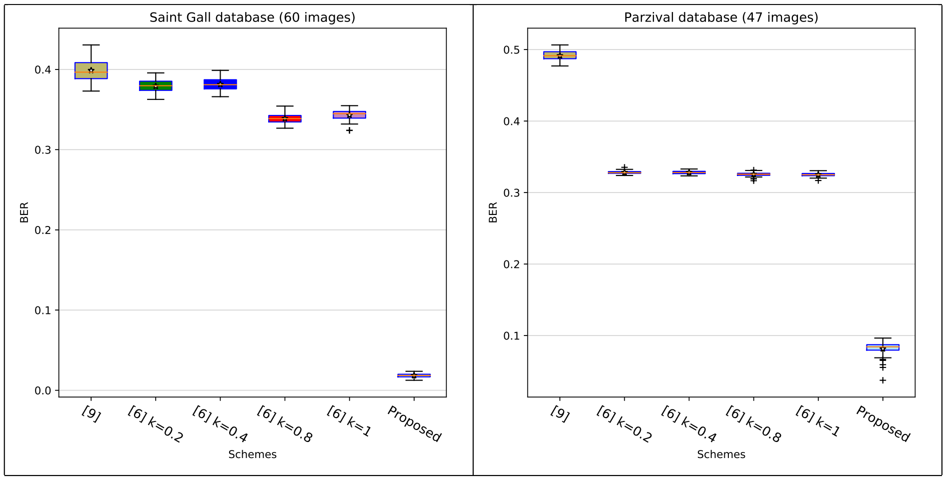

Fig. 7. BER values for watermarked images with JPEG compression (QF=25%).

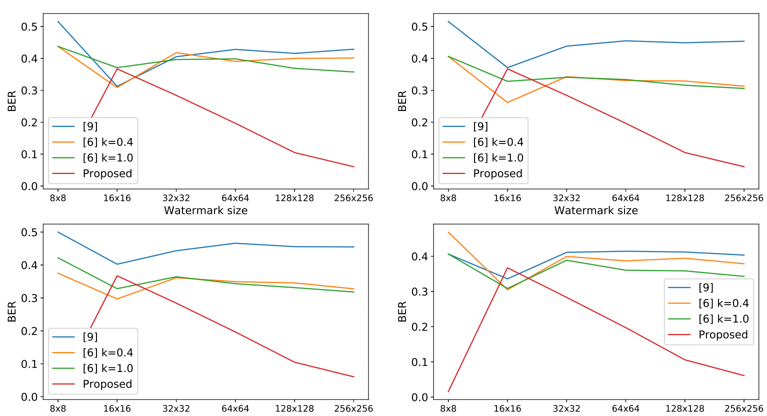

Fig. 8. BER behavior to mark the image "csg562-003.jpg" of Saint Gall database with watermarks of different sizes.

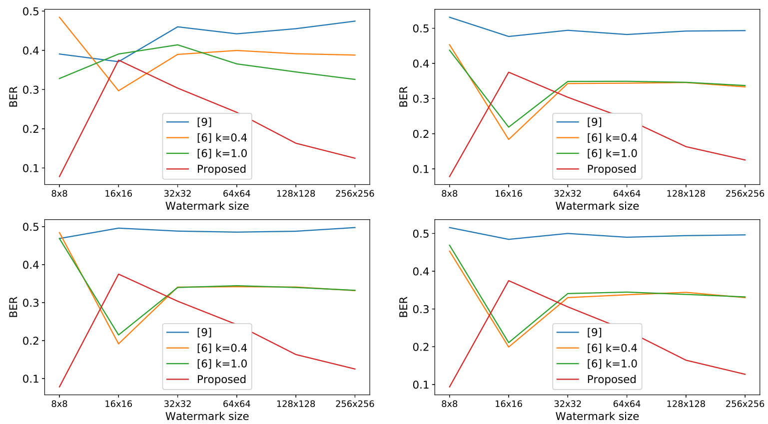

Fig. 9. BER behavior to mark the image “d-006.jpg” of Parzival database with watermarks of different sizes.

4 Conclusions

In this paper, a dual digital watermarking technique based on Krawtchouk moments and MD5 hash function was implemented. The results show a BER less than ... In addition, the values corresponding to the PSNR were improved compared to previously presented papers.

References

1. Arnol’d, V.I., Avez, A.: Ergodic problems of classical mechanics. The mathematical physics monograph series, W. A. Benjamin, New York, NY (1968), http://cds.cern.ch/record/1987366
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. 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)
4. 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)
5. 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)

6. 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)
7. Mohanty, S.P., Ramakrishnan, K., Kankanhalli, M.: A dual watermarking technique for images. In: Proceedings of the seventh ACM international conference on Multimedia (Part 2). pp. 49–51. Citeseer (1999)
8. 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)
9. 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)
10. Singh, A.: Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. Multimedia Tools and Applications pp. 1–11 (2019)
11. Singh, R.K., Shaw, D.K.: A hybrid concept of cryptography and dual watermarking (lsb_dct) for data security. International Journal of Information Security and Privacy (IJISP) **12**(1), 1–12 (2018)
12. Wang, N., Li, Z., Cheng, X., Chen, Y.: Dual Watermarking Algorithm Based on Singular Value Decomposition and Compressive Sensing. In: 2017 IEEE 17th International Conference on Communication Technology (ICCT). pp. 1763–1767. IEEE (2017)
13. Yap, P., Paramesran, R., Ong, S.H.: Image Analysis by Krawtchouk Moments. IEEE Trans. Image Process. **12**(11), 1367–1377 (2003)