A novel QR-code based watermarking scheme for digital rights

Stefano Chiavarelli
Presidency of the Council of Ministers
Via di Santa Susanna 15, 00187 Rome, Italy
chiaste@gmail.com

Fabrizio d'Amore
Sapienza University of Rome
Via Ariosto 25, 00185 Rome, Italy
damore@diag.uniroma1.it

Abstract

This paper presents a digital rights protection scheme for both colour and grayscale images using a novel approach that combines watermarking and cryptography. The schema involves two parties: the owner of the digital rights and a generic user who acquired some rights on a copy of the image that will be watermarked. The watermark, a QR code derived from a signed "License Agreement", is repeatedly inserted, and scrambled, by the image right's owner, into the frequency components of the image, thus producing the watermarked image. The schema, a non-blind type, achieves good perceptive quality and fair robustness using the 3rd level of the Discrete Wavelet Transform. The experimental results show that, inserting more occurrences of a scrambled QR code, the proposed algorithm is quite resistant to JPEG compression, rotation, cropping and salt & peeper noise.

CEUR-WS.org/Vol-2254/10000029.pdf

1 Introduction

Due to the fast ICT evolution of the last 25 years and the very low cost of digital equipment, images are nowadays very popular and can be considered a basic tile of modern documents; hence the vital need for protecting the digital content and in particular the digital rights. Possible scenarios are for example a photographer who wants to sell a particular image to a newspaper, for a use exclusive or not, and wants to preserve her intellectual rights or a bookstore that sells a digital copy of a book, article or paper to a customer and wants to "mark" that copy in order to avoid its illegal diffusion. Author's proofs of ownership and intellectual property are usually specified outside the image, using a visible watermark or embedded into specific fields of the EXIF standard format. Either visible watermarks or EXIF fields can be deleted using for example image editors. An invisible and scrambled watermark could be a valid solution, discouraging unauthorized copying and distribution of digital data. In this paper, we propose a novel digital image watermarking algorithm based on the combination of Discrete Wavelet Transform [Dau90, RVH96], QR Code[Wav] and cryptography. We will show that the use of these three elements assures good imperceptibility, watermark extraction performance and robustness against most common image manipulations like JPEG compression, rotation, cropping and additive noise.

In particular, a document describing digital rights definition on an image is used as the input of a hmac-sha256 function whose result is then injected, as a watermark, into a copy of the image. To embed such

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Marco Schaerf, Massimo Mecella, Drozdova Viktoria Igorevna, Kalmykov Igor Anatolievich (eds.): Proceedings of REMS 2018 – Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, Stavropol – Dombay, Russia, 15–20 October 2018, published at http://ceur-ws.org

data into the image, the original copy is decomposed into its 3rd level Discrete Wavelet components, where the watermark is inserted into the lower frequency components. We chose a QR Code as type of watermark [KLH13, CCC14] because of its error correction capability and because it is visually perceptible. In order to improve imperceptibility and extraction performances, we insert it into the host image more times, in a key-scrambled version. After watermark insertion we need to perform an Inverse Discrete Wavelet transform to obtain the watermarked image. For such a non-blind schema, to extract the watermark is necessary to provide the original image, while the QR Code is used only to compare its payload to the one extracted from the watermarked image.

2 Preliminaries

Digital watermarking could be considered a sort of steganography. Image watermarking techniques can be classified [CCCM10, HH13, Rak13, HYAAQ12, KK11] into different categories according to the type of domain in which data embedding takes place and the type of information is needed to extract the watermark. There are mainly two domain types [RCSD13]: spatial and frequency. Regarding what is needed to extract the watermark from the image we can divide the cases into blind, semi-blind and non-blind systems [NVR16]. A blind watermark, or public watermarking algorithm, requires neither the cover image (original image) nor the embedded watermark to extract it from the watermarked image; a semi-blind, or semi-private scheme, requires only the watermark and finally a blind scheme requires at least the cover image. Spatial image watermarking techniques [RMK15] are commonly used in a “pure” steganographic context because, hiding data into the least significant bits of an image, achieves to embed large quantity of data but the watermark is not robust to common manipulations like JPEG compression [TCZA14]. In frequency domain the most common techniques [SK15] are based on Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). Due to the block divide algorithm used generally by DCT watermarking, these techniques are robust against JPEG compression but are not resistant to rotation, translation and image cropping. Instead, embedding data using the DWT assures good robustness against the most popular image manipulations [XSSL04]. Wavelet transform is a modern technique that was first used to study non-stationary events like earthquakes. Digital images properties can be better expressed through a wavelet transform since the frequency components are quickly varying around the image area. The main difference from the DCT is that the DWT transform is based on a sum of scaled and shifted “mother” wavelets that have a limited duration. Through the wavelet decomposition the original signal can be represented by its coefficients which contains the spatial information. Each level of a DWT produces four types of coefficients: LL, or approximation coefficients, that represent the low frequency part of the image (most of information) and the details coefficients LH, HL and HH (vertical, horizontal and diagonal). Fig. 1 illustrates the sub-band decomposition of an image using 2D wavelet transform after 3 levels of decomposition. In every level the decomposition is obtained on the LL component of the previous level. The original signal can be completely reconstructed performing the Inverse Wavelet Transformation [Mal89] on these coefficients. In order to achieve a good visual imperceptibility, according to the spectral sensitivity of human eye, the blue component of a colour image is most suitable for hiding data [Gol09]. Data hiding system performances [Ber14] are described in terms of imperceptibility, embedding capacity and robustness. For digital watermarking the most important are imperceptibility and robustness.

To measure visual imperceptibility between two images the most used indices are Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity [WBSS04]:

$$\mathrm{MSE} = \frac{1}{m \cdot n} \sum_{i=1}^{m} \sum_{j=1}^{n} (X(i,j) - X'(i,j))^2$$

$$\mathrm{PSNR} = 10 \log_{10} \frac{\mathrm{MAX}_i^2}{\mathrm{MSE}}$$

$$\mathrm{SSIM} = \frac{(2\mu_i \mu_j + C_1)(2\sigma_{ij} + C_2)}{(\mu_i^2 + \mu_j^2 + C_1)(\sigma_i^2 + \sigma_j^2 + C_2)}$$

where:

- m and n are the number of rows and columns of the image expressed in pixel, $X(i,j)$ is the value of the pixel at row i and column j of the original image, $X'(i,j)$ is the value of the pixel at row i and column j of the watermarked image;

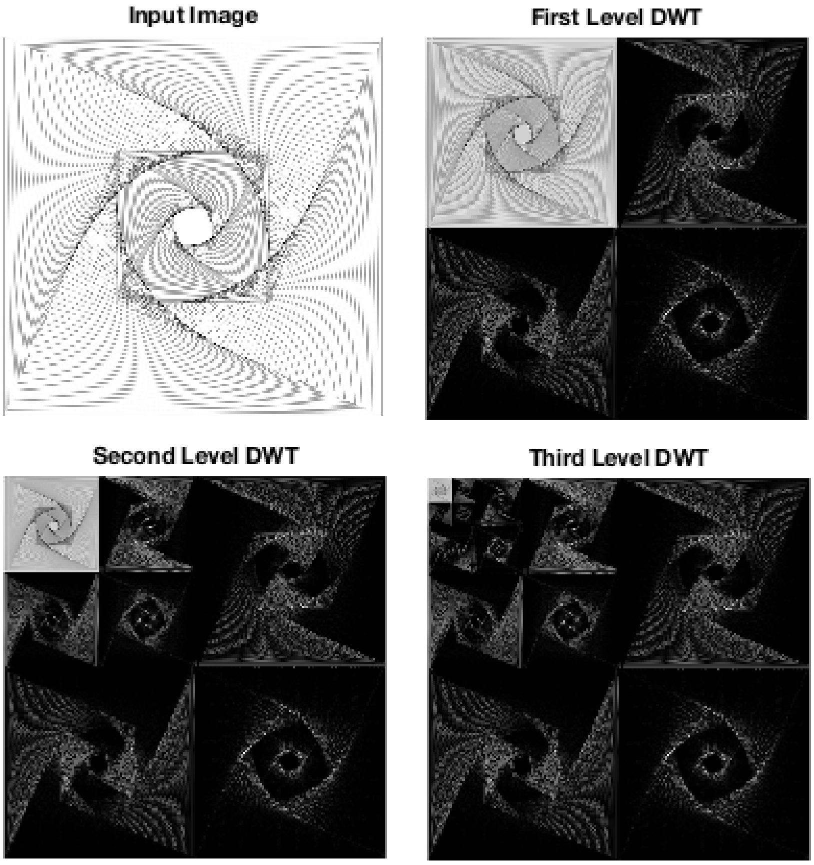


Figure 1: Original image, DWT Levels 1, 2 and 3.

- MAX_i is the biggest value of a pixel, MSE is the Mean Squared Error;
- μ, σ and σ_{ij} are, respectively, mean, standard deviation and correlation, and C_1, C_2 are constants.

Digital image watermarking robustness can be evaluated in terms of correct watermark extraction after an image alteration. Common image manipulations regard JPEG compression, rotation, cropping and additive noise.

The Quick Response Code (QR Code) was developed during the 80's in Japan by Denso Wave company and used to monitor automotive spare parts and became a standard more than 20 years ago. It consists of black squares arranged into a white grid and uses Reed-Solomon error correction codes [ISO15]. According to its visual identification and error correction property it achieves good robustness against image degradation.

3 Technical design

In this section we describe the procedure to both generate and verify the watermarked image, starting from the original image and its digital rights specification. Suppose Bob is the owner of the original image and Alice is interested in buying a copy of it, whereas Bob prefers to keep his digital rights. So they create a document containing at least these items:

- original image thumbnail and hash;
- Bob personal data;
- digital rights regarding the image;
- Alice personal data.

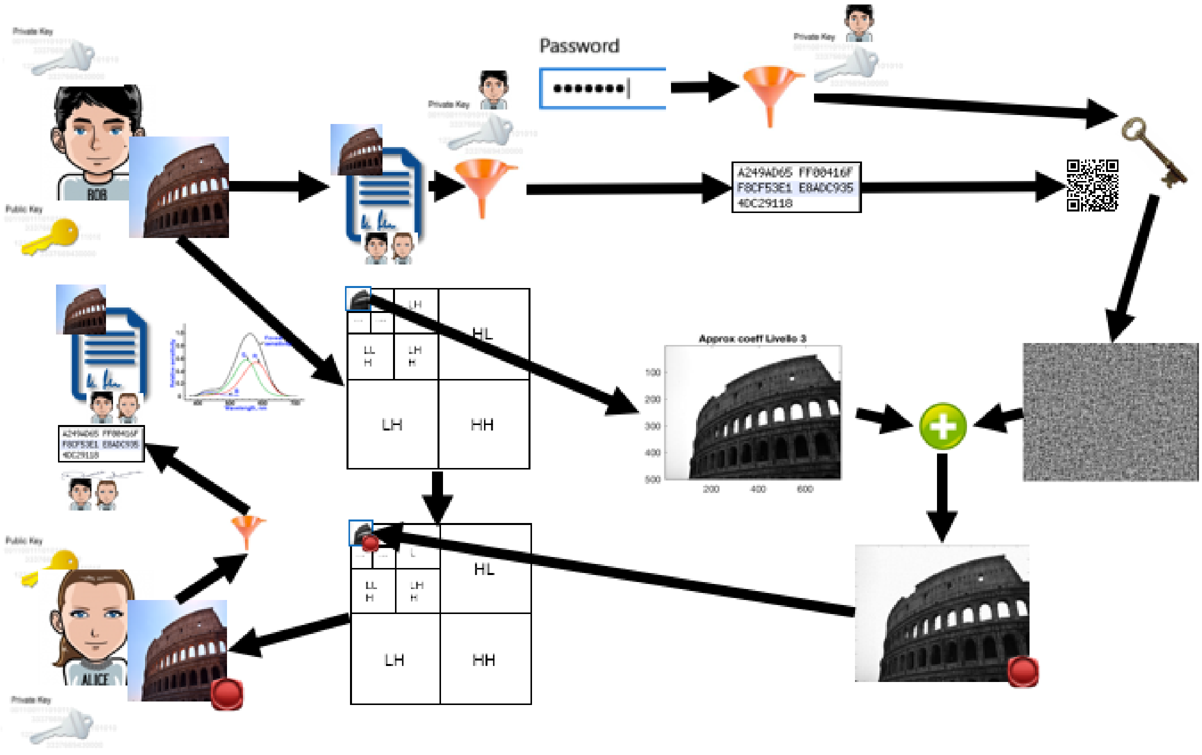


Figure 2: Injection schema

This document is then signed by both parties using their own private keys. Fig. 2 presents the watermark injection procedure. Starting from the original image (Fig. 4(a)) and the signed document, Bob produces the watermarked image for Alice by the following steps:

- computes the approximation coefficients of level 3 ($\mathrm{AC}_{\mathrm{LL3}}$) by performing a third-level decomposition of the image using a wavelet (blue component in case of colour image);
- produces a QR-code encoding the hmac-sha256 of the signed document using his private key;
- derives a scrambling key from a hmac-sha256 of a password and use it to scramble the QR-code repetitions necessary to fit the size of the $\mathrm{AC}_{\mathrm{LL3}}$ $(N \times M)$ (Fig. 3(a)) of the image obtaining WIM $(N \times M)$ (Fig. 3(b));
- insert the watermark into the approximation coefficients of level 3 of the watermarked image $\mathrm{WAC}_{\mathrm{LL3}}(i,j) = \mathrm{AC}_{\mathrm{LL3}}(i,j) + k \cdot \mathrm{WIM}(i,j)$, $i = 1, 2, \dots, N$ and $j = 1, 2, \dots, M$, with $k = 20000$ for colour images and $k = 15000$ for black and white ones;
- obtain the watermarked image (Fig. 4(b)) by performing the inverse discrete wavelet transform.

The hash of the resulting watermarked image is appended to the signed document and finally signed once again by both Bob and Alice. The watermark extraction procedure (Fig. 5) can be done only by Bob because we need his private key and the unscrambling password. Starting from the original image (Fig. 4(a)) and the watermarked image it is necessary to:

- compute the approximation coefficients of level 3 by performing a third-level decomposition of the image using a wavelet (blue component in case of colour image) for both original ($\mathrm{AC}_{\mathrm{LL3}}$) and watermarked image ($\mathrm{WAC}_{\mathrm{LL3}}$);
- reconstruct WIM:

$$\mathrm{WIM}(i,j) = \begin{cases} 1 & \text{if } \mathrm{WAC}_{\mathrm{LL3}}(i,j) - \mathrm{AC}_{\mathrm{LL3}}(i,j) \geq t \\ 0 & \text{otherwise} \end{cases}$$

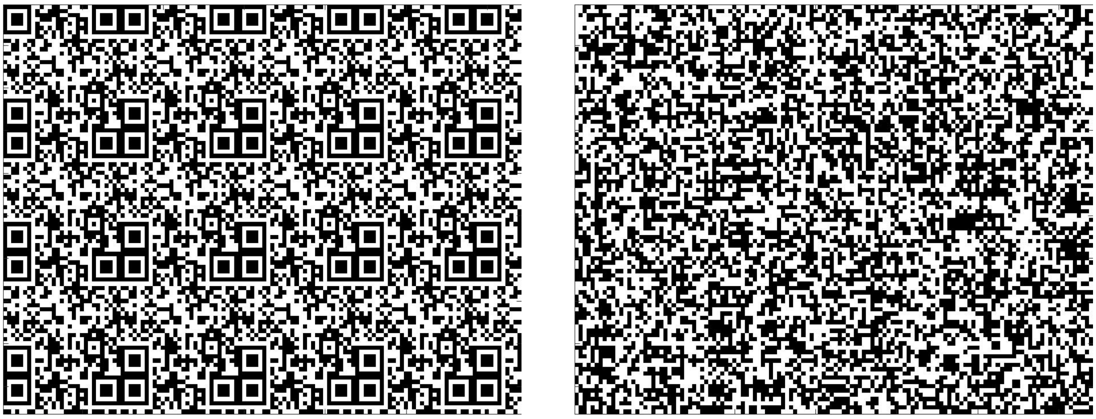

(a) (b)

Figure 3: WIM: (a) unscrambled; (b) scrambled.

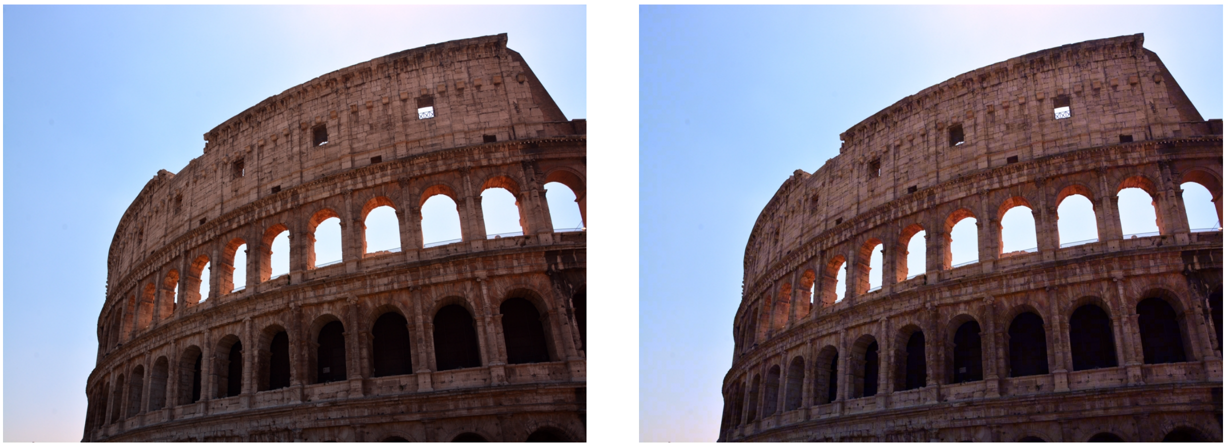

(a) (b)

Figure 4: Images: (a) original picture; (b) watermarked picture.

for $i = 1, 2, \ldots, N$ and $j = 1, 2, \ldots, M$, with $t = 40$ for colour images and $t = 22.5$ for black and white ones, obtaining a scrambled watermark (Fig. 3);

- descramble by using the key derived from the hmac-sha256 of Bob's password;
- compute hmac-sha256 of the document using Bob's private key;
- recover the QR-code from the single QR-code repetions occurring in the descrambled image (Fig. 3) and verify if the decoded value is equal to the hmac-sha256 of the document (for payload extraction is used either each single extracted repetition of a QR code either a reconstructed QR code based on majority pixel value matching, upon 1 to the maximum value of them).

4 Results and examples

We implemented this technique in MATLAB using as original images the ones represented in Fig. 7.[1] We used the open-source library "libqrencode" [Ken18] for QR code generation and the "quirc" library [Dan12] for QR code decoding. All images are of equal size 512 × 512 and were tested with different Alice and Bob keys with the first 20 wavelets of the Daubechies family [Dau92]. The results show that the algorithm achieves fairly good results in terms of imperceptibility (Fig. 8). For every image and wavelet the robustness of the watermarking schema was evaluated through the correct extraction and decoding of the QR code from the watermarked image that has

[1] Source code, available under the GPL-3.0 license, can be dowloaded from `http://www.diag.uniroma1.it/~damore/watermarking/src/sorgenti.tar.gz`.

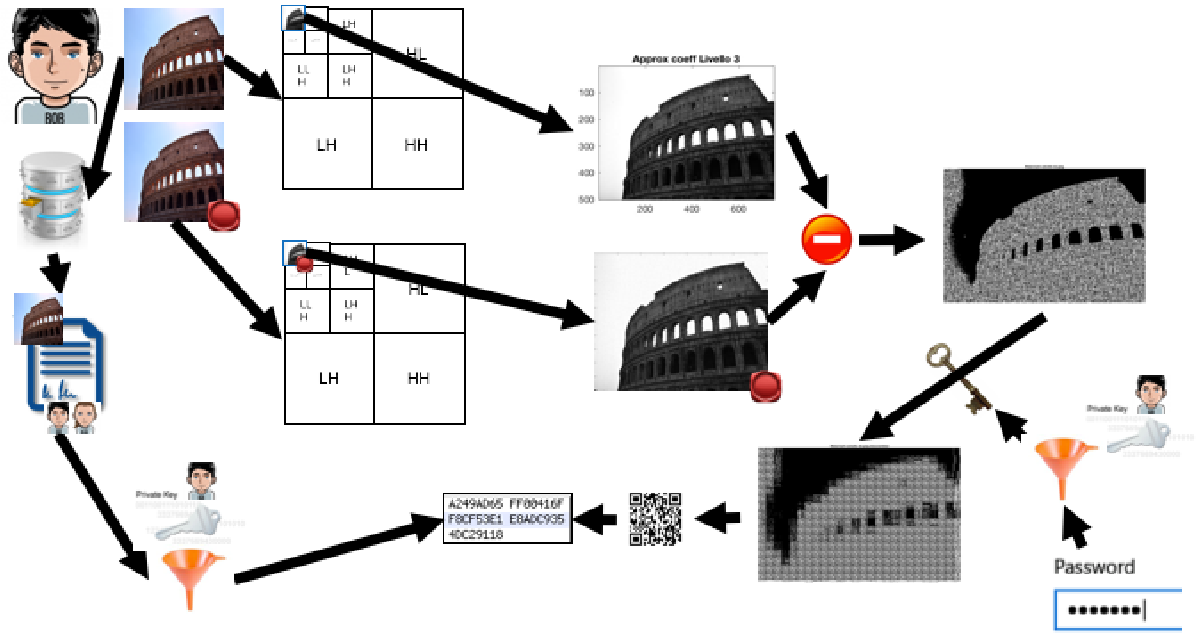
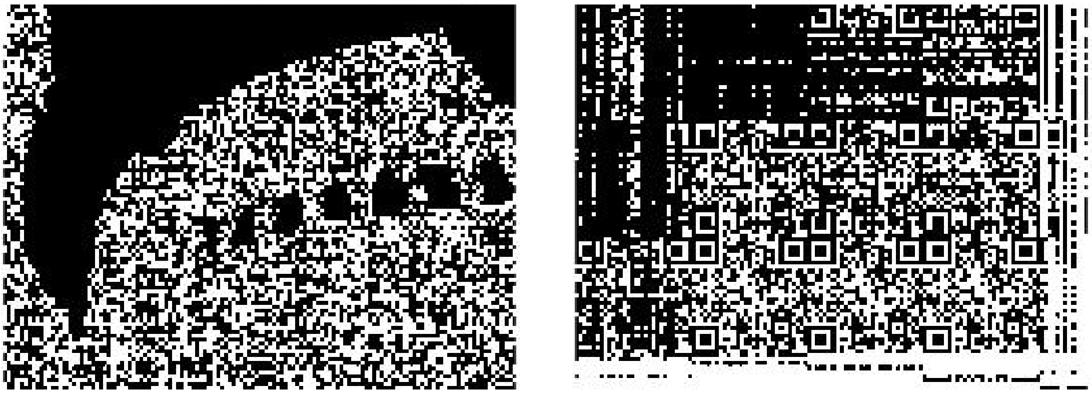


Figure 5: Extraction schema

been JPEG compressed (quality factors ranging in $[50, 100]$), $\pi/4$ rotations (rotations maintaining the bounding box of the original image imply also cropping) and with presence of salt & pepper noise. Salt & pepper noise case extraction (SPNOW) was evaluated also preprocessing the watermarked image with a median filter (SP) [CT15]. The results in Fig. 9, 10, 11, 12 and 13 show that db7 wavelet obtains the best results among the first 20 wavelets of Daubechies family and that salt & pepper noise impacts more than the other attacks on watermark robustness. Further tests were performed on the image of Fig. 14 by taking 4 occurrences of different size: 4641×3315, 1280×914, 1920×1371 and 640×457 pixels. We achieved a fully correct reconstruction in the first 3 sizes, confirming the robustness of the proposed schema. On the other hand the results for the smallest sample (640×457) in Fig. 15 confirm how salt & pepper noise has a deeper impact affecting the reconstruction, when one the size of the image is smaller than 512 pixel. This is explained by the reduced number of QR code occurrences, clearly insufficient to appropriately obtain the correct QR code (Fig. 16).



(a)

(b)

Figure 6: Extracted watermark: (a) without scrambling; (b) after key scrambling.

(a) (b) (c) (d) (e)

Figure 7: Test images: (a) Lena; (b) Barbara; (c) Baboon; (d) Boat; (e) Peppers.

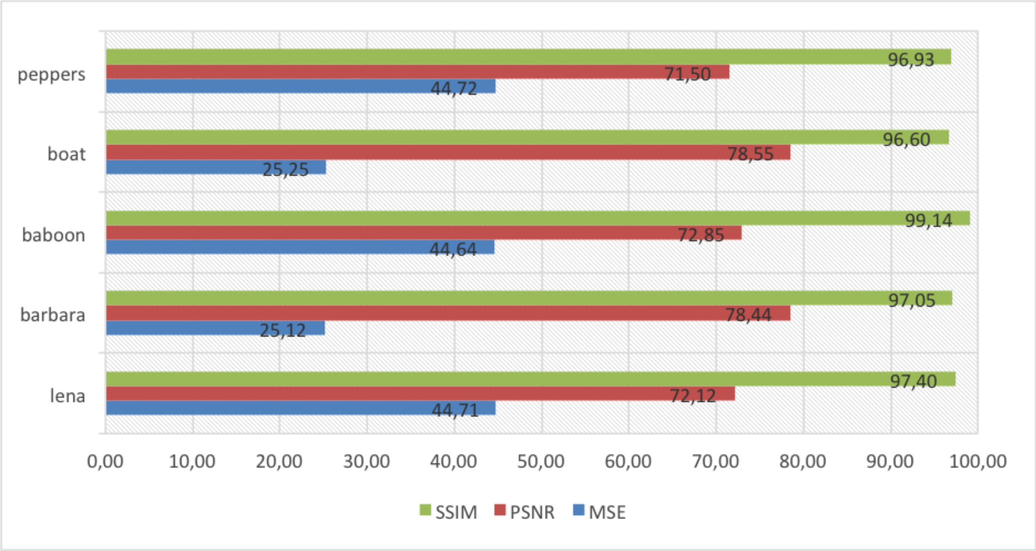


Figure 8: Quality evaluation of the test images.

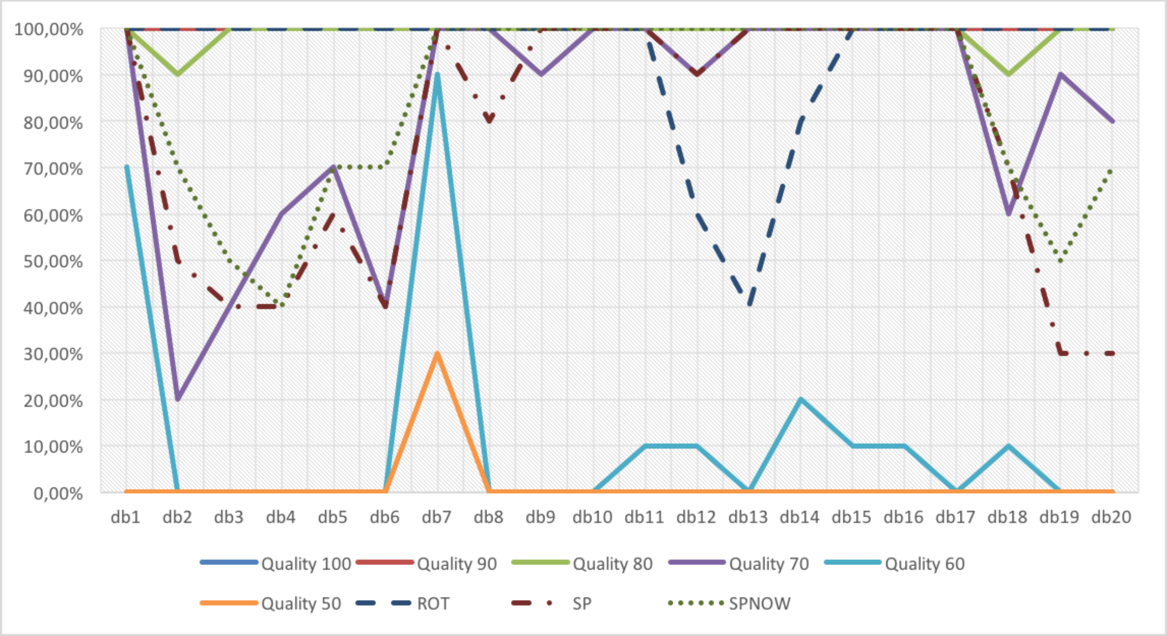


Figure 9: Results on the test image Lena.

5 Conclusion and future work

A novel digital rights protection scheme based on the 3rd level DWT image watermarking technique has been designed, implemented and evaluated. This schema can embed scrambled intellectual property references within an image with almost no effect on its quality. Experimental results show that such a schema provides quite good quality and robustness. Further analysis could be done by investigating on single image adaptive constants k (see Section 3) in order to improve the robustness and the reconstruction of the QR code from its occurrences. Another interesting application could be testing such a schema on the single frames of a video.

References

[Ber14] Fariba Ghorbany Beram. Effective parameters of image steganography techniques. *International Journal of Computer Applications Technology and Research*, 3(6):361–363, 2014.

[CCC14] Ji-Hong Chen, Wen-Yuan Chen, and Chin-Hsing Chen. Identification recovery scheme using quick response (qr) code and watermarking technique. *Applied Mathematics & Information Sciences*, 8(2):585, 2014.

[CCCM10] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3):727–752, 2010.

[CT15] Pratap Singh Chahar and Vandana Vikas Thakre. Performance comparison of various filters for removing salt & pepper and speckle noises. *International Journal of Computer & Communication Engineering Research (IJCCER)*, 3(5), 2015.

[Dan12] Daniel Beer. Quirc, 2012. https://github.com/dlbeer/quirc.

[Dau90] Ingrid Daubechies. The wavelet transform, time-frequency localization and signal analysis. *IEEE Trans. Information Theory*, 36(5):961–1005, 1990.

[Dau92] I. Daubechies. *Ten Lectures on Wavelets*. Society for Industrial and Applied Mathematics, 1992.

[Gol09] E.B. Goldstein. *Sensation and Perception*. Cengage Learning, 2009.

[HH13] Mehdi Hussain and Mureed Hussain. A survey of image steganography techniques. *International Journal of Advanced Science and Technology*, 54:113–124, May 2013.

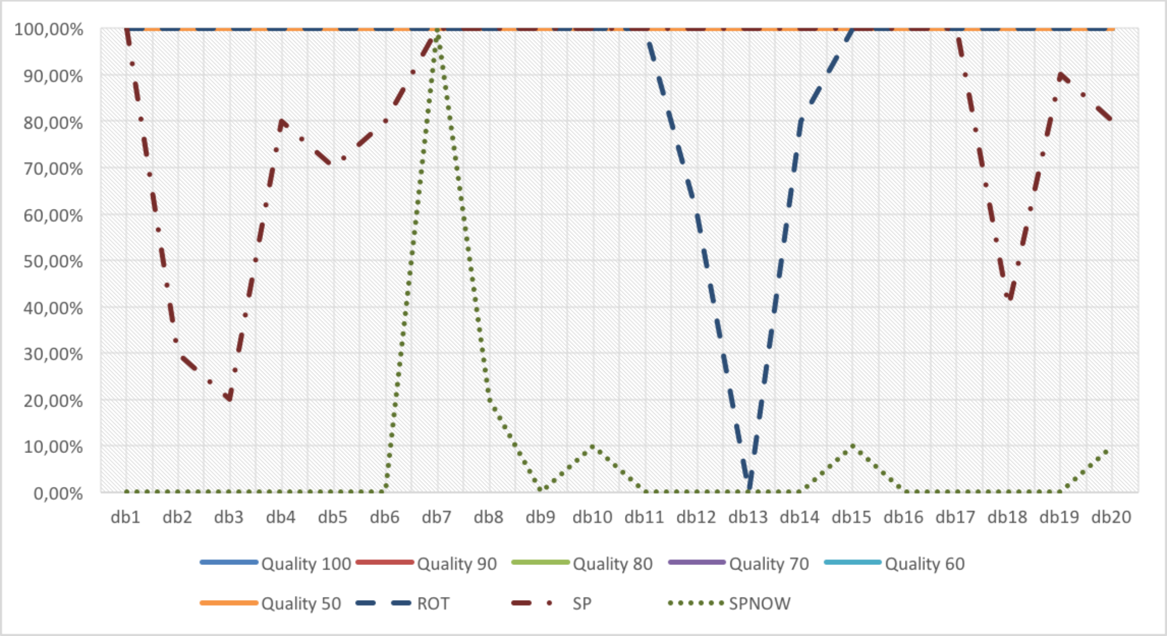


Figure 10: Results on the test image Barbara.

[HYAAQ12] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi. Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, 6(3):168–187, 2012.

[ISO15] Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification. Standard, International Organization for Standardization, Geneva, CH, February 2015.

[Ken18] Kentaro Fukuchi. libqrencode, 2018. https://fukuchi.org/works/qrencode.

[KK11] Jagvinder Kaur and Sanjeev Kumar. Study and analysis of various image steganography techniques. *IJCST*, 2(3):2229–433, 2011.

[KLH13] M Kim, D Li, and S Hong. A robust and invisible digital watermarking algorithm based on multiple transform method for image contents. In *Proceedings of the World Congress on Engineering and Computer Science*, volume 1, 2013.

[Mal89] Stephane G. Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE transactions on pattern analysis and machine intelligence*, 11(7):674–693, 1989.

[NVR16] Mohammad Ali Nematollahi, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. *Digital Watermarking: Techniques and Trends.* Springer Publishing Company, Incorporated, 1st edition, 2016.

[Rak13] Suresh Gawande Rakhi. A review on steganography methods. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2(10), 2013.

[RCSD13] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, and Narayan C Debnath. Evaluating image steganography techniques: Future research challenges. In *Computing, Management and Telecommunications (ComManTel), 2013 International Conference on*, pages 309–314. IEEE, 2013.

[RMK15] R. Rejani, D. Murugan, and Deepu V. Krishnan. Comparative study of spatial domain image steganography techniques. *International Journal of Advanced Networking and Applications*, 7(2):2650, 2015.

[RVH96] K. Ramchandran, M. Vetterli, and C. Herley. Wavelets, subband coding, and best bases. *Proceedings of the IEEE*, 84(4):541–560, April 1996.

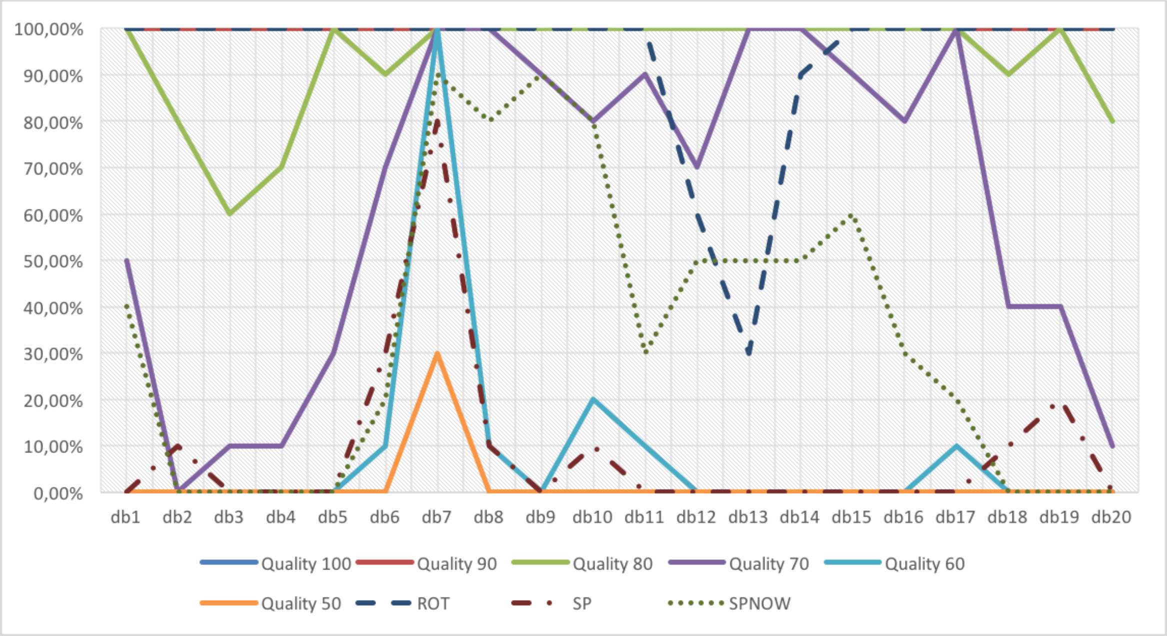


Figure 11: Results on the test images Baboon.

[SK15] Sudhanshi Sharma and Umesh Kumar. Review of transform domain techniques for image steganography. *International Journal of Science and Research*, 2(2):1, 2015.

[TCZA14] Hai Tao, Li Chongmin, Jasni Mohamad Zain, and Ahmed N Abdalla. Robust image watermarking theories and techniques: a review. *Journal of applied research and technology*, 12(1):122–138, 2014.

[Wav] Denso Wave. Answer to your questions about the QR Code. http://www.qrcode.com/en/ [accessed 15-Jun-2018].

[WBSS04] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE Trans. Image Processing*, 13(4):600–612, 2004.

[XSSL04] Jianyun Xu, Andrew H Sung, Peipei Shi, and Qingzhong Liu. Jpeg compression immune steganography using wavelet transform. In *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, volume 2, pages 704–708. IEEE, 2004.

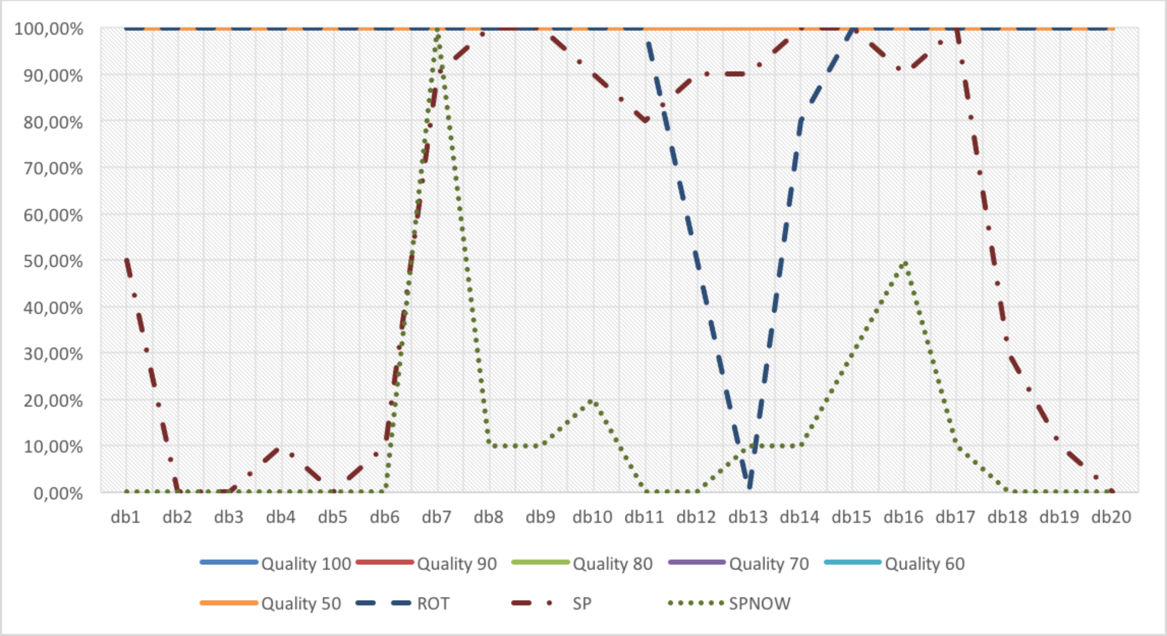


Figure 12: Results on the test images Boat.

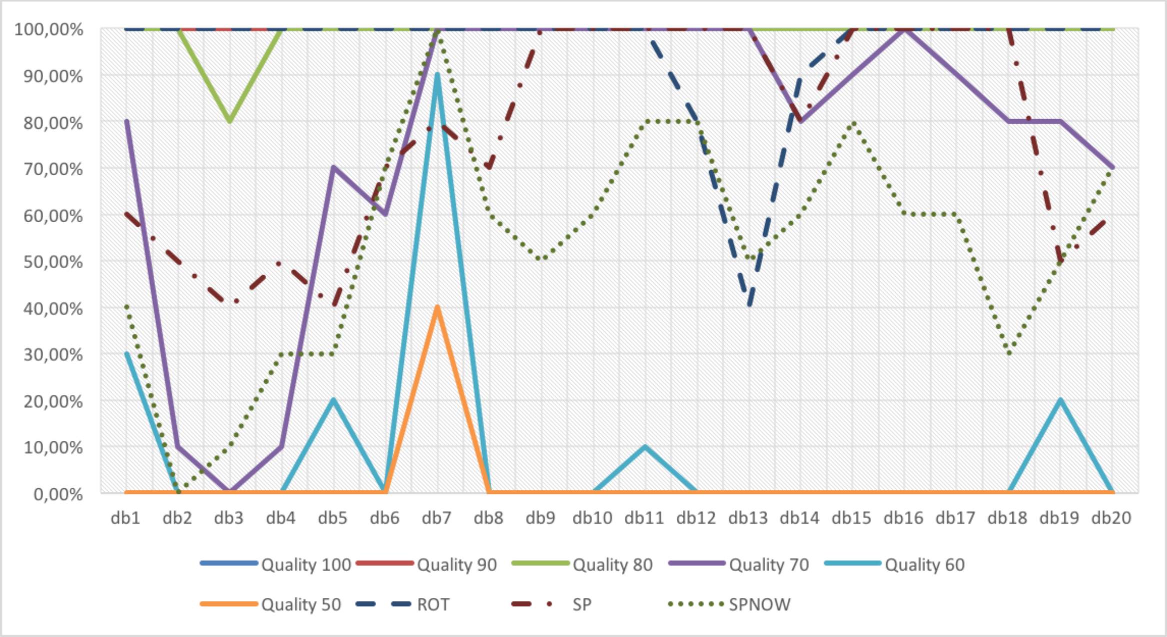


Figure 13: Results on the test images Peppers.

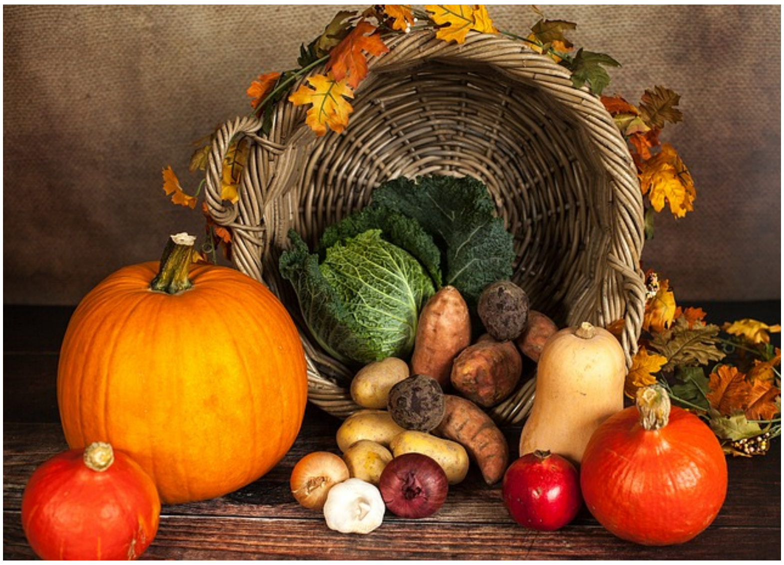


Figure 14: Still life.

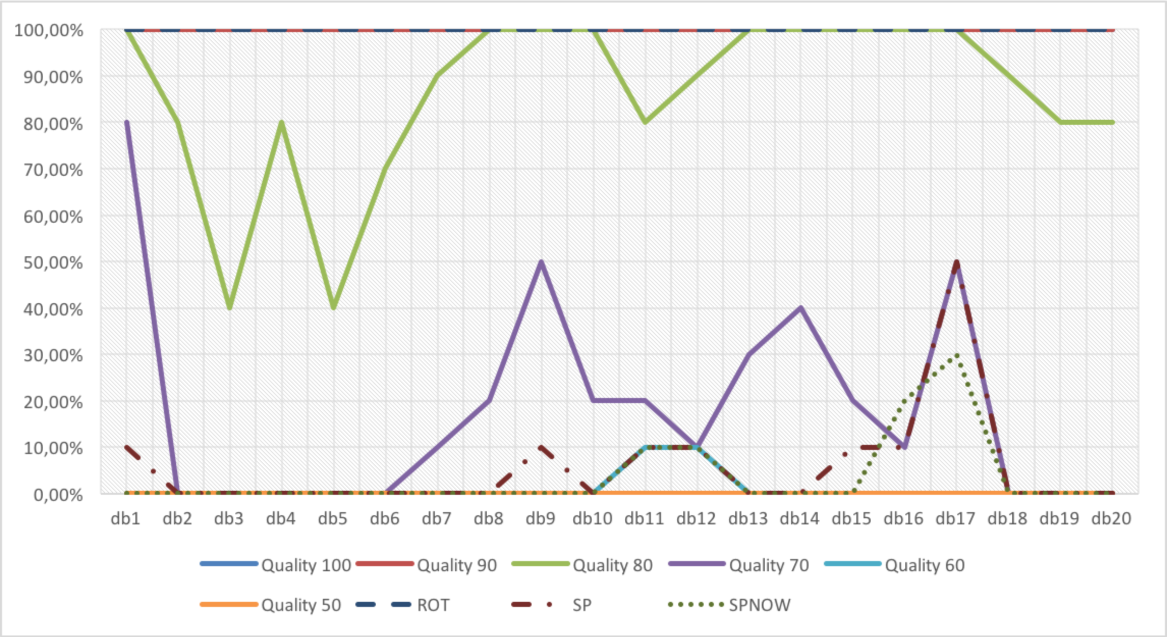


Figure 15: Results on still life 640 × 457.

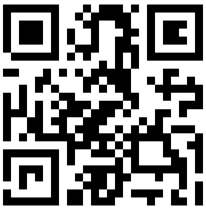


Figure 16: One occurrence of the extracted QR code in the case of small image.