An Efficient and Robust Hybrid Watermarking Scheme for Text-images

Lamri Laouamer[1,2] and Omar Tayan[3]
(Corresponding author: Lamri Laouamer)
Department of Management Information Systems, CBE, Qassim University[1]
P.O. Box 6633 Buraidah, 51452 Qassim, KSA
Lab-STICC (UMR CNRS 6285), University of Bretagne Occidentale[2]
20 avenue Victor Le Gorgeu, BP817-CS 93837-29238 Brest Cedex, France
IT Research Center for the Holy Quran (NOOR) & College of Computer Science and Engineering, Taibah University[3]
Al-Madinah Al-Munawwarah 41411, KSA
(Email: laoamr@qu.edu.sa)
(Received Aug. 13, 2015; revised and accepted Nov. 27, 2015)

Abstract

Addressing fraud and illegal use of multimedia requires the development of more powerful and robust algorithms. One of the solutions that can contribute significantly to solve such problems can be found in the use of image watermarking. In image watermarking, a watermark is introduced within an image in order to protect it against illegal use. This paper proposes a new hybrid text-image watermarking algorithm based on the singular value decomposition (SVD) and the discrete cosine transform (DCT) with linear interpolation in the embedding/extraction process. Despite a considerable number of works found to-date, the robustness in existing watermark approaches remains a major challenge worthy of further improvement. Furthermore, text-images are used as samples in this work to test our scheme under further challenges and constraints imposed by such images on the embedding techniques used. In contrast to many existing approaches, we achieved through the proposed algorithm a high robustness results against the most dangerous attack scenarios. A major contribution in this paper is found in our unique watermark extraction scheme which differs from the existing literature and takes into account three inputs including the attacked watermarked image. Finally, we discuss the results obtained for our approach under various attack scenarios.

Keywords: Attacks, DCT, linear interpolation, robustness, SVD, watermark

1 Introduction

The evolution of communication technologies and data transmission has enhanced global access to information. Consequently, the dissemination and sharing of digital data has become easily accessible to users. However, the robustness issue has become an increasing problem since existing protection techniques relying solely on encryption have become insufficient to address the advancing requirements of data protection. The influence of digital-watermarking is increasing as a solution for countering various forms of illegal manipulation and piracy. Essentially, it consists of introducing an invisible signature in the host data, and then detecting possible manipulations applied on the watermarked data. Several techniques have been proposed in the literature, however, it remains that the invisibility versus robustness compromise under all attack scenarios remains an elusive goal in the research community.

In this paper, we focus on image watermarking and highlight the image watermarking approaches based on the hybrid singular value decomposition (SVD) and the discrete cosine transform (DCT) techniques. For this purpose, we expose some important image watermarking works from the literature based on SVD and DCT. Before examining those works, we review some important concepts of the SVD and the DCT transforms.

2 Background and State-of-art

The SVD Transform consists of factorizing a matrix M, into three matrices (components) U, S, V such that:

$$[M] = [U][S][V^T]$$

In fact, the inverse transform of the SVD is not entirely reversible, but rather is the product (Equation (1)):

$$M_{mn} = U_{mm}.S_{mn}.V_{nn}^T \quad (1)$$

where m, n are the image size (m represents the rows and n the columns). And U_{mm} is the left singular vector,

S_{mn} are the singular values and V_{nn} is the right singular vector. The DCT transform consists of changing the data from the spatial domain into the frequency domain. The corresponding DCT transform blocks are given by the following Equation (2):

$$F(u,v) = \frac{2}{N}c(u)c(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} pixel(x,y) \\ cos[\frac{\pi}{N}u(x+\frac{1}{2}]cos[\frac{\pi}{N}v(y+\frac{1}{2}] \quad (2)$$

The DCT inverse is given by the Equation (3):

$$f(x,y) = \frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} c(u)c(v)F(u,v) \\ cos[\frac{\pi}{N}u(x+\frac{1}{2}]cos[\frac{\pi}{N}v(y+\frac{1}{2}] \quad (3)$$

Where $c(u)$, $c(v) = (2)^{-1/2}$ for u, $v = 0$, $c(u)$, $c(v) = 1$ for u, $v = 1, 2, \cdots, N-1$, pixel(x, y) is the pixel value at position (x,y). The authors in [1] applied a differential evolution (DE) algorithm in the DCT domain to balance the trade-off between robustness and imperceptibility by exploring multiple scaling factors in image watermarking. The DC coefficients from each block were collected to construct a low-resolution approximation image and applied SVD on this image approximation. Experimental results show that the proposed scheme maintained a satisfactory image quality, with the watermark still identifiable following serious distortion to the image. In [2], an optimal DCT-SVD based image watermarking scheme using Pareto-based Multi-objective Genetic Algorithm (MOGA) was presented. After applying the DCT to the cover image, they map the DCT coefficients in a zigzag order into four quadrants, and apply SVD to each quadrant. The proposed algorithm in [2] was not perfectly robust, particularly against rotation attacks.

The work presented in [6] consists of a new robust hybrid image watermarking scheme based on SVD and DCT. After applying SVD to the cover image blocks, DCT was performed on the macro block comprised of the first singular values (SVs) of each image block. In the work by [6], an improved watermarking extraction scheme was demonstrated, particularly against median-filtering, rotation and cropping attacks. A robust lossless copyright protection scheme based on overlapping DCT and SVD was presented in [12] where direct current (DC) coefficients were extracted from the transformed blocks to form a DC-map. A series of random positions were selected on the map, and SVD was applied to construct an ownership share which is used for copyright verification. Experimental results were conducted to demonstrate the robustness of the proposed algorithm against several kinds of attacks, but with some weaknesses in the case of cropping, rotation and print-scan attacks.

The approach proposed in [4] presents a normalization-based robust image watermarking scheme which encompasses SVD and DCT techniques. The host image is first normalized into standard form and divided into non-overlapping image blocks. A watermark bit is then embedded in the high frequency band of an SVD-DCT block by imposing a particular relationship between two pseudo-randomly selected DCT coefficients. The experimental results show that the proposed approach was not perfectly robust against many attack scenarios.

In this paper, we propose a new hybrid algorithm based on SVD and DCT for the protection of online textual-images against several kinds of known attacks. In fact, the extraction method requires three inputs contrarily to the conventional semi-blind methods. The proposed embedding method is also based on linear interpolation with invisible watermarking. Additionally, text-images are applied as inputs since they present a particularly interesting research challenge (and relatively unexplored branch of image-watermarking) due to the limited solution-space available in the host-images used, as evidenced in the limited use of colours and textures, with clearly defined characters and whitespace etc. Nevertheless, our scheme can also be applied on general images comprising of a rich colour-set and more relaxed-constraints on the embedding process as considered in most related literature works. To determine the robustness of the proposed algorithm, we conducted several attacks on the watermarked images and compared the original watermark to the extracted one. The following section details our proposed algorithm.

3 Proposed Watermark Embedding Scheme

In this work, the embedding process is achieved using a linear interpolation of type (Equation (4)):

$$i_w = (1-\alpha)w + \alpha i \quad (4)$$

where i_w, w, i are the RGB images, the watermarked image, the original image, and the watermark respectively, and α, is a variable between 0 and 1 as explained in the Equation (5):

$$U_{iw} = U_i, S_{iw} = (1-\alpha)S_w + \alpha S_i \text{ and } V_{iw} = V_i \quad (5)$$

The illegible components U_{iw}, S_{iw}, V_{iw} are the corresponding matrices of the image i_w. Hence, obtaining the product of those three components (Equation (6)) gives a significant (readable) image i_w.

$$i_w = U_{iw} \times S_{iw}b \times V_{iw}^T \quad (6)$$

In our proposed embedding process, only the S-component (e.g. the singular values matrix) of the images i and w were used to achieve the data embedding (Equation (7)), which suggests that:

$$U_{iw} = U_i, \ \ S_{iw} = (1-\alpha)S_w + \alpha S_i \text{ and } V_{iw} = V_i \quad (7)$$

Obtaining an invisible watermark requires that the value of α (e.g. our used watermarking key) be set close

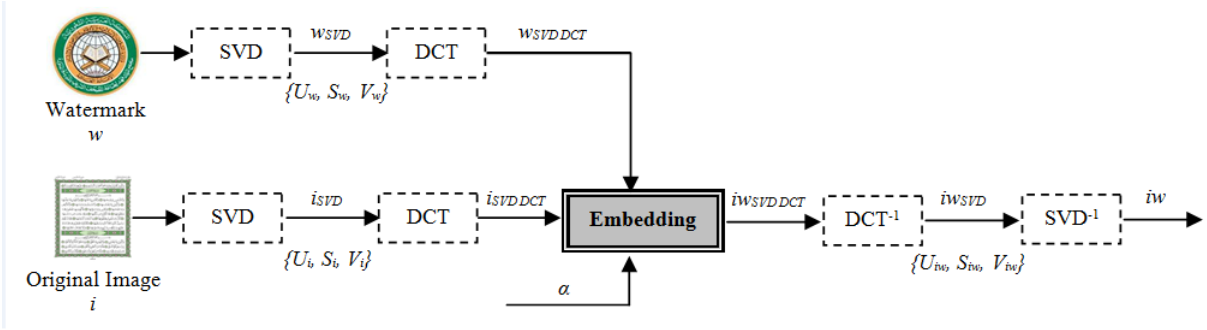


Figure 1: Watermark embedding algorithm

to 1 with $i_w \rightarrow i$, while a visible watermark signifies that α should be set close to 0 with $i_w \rightarrow w$. We summarize our embedding scheme in Figure 1.

Algorithm 1 Embedding algorithm

1: First compute the matrices: U, S, V , corresponding to both the original image i and the watermark w.
2: Apply the DCT embedding on the S_i and S_w components produced, suggesting that the embedding exists for only the singular-value matrices (e.g. following the DCT operation on the singular-value matrix of the original image i and the DCT operation on the singular-value matrix of the watermark). The embedding formula applied at this stage is given as follows: $U_{iw}=U_i$, DCT $(S_{iw})=(1-\alpha)DCT(S_w) + \alpha\ DCT(S_i)$ and $V_{iw}=V_i$
3: Next
4: Calculate the DCT inverse of the $DCT(S_{iw})$, and apply the SVD^{-1} term to obtain the watermarked image i_w as a result of the embedding. It is important to mention that the SVD^{-1} term does not mean the entire inverse transform, but rather, it is the product of the three matrices U, S, V^T. This suggests that SVD process is not completely reversible.

4 Proposed Watermark Extraction Scheme

In our proposed algorithm, the extraction process consists of applying three inputs i_w, w and i_{wa}, representing the watermarked image, the watermark, and the attacked watermarked-image respectively. This unique combination of inputs and operations in the extraction process was not found elsewhere in the related literature and was used effectively to obtain promising results through perfect extraction of the watermark as reported in the next section. The extraction process is as illustrated in Figure 2.

For the embedding operation (Equation (8)), we note that:

$$S_{wi} = (1-\alpha)DCT(S_{iw}) + \alpha DCT(S_w) \quad (8)$$

Next, the Unmark operation as illustrated in the Equation (9), consists of the reverse embedding process, which follows from:

$$W_{\alpha SVD} = \frac{1}{\alpha} W_{iSVD} - \frac{1-\alpha}{\alpha} i_{waSVD} \quad (9)$$

where w_a, i_{wa} are the extracted watermark and the attacked watermarked-image respectively. We note by Siw the singular value of the watermarked image i_w, however the S_{wi} consists to the results of the watermark embedding in the image i_w and not the image i (it is simply for differentiating notations).

Algorithm 2 Extraction algorithm

1: First, compute the matrices: U, S, V , for the watermark w, the watermark-image i_w, and the attacked watermarked image i_{wa}.
2: Apply the embedding of DCT(S_w) using the $DCT(Si_w)$ term. The embedding result of this step gives $w_{iSVDDCT}$. This embedding exists for only the singular-value matrices of the DCTs of S_w and S_{iw} respectively (e.g. following from the DCT operation on the singular-values matrix of the watermark w, and the DCT operation on the singular-values matrix of the watermarked image). The embedding formula used at this stage is given by (Equation (10)):

$$DCT(S_{wi}) = (1-\alpha)DCT(S_{iw}) + \alpha DCT(S_w) \quad (10)$$

3: Next, run the Unmark process between $i_{waSVDDCT}$ and $w_{iSVDDCT}$, which gives the matrix $w_{aSVDDCT}$ according to the Equation (11):

$$W_{\alpha SVDDCT} = \frac{1}{\alpha} W_{iSVDDCT} - \frac{1-\alpha}{\alpha} i_{waSVDDCT} \quad (11)$$

4: Finally, compute the DCT and the SVD inverse to obtain the extracted watermark, w_a.

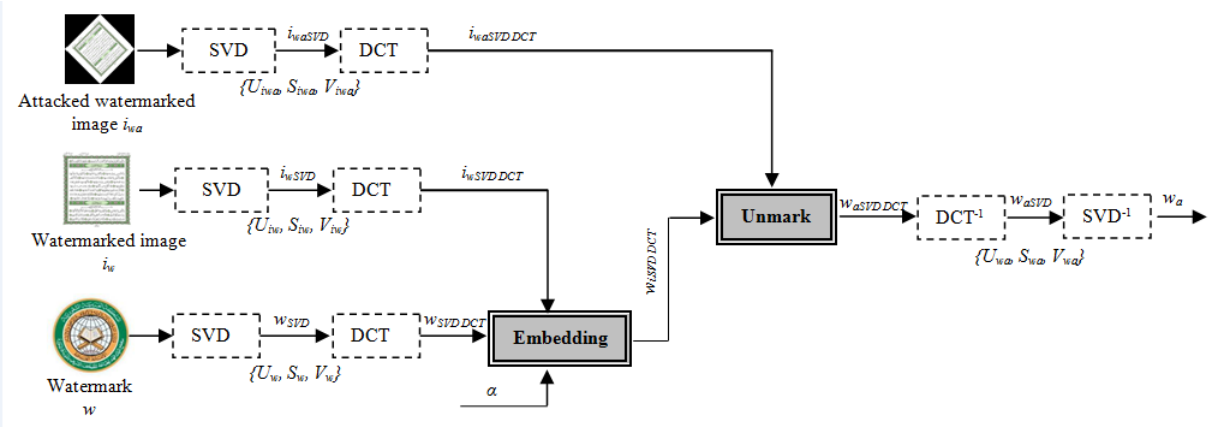


Figure 2: Watermark extraction algorithm

5 Tests and Robustness Evaluation

In this work, tests were conducted on a database of 120 text-image samples. The original images i [9] and the watermark w [9] are represented by colour text-images of size $256 \times 256 \times 3$. Figure 3 shows the images used in our tests by watermarking i with w using several values of the key α =0.1; 0.5; 0.98. We performed both the embedding/extraction processes only in the case of invisible watermarking, where $\alpha = 0.98$ (close to 1). The benchmark applied is that of the Stirmark benchmark from [8].

This benchmark is the most used attacks software and is well used by scientists in the digital-watermarking domain [8] for simulating attack scenarios.

We applied all the existing attacks from the Stirmark benchmark and obtained an attacked watermarked-image, i_{wa}, for each attack. We illustrate some of the most dangerous attacks, including: affine transformation, cropping, JPEG compression, median-filtering, additive-noise and rotation attacks, as shown in Table 1.

As known, attacks such as cropping, rotation and noise are considered as dangerous attacks due to their nature as a non linear transformation. The robustness of the proposed approach can be justified for two reasons: 1) The perfect invisibility of the watermark (in the embedding process); 2) embedding the watermark only in the singular values matrix S. the singular values matrix is known that contain the most important information in the image, which can very helpful to extract the watermark.

The robustness evaluation of the proposed approach is based on calculating the most known similarity measures. Hence, our performance evaluation cost-function consists of comparing the similarity degree PSNR and SSIM [7] between the original watermark and the extracted one following each attack. In Table 1, we have calculated those measures in the case of all the presented attacks. The PSNR measure is a critical metric in our experiments and is defined by the Equation (12):

$$PSNR = log_{10}(\frac{Max_w}{\sqrt{MSE}}) \tag{12}$$

Given that

$$MSE = \frac{1}{MN} \sum_{0}^{m-1} \sum_{0}^{n-1} \|w(i,j) - w_a(i,j)\|^2 \tag{13}$$

Where m, n are the image size and w(i,j), w_a(i,j) are the values of the pixels in the position (i,j). The SSIM calculation is given by Equation (13):

$$SSIM = \frac{(2\mu_w\mu_{wa} + c_1)(2\sigma_{wwa} + c_2)}{(\mu_w^2 + \mu_{wa}^2 + c_1)(\sigma_w^2 + \sigma_w^2 + \sigma_{wa}^2 + c_2)} \tag{14}$$

Given that:

μ_w and μ_{wa} are respectively the average of w and w_a.

$\sigma^2{}_w$ and $\sigma^2{}_w$ are respectively the variance of w and w_a.

σ_{wwa} is the covariance of w and w_a.

L is the dynamic range, of the pixel intensity (typically $2^{\#bitsperpixel}$ -1).

$c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ with k_1=0.01 and k_2=0.03.

From Table 1, it is observed that the similarities between the original watermark and the extracted ones in the case of PSNR are in excess of 34db, which suggests a high similarity between the original watermark and the extracted watermark under those attack scenarios. For the SSIM, we see that its values are very close to 1, also suggesting that the original watermark and the extracted watermark are very similar. Moreover, the amplified differences in Table 1 demonstrate that visibly perfect watermark extraction was possible using our approach. We used the amplified difference to demonstrate where exactly the differences zones between the original watermark w and the extracted wa. Showing a simple difference between w and wa can not allow to distinguish visually the differences between w and w_a.

We compared the approach we propose regarding to some of the most remarkable works in the literature and

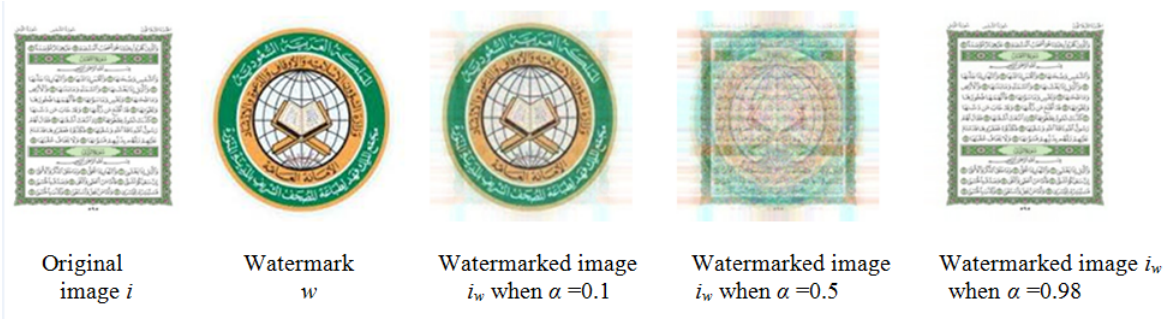
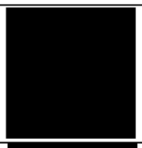
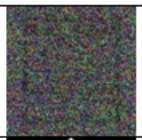


Figure 3: Watermark embedding with varying values of key (α)

Table 1: Results of extracted watermarks under several attack scenarios

Attack Type	Attacked watermarked image (i_{wa})	Extracted watermark (w_a)	Difference $\lvert w_a - w \rvert$	Amplified difference (+150)	PSNR (dB)	SSIM
Affine_7					45.21	0.971
Cropping_50					46.37	0.987
Jpeg_90					43.92	0.976
Median_9					46.11	0.984
Noise_80					36.72	0.954
Rotation_45					38.63	0.962

which are based on the combination of SVD and DCT watermarking. We note that the results obtained in our work in terms of PSNR measure is better, which means a higher robustness comparing to works bellow. The Table 2 shows a comparison of our approach with those works.

It should be noted that the proposed approach has a high complexity due to the quantity of information to embed presented by an entire image as a watermark. A compromise between robustness and hiding capacity is a major challenge in the literature. Unfortunately, till date there is no a watermarking scheme which can reach this compromise: Little information quantity to embed, low complexity and high robustness.

6 Conclusion

Copyright protection is a challenge that requires further research efforts in addition to the existing literature works. Multimedia protection is a topic of particular importance in recent years due to its economic and moral impacts. To address this problem, we propose a hybrid watermarking scheme based on SVD and DCT to ensure the originality and authenticity of text-images against illegal manipulations. It should be noted that many studies in this field have been presented but most of those studies present weaknesses at the robustness level, particularly against specific types of geometric attacks. The main contribution in this paper is found in the watermark extraction process that involves a third parameter; which is the attacked watermarked-image in the hybrid watermarking algorithm based on DCT and SVD. We tested our approach against many attack-types, and have only presented the most dangerous types in this paper (e.g. that include median-filtering, rotation, additive-noise attacks etc...). The most dangerous attacks consist to make alteration in the whole of the image (pixel by pixel) and not for specific zones.The robustness of our algorithm has been evaluated using widely known metrics from the literature: namely, the PSNR and SSIM metrics. The results obtained were very encouraging, allowing us to extract the watermark against attacks almost perfectly. The similarity between the original watermark and the extracted watermarks for each attack were very close. The only disadvantage of our approach algorithm was that it resulted with a higher complexity.

Acknowledgments

The authors would like to thank and acknowledge the IT Research Centre NOOR at Taibah University for their financial support during the academic year 2012/2013 under research grant reference number NRC1-126.

References

[1] M. Ali, C. W. Ahn, M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain", *Optik-International Journal for Light and Electron Optics,* vol. 125, no. 1, pp. 428–434, 2014.

[2] H. N. Andevari, S. Mirzakuchaki, "Image Watermarking Optimization in DCT-SVD Domain Using NSGA-II," *International Journal of Computer Theory and Engineering,* vol. 4, no. 2, pp. 309, 2012.

[3] G. Bhatnagar, B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards & Interfaces,* vol. 31, no. 5, pp. 1002–1013, 2009.

[4] S. W. Foo, Q. Dong, "A normalization-based robust image watermarking scheme using SVD and DCT," *World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering,* vol. 6, no. 1, pp. 205–210, 2010.

[5] F. Huang, Z. H. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR," *Pattern Recognition Letters,* vol. 25, no. 15, pp. 1769–1775, 2004.

[6] Z. Li, K. H. Yap, B. Y. Lei, "A new blind robust image watermarking scheme in SVD-DCT composite domain," in *18th IEEE International Conference on Image Processing (ICIP),* pp. 2757–2760, 2011.

[7] L. Laouamer, O. Tayan, "An enhanced SVD technique for authentication and protection of text-images using a case study on digital Quran content with sensitivity constraints," *Life Science Journal,* vol. 10, no. 2, pp. 2591–2597, 2013.

[8] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Attacks on copyright marking systems," in *Proceedings of Second International Workshop on Information Hiding (IH'98)*, LNCS 1525, Springer-Verlag, pp. 219-239, 1998. (`http://www.petitcolas.net/fabien/watermarking/stirmark/`)

[9] Quran Complex, 2016. (`http://www.qurancomplex.org/`)

[10] D. Rosiyadi, S. J. Horng, P. Fan, et al. "Copyright protection for e-government document images," *IEEE Transactions on Multimedia,* vol. 19, no. 3, pp. 62–73, 2012.

[11] A. Sverdlov, S. Dexter, A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies," in *IEEE 13th European Signal Processing Conference,* pp. 1–4, 2005.

[12] X. Wu, W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Applied Soft Computing,* vol. 13, no. 2, pp. 1170–1182, 2013.

[13] X. Wu, W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Applied Soft Computing,* vol. 13, no. 2, pp. 1170–1182, 2013.

Table 2: Comparison of the proposed approach with some related works

Attack Scenario	PSNR in Proposed approach	PSNR in [1]	PSNR in [2]	PSNR in [6]
JPEG	43.92	31.92	48.3998	28.36
Rescaling	39.241	19.9781	37.1756	21.73
Gaussian Noise	36.72	14.2658	29.783	23.33
Median Filtering	46.11	13.9449	35.7747	25.52
Cropping	46.37	36.4068	12.2786	11.30
Rotation	38.63	6.4717	15.8719	12.32

[14] B. Wang, J. Ding, Q. Wen, et al. "An image watermarking algorithm based on DWT DCT and SVD," in *IEEE International Conference on Network Infrastructure and Digital Content,* pp. 1034–1038, 2009.

Lamri Laouamer is an assistant professor at the department of Management Information Systems, College of Business and Economics at Qassim University, KSA. He is also an associate researcher at the Laboratoire des Sciences et Techniques de Information, de la Communication et de la Connaissance (Lab-STICC), University de Bretagne Occidentale, Brest, France. He received his PhD in computer science, in the field of information security, from University de Bretagne Occidentale, France, in 2012; his MSc in computer science and applied mathematics from the University of Quebec at Trois Rivieres, Canada, in 2006; and his B.Sc. in computer science from the University of Setif, Algeria, in 1999. His research interests include multimedia watermarking, cryptology and information security. Dr. Lamri Laouamer is an associate editor of the Journal of Telecommunication Systems, published by Springer, and associate editor of the Journal of Innovation in Digital Ecosystems, published by Elsevier.

Omar Tayan completed his undergraduate degree in Computer and Electronic Systems from the University of Strathclyde, Glasgow, UK and his PhD in Computer Networks, Department of Electronic & Electrical Engineering from the same university. He currently works as an Associate Professor at the College of Computer Science and Engineering (CCSE) and IT Research Center for the Holy Quran and Its Sciences (NOOR) at Taibah University, Saudi Arabia. He was a consultant to the Strategic and Advanced Research and Technology Innovation Unit at the university and is one of the founding members of the "IT Research Center for the Holy Quran and Its Sciences (NOOR)" at Taibah University. His research interests include; Information Security, E-Learning technologies, performance modeling and simulation, high-speed computer networks and architectures, software simulation techniques and queuing theory, Wireless Sensor Networks for Intelligent Transportation Systems, Networks-on-Chip (NoC).