An Enhanced SVD Technique for Authentication and Protection of Text-Images using a Case Study on Digital Quran Content with Sensitivity Constraints

Lamri Laouamer [1], Omar Tayan [2]

[1] Department of Information Systems, CBE, University of Al Qassim, Buraidah, KSA.
[2] IT Research Center for the Holy Quran (NOOR) & College of Computer Science and Engineering,
Taibah University, Al-Madinah Al-Munawwarah, KSA.
laoamr@qu.edu.sa , otayan@taibahu.edu.sa

Abstract: This paper addresses originality and authenticity verification of sensitive online content propagated electronically by detecting and preventing third-party modifications. The problem arises when sensitive online textual-images are targeted for counterfeiting or modifications through intentional or unintentional manipulations, whereby any change to the data would result with a fake copy being published. The emergence of third-party manipulations suggest that new techniques for authentication of sensitive digital content has become essential for electronic publishers of online information. Hence, a new enhanced approach based on singular value decomposition (SVD) for watermarking the data is proposed to confirm the authenticity of published online text-image content, and is applied on digital-Quran text-images as an ideal case study of content with challenging sensitivity constraints. The paper demonstrates that the proposed approach has strong robustness and security against the most dangerous attacks for textual image-based digital content that includes geometrical attacks on the content. Finally, we discuss the results of the proposed approach on sample text-images used, and demonstrate how authenticity and originality of the Quranic content can be successfully verified. A significant advantage of the proposed approach is evident in its broad applicability since it can be easily extended for the protection and authentication of other sensitive digital text-image content.

[Laouamer L, Tayan O. **An Enhanced SVD Technique for Authentication and Protection of Text-Images using a Case Study on Digital Quran Content with Sensitivity Constraints.** *Life Sci J* 2013;10(2):2591-2597] (ISSN:1097-8135). http://www.lifesciencesite.com. 359

Keywords: text-images; authentication; protection; single value decomposition, attacks, similarity, digital-Quran content.

1. Introduction

The development of capture and transmission technologies for digital images and video has opened up great opportunities for creating and manipulating visual content relating to both scientific and artistic works. The Internet has become the primary communications forum in our digital society, with large amounts of data being transferred continuously. Furthermore, the Internet offers a quick way to share information, however, does not necessarily provide a safe means for the data-transfer. In contrast, it is pointed out that the benefits of the Internet are also accompanied with the problems and threats associated with ensuring digital copyright protection, preventing digital counterfeiting, proof-of-authentication and content-originality verification. Additionally, the ignorance of information-processing tools and image transmission technology has since allowed for illegal copying and distributing of digital information, therefore presenting the problem of not being able to control who has invalid copies of the digital works. This paper addresses the problem of integrity protection for widely disseminated digital-publications of the Holy Quran textual-image content, which is characteristic of sensitive content intolerable to even the slightest of modifications by any third-party, which may result with a compromise on the validity of the published content. Hence, a pivotal requirement addressed in this paper is to ensure that all digital Quran text-image content that had originated from a known publisher is secure from being tampered with or modified by anyone in any way without detection. Digital content protection is essential in this paper to allow the legitimate owners of Quran images (the authorized owners and publishers) with the ability to prove their rights to the text-image content. The legitimate owners are then able to detect or report illegal copies/derivations of the original-image, and to announce the flaws of these derived images when inconsistencies are found upon comparison with the original approved images. The techniques that are employed in this paper to provide the necessary security for such digital content are known as digital-image watermarking.

Digital watermarking is considered to offer a promising solution for dealing with copyright issues and online content-legitimacy. In digital watermarking, the signal to be protected (the host signal) is considered as the channel of communication, while the signature (the watermark) is considered to be the useful signal to be transmitted. The idea then is to embed the signature (logo or identifier) within the content of the host signal (e.g. the Qur'an text-image) with the goal to produce an invisible watermark, resistant to malicious or unintentional attacks. A digital-watermarking algorithm can then be designed to detect unauthorized modifications of the image. The watermark (credible proof-copy) embedded within the image is characterized as non-fragile in order to ensure that any change would also produce a detectable change in the image of the brand. An image can also be watermarked discretely in order to exchange secret watermarks. These are hidden in the image and require a secret key to be decoded.

Many methods have emerged in the field of digital image watermarking. Some act directly in the spatial plane for hiding the watermark image according to various models; a good example is the Least Significant Bit (LSB) approach. Other methods operate in the transform-domain, whereby the image components are best separated and represented. Currently, we tend to perceptual approaches based on the mechanisms of the Human Visual System (HVS). Three important parameters used to evaluate the performance of the watermarking scheme are used. Those parameters consist of the capacity, imperceptibility and robustness metrics. The capacity is a measure of the information quantity required by the watermark, while the imperceptibility is directly related to the quality of watermarked image, and finally, the robustness parameter, which provides a measure of the resistance against malicious and unintentional attacks. The last two parameters are closely related and are practically difficult to reconcile, resulting with a tradeoff between the two metrics. For instance, a required increase in the robustness-level in order to enhance resistance against attacks would also require increasing the watermark data that affect its visibility level and therefore degrades the image quality.

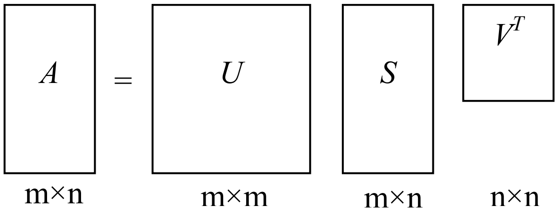
In the literature, a number of techniques can be found operating in the transform domain, including, the singular value decomposition technique (SVD), with other techniques found that also operate in the same space, such as the Discrete-Cosine transform (DCT), Discrete-Wavelet transform (DWT) and the Fast-Fourier transform (FFT), etc. For the purposes of this paper, the SVD-technique is considered due to the advantages found when comparing with the other techniques in the literature.

The singular value decomposition (SVD) is an important topic in linear algebra for matrices-factorization. It has many theoretical and practical applications other than image compression, and is also used for signal processing applications for solving the problems associated with communication, image processing, etc. (Golub and Van Loan, 1996).

The SVD technique can be used in many ways. On the one hand, it can be applied as a method to transform correlated variables into a set of uncorrelated variables that better expose the various relationships in the image data. Additionally, it is a method to identify and order the dimensions in which the data have most variation. Once the greatest variation is identified, it is possible to find the best approximation of the original data using fewer dimensions. Therefore, the SVD can be seen as a method of data reduction.

The particularity of the SVD technique is that it can be performed on any matrix (m, n) of real values. In this case, a matrix *A* it factorized into three matrices *U*, *S*, *V* such that:

$$A_{mn} = U_{mm} . S_{mn} . V^{T}_{nn}$$



where *U* and *V* are orthogonal matrices and *S* is a diagonal matrix.

The matrix *U* is the left singular vectors, and the matrix *V* is the right singular vectors, while the matrix *S* is the singular values. These singular values are arranged on the diagonal with descending order where:

$$s_1 \geq s_2 \geq s_3 \geq \ldots\ldots\ s_k \geq s_{k+1} = \ldots\ s_p = 0,$$

where *k* is the rank of the matrix *A*. This rank is equal to the number of non-zero singular values of *A*.

Neglecting the small singular values normally from the middle of the matrix *S* , allows us to obtain approximations of the A_k matrix in which the rank *k* is the number of other singular values. The singular values are displayed in descending order. The matrix approximation formula can then be expressed as:

$$A_k = u_1\, s_1\, v_1^T + \ldots\ldots + u_k\, s_k\, v_k^T$$

In fact, the SVD technique has several advantages, including:

a) the SVD of an image has very good stability, which means that when a small value is added to an image, it does not affect the quality with large variation.

b) the SVD is able to effectively represent the algebraic intrinsic properties of an image, where the singular values correspond to the image brightness and the singular vectors reflect the characteristics of the image geometry.

c) the image matrix has many small singular values compared to the first singular values. Even ignoring these small singular values in the image reconstruction does not affect the quality of the reconstructed image.

2. Previous Work

Among the proposed methods for digital image watermarking, the method developed by (Razafindradina and Randriamitantsoa, 2008) proposes a watermarking method that involves inserting a few bits of the watermark in the singular values of the original image matrix. In contrast to many existing watermarking algorithms, this watermarking algorithm is blind and shows remarkable results, particularly against JPEG compression and conversion format attacks in the case of GIF. The measured PSNR for his method was about 49.63 dB. On the other hand, (Bergman and Davidson, 2005) proposes a method by inserting the watermark in the matrix U (eigenright vectors). This method is not robust against image manipulations such as cropping, rotation or compression.

The work in (Liu R and Tan, 2002) proposes to add to the watermark into singular values *S* of the original image using a weight variable insertion. This method shows acceptable results against very destructive attacks such as nosing and rotation attacks. The extraction of the watermark was not perfect in the sense that the difference with the original watermark was so important.

(Sverdlov *et al*., 2005) offers a hybrid watermarking scheme based on DCT-SVD to improve robustness. This method has poor resistance against attacks that include Gaussian noising, rotation and other attacks. A watermarking approach using SVD was proposed in (Agarwal and Santhanam, 2008). The main idea is to insert the matrix *V* (eigenleft vectors) of the watermark in the matrix *V* of the original image. This approach consists of both colors and grayscale images. The attacks tested using this approach include, cropping, noising, compression and rotation attacks. The PSNR error measured in the case of the noising attack between the original watermark and the extracted watermark is in the order of 16.3dB, which suggests a lack of robustness in the approach.

In (Zhen *et al*., 2011), a new robust hybrid image watermarking scheme based on SVD – DCT is presented. After applying SVD to the cover image blocks, the approach then performs DCT on the macro block comprised of the first singular values (SVs) of each image block. The work in (Zhen *et al*., 2011) also developed a new method to embed the watermark in the high-frequency band of the SVD-DCT block by imposing a particular relationship between some pseudo-randomly selected pairs of the DCT coefficients. Experimental results showed that the proposed method here does not provide high resistance to particular attacks that includes; rotation, cropping and resizing attacks.

The work presented in (Khorasani and Sheikholeslami, 2012; Sukumar *et al*., 2009) presents a novel watermarking method based on DWT-SVD. The watermark was realized using SVD in various DWT components and levels. The PSNR calculated after extraction of the watermark had shown low values as compared to the desired values, with results being below the 34 dB threshold and in the case of several attacks such as JPEG, noising, and rotation attacks etc.

3. Proposed Algorithm

Watermark Embedding Process

The embedding process shown in figure 1 consists of embedding the matrix *S* of the watermark (singular values) in the matrix *S* of the host image (original image), since the most important information of the image is found in this component, and since this component is more stable and robust (Calagna *et al*., 2002). Obviously, this allows a real-time operation compared to if the operation was realized with the three components (*U, S, V*), which makes the watermarking algorithm longer with high complexity.

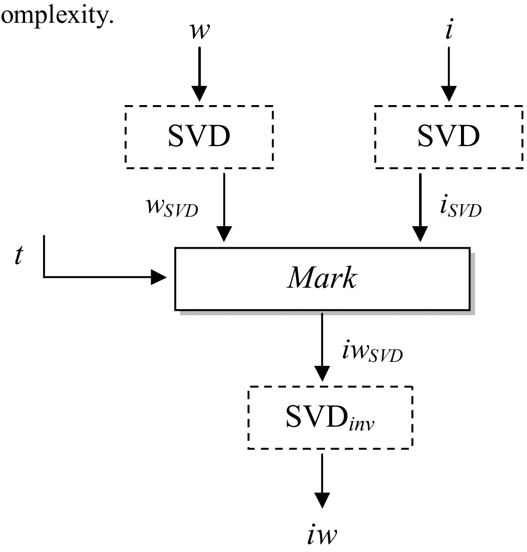


Figure 1: Watermark Embedding Process

The singular value decomposition of the image *i* gives the three components { U_i, S_i, V_i }, and of the watermark image *w* gives { U_w, S_w, V_w}. The embedding algorithm is described as follows:

The embedding process is achieved by linear interpolation of type: i_w=(1-t)*w*+t*i*, where i_w, *w*, *i*, *t* are respectively the watermarked image, the original image, the watermark and *t;* a value between 0 and 1 which is different from 0 and 1.

$$U_{iw} = U_i$$
$$S_{iw} = (1-t)S_w + tS_i$$
$$V_{iw} = V_i$$

where U_{iw}, S_{iw}, V_{iw} are the three components of the image i_w.

SVD$_{inv}$ does not suggest the inverse transform, but rather is the product of the three components: *U*, *S*, V^T. We realize the SVD$_{inv}$, which is the product of the three components in order to obtain a significant image which is given as follows:

$$iw = U_{iw} \times S_{iw} \times V_{iw}^T \qquad (1)$$

In our case, the embedding process consists only of the components *S* of the images *i* and *w*, which suggests that:

U_{iw}=U_i and V_{iw}=V_i ,

This means that we have:

$$iw{=}U_iS_{iw}V_i^T = U_i((1-t)S_w+tS_i)V_i^T = tU_iS_iV_i + (1-t)U_iS_wV_i^T = ti+\beta \qquad (2)$$

while: $\beta = (1-t)U_iS_wV_i^T$

We note that the only unknown in the equation (2) is *t*; this can be interpreted by two cases:-

Case 1 : *t* close to 0, then :

$$iw \rightarrow U_iS_wV_i^T$$

This means that the image i_w is very different from the image *i*.

Case 2: *t* close to 1, then :

$$iw \rightarrow i$$

This means that the image i_w is almost identical to the original image *i.*

Figures 4, 5 and 6 illustrate the resultant image i_w of the embedding process with several values of *t*={0.1 ; 0.5 ; 0.98}, noting that an invisible watermark is achieved in the case where t = 0.98 (close to 1).

Watermark Extraction Process

From the extraction scheme illustrated in figure 2, we note that:

$$U_{wi} = U_w$$
$$S_{wi} = (1-t)S_{iw} + tS_w$$
$$V_{wi} = V_w$$

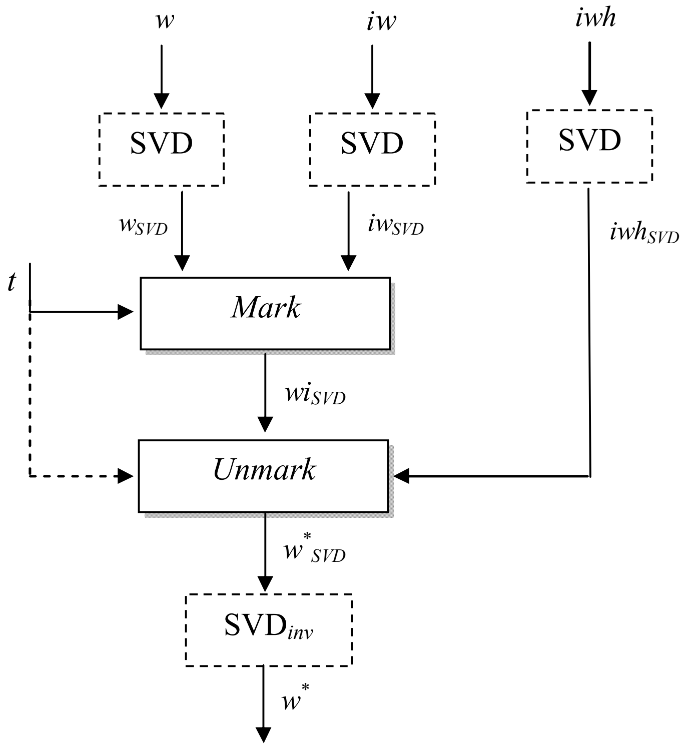


Figure 2: Watermarking Extraction Process

The *Unmark* operation consists of the reverse process, which means that:

$$w^*_{SVD} = \frac{1}{t} w_{iSVD} - \frac{1-t}{t} i_{whSVD} \qquad (3)$$

where i_{wh} is the attacked watermarked image.

Since the embedding process consists of only the *S* components of the original image *i* , and the watermark *w*, we obtained through the extraction process of the extracted watermark *w** in equation (4):

$$t^3 w^* = (U_w - (1-t)U_{iwh})((1-t)S_{iw} + tS_w - (1-t)S_{iwh})(V_w^T - (1-t)V_{iwh}^T) \qquad (4)$$

In equation (4), the only unknown parameter is *t*, which suggests that when t→1, then we have:

$$w^* \rightarrow U_wS_wV_w^T \rightarrow w \qquad (5)$$

This means that the extracted watermark w^* is close to the original watermark *w.*

4. Results and Analysis

For purposes of experimentation with our proposed approach, an original image *i* , and a watermark *w* were chosen as color images of size 256 × 256 × 3. The embedding and extraction processes were both executed using several values of *t* = {0.1, 0.5, 0.98) in order to demonstrate cases of visible and invisible watermarking in the host data. In this paper, the Stirmark Benchmark (Petitcolas, 2012) was used to apply the effect of different attacks on the obtained i_w images for each value of t. For space-limitations in this paper, only the most dangerous attacks are shown to judge the robustness of our proposed approach. Figures 4, 5 and 6 show the extracted watermarks after each attack.

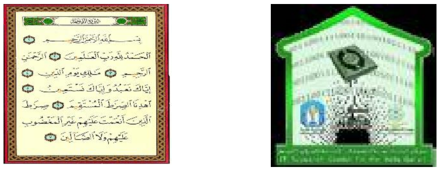


Figure 3: The Original Content and Watermark images used during experimentation (Quran sample, 2013; NOOR, 2013).

For t=0.1 :

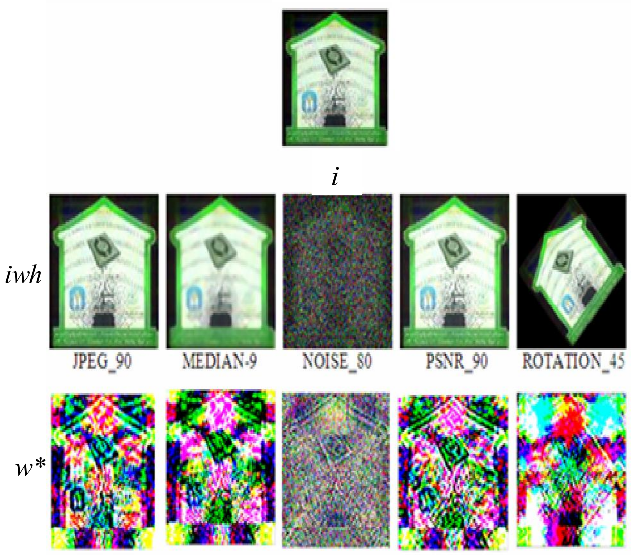


Figure 4: Extracted Watermark when t=0.1

For t=0.5:

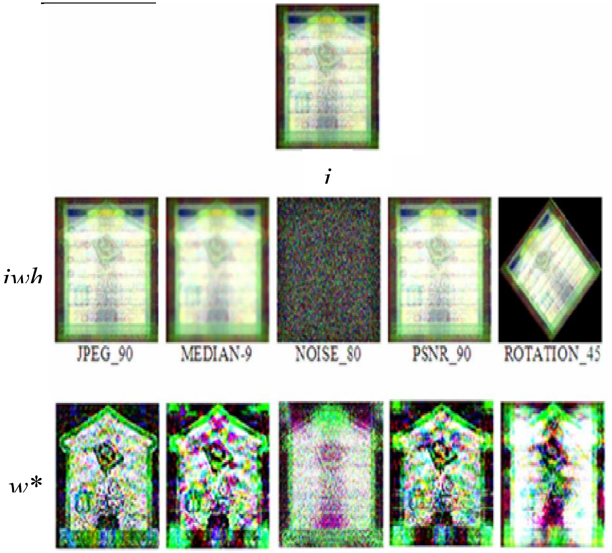


Figure 5: Extracted Watermark when t=0.5

For t=0.98:

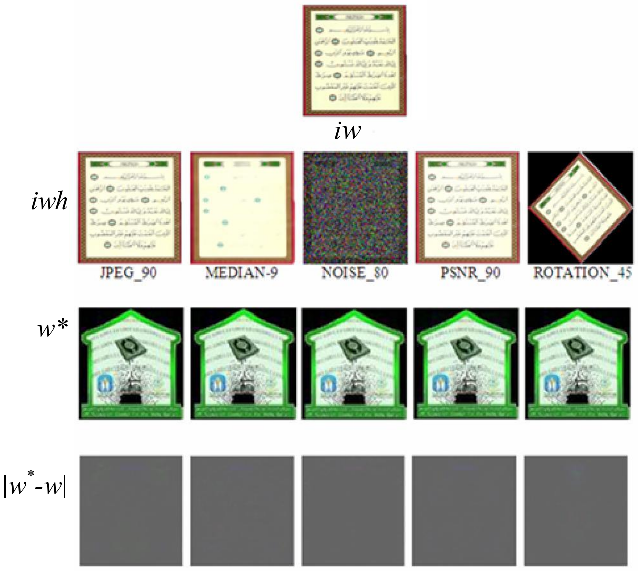


Figure 6: Extracted Watermark when t=0.98

In the purposes of the tests conducted, it was required to calculate the similarity between the original watermark *w* and the extracted one w^* in the case of invisible watermarking (with *t* close to 1) using two different perspectives for analysis of the results. The first perspective is purely mathematical in which we seek the watermark *w* depending on the extracted one, *w** , for the case of invisible watermarking (t → 1), resulting with the conclusion that the extracted watermark *w** is almost identical to the original watermark *w* through equation (5). The second perspective is purely empirical and based on the most known similarity measuring techniques used in the scientific community, including; the Peak Signal-to-Noise-Ratio (PSNR) (Dubolia *et al.*, 2011), the Structural Similarity Index (SSIM) (Brunet *et al.* 2012), the Visual Information Fidelity (VIF) (Sheikh and Bovik 2006), the Universal Quality Index (UQI) (Wang and Bovik. 2002), and the Noise Quality Measure (NQM) (Damera-Venkata *et al.*, 2000). Furthermore, the second analysis-perspective is also used in the case of invisible watermarking, since in other cases, the extraction of the watermark after attacks is significantly different from the original watermark as shown in Figure 4 and 5. The results obtained are shown in Table1 (with $t = 0.98$).

Table1: Performance Results for similarity metrics between w and w^* for various attacks.

	PSNR	SSIM	VIF	UQI	NQM
JPEG	44.8953	0.9874	0.9348	0.9307	35.4979
MEDIAN	45.8716	0.9932	0.9434	0.9353	36.6886
NOISE	37.5956	0.9791	0.8511	0.9035	32.9222
PSNR	48.2278	0.9952	0.9563	0.9443	38.2409
ROTATION	39.3199	0.9628	0.9203	0.9111	32.9946

The significance of each performance metric and the analysis of the results obtained for the various types of attacks are now summarized as follows:

- *PSNR*: is a metric traditionally used for visual quality assessment and still widely used in evaluating the performance of image similarity. Although the performance of PSNR is worse than many other image quality metrics in certain distortion types and respective domains, it is still an appealing performance metric, since it is simple to compute, has clear physical meaning and is mathematically convenient in the context of optimization. Notably from Table 1, all the PSNR results obtained are greater than 34 dB, which suggests a large degree of similarity between the original and the extracted watermarks.
- *SSIM*: is to compare structural information between the reference and distorted images. Considering the assumption that the human visual system is highly adaptive for extracting structural information from a scene, a similarity measure can be constructed based on results of the luminance-comparison, the contrast-comparison and the structure-comparison between the reference and distorted images. From Table 1, it is noted that all SSIM results are very close to 1, which suggests a large degree of similarity between the original and the extracted watermarks.
- *VIF*: is to quantify loss of image information to the distortion process based on natural scene statistics, the human visual system and an image distortion model in an information theoretic framework. It is noted from Table 1 that all VIF results are very close to 1 which suggests a large degree of similarity between the original and the extracted watermarks.
- *UQI*: is similar to SSIM, and it is used to model image distortions as a combination of three factors; loss of correlation, luminance distortion and contrast distortion. It is noted from Table 1 that all UQI results are very close to 1 which suggests a large degree of similarity between the original and the extracted watermarks.
- *NQM*: is a measure aimed at quality assessment of additive noise by taking into account variation in contrast sensitively, variation in local luminance, contrast interaction spatial frequencies and contrast masking effects. From Table 1, it is noted that all NQM results are very above 30, which suggests a large degree of similarity between the original and the extracted watermarks.

In summary of the results, this paper has demonstrated the robustness and security of the proposed approach under known severe attacks from Table 1 in order to maintain the authenticity of the Quran text-image content. Essentially, the approach can be used to establish content-verification and traceability back to its original and legitimate source/publisher through extraction of the watermark that identifies the original source/publisher.

5. Conclusions

This paper addressed the problem of text-image protection and authentication for sensitive digital content using the digital Quran text-image content as a case study. We proposed a very robust and secure approach against the most severe attacks in order to maintain the authenticity of the Quran text-image content and ensures content traceability back to its original and legitimate source/publisher through extraction of the watermark that identifies the genuine source/publisher. The proposed approach shows that the results obtained are very encouraging, and had demonstrated that the watermark could be extracted almost perfectly in most cases following various types of known attacks. In order to analyze the performance results of the proposed approach, a measure of the similarity between the original watermark and the extracted watermark was considered using two perspectives; the first analysis was purely mathematical, where the extracted watermark as a function of the original watermark was used. The first analysis had demonstrated the robustness of our proposed approach. The second analysis was purely empirical, which is widely used approach by researchers in the digital watermarking community. A significant advantage of the proposed approach in this paper was evident in its broad applicability since it can easily be applied for the protection and authentication of other sensitive digital text-image content. Finally, it is anticipated that this work will stress the importance of research directions aimed at developing and advancing the state-of-the-art in multimedia-based watermarking for the specific and stringent requirements of the multimedia host-data/contents under the two major application domains of copyright protection and authenticity-verification/tamper-detection.

Acknowledgements:

The authors acknowledge and thank the support provided by the IT Research Center for the Holy Quran (NOOR) at Taibah University for funding this work under project number NRC1-126, 2012-2013.

Corresponding Author:
Dr. Omar Tayan
College of Computer Science & Engineering and IT Research Center for the Holy Quran and Its Sciences (NOOR)
Taibah University, Saudi Arabia
E-mail: otayan@taibahu.edu.sa

References

1. Golub G. H, and Van Loan C. F, 1996. "The Singular Value Decomposition and Unitary Matrices", *§2.5.3 and 2.5.6 in Matrix Computations*, 3rd ed. Baltimore, MD: Johns Hopkins University Press, pp. 70-71 and 73.
2. Razafindradina H. B, and Randriamitantsoa P. A., 2008. "Robust and Blind Watermarking in the Singular values domain", *Journal Marocain de l'Automatique, de l'Informatique et du traitement de Signal*.
3. Bergman C., Davidson J., 2005. "Unitary Embedding for Data Hiding with the SVD", *Security, Steganography and Watermarking of Multimedia Contents VII*, SPIE Vol. 5681, San Jose, CA, USA.
4. Liu R., Tan T., 2002. "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", *IEEE Transactions on Multimedia*, Vol. 4, No. 1, pp. 121-128.
5. Sverdlov A., Dexter S., Eskicioglu A. M., 2005. "Robust DCT-SVD domain image watermarking for copyright protection : Embedding Data in all Frequencies", 13th European Signal Processing Conference (EUSIPCO 2005), Antalya, Turkey, p. 4-8.
6. Agarwal R., Santhanam M., 2008. "Digital watermarking in the Singular Vector Domain", *International Journal of Image and Graphics,* volume 8, pp 351-362.
7. Zhen L., Kim-Hui Y., and Lei B.Y., 2011. "A New Blind Robust Image Watermarking Scheme In SVD-DCT Composite Domain", 2011 18th IEEE International Conference on Image Processing, pages: 2757-2760.
8. Khorasani M.K., Sheikholeslami M.M., 2012. "An DWT-SVD Based Digital Image Watermarking Using a Novel Wavelet Analysis Function", 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks, pages: 254-256.
9. Sukumar K., Hemalatha T., Soman K.P., "Multi Image-Watermarking scheme based on Framelet and SVD", 2009 International Conference on Advances in Recent Technologies in Communication and Computing, pages: 37-381.
10. Calagna M., Guo H., Mancini L.V., Jajodia S., 2002. "A Robust Watermarking System based on SVD Compression", *IEEE Transactions on Multimedia*, Vol 4, Issue 1, pages:121-128.
11. Petitcolas F., 2012. Watermarking Stirmark, http://www.petitcolas.net/fabien/watermarking/stirmark/.
12. Quran Text-Image Sample, 2013. http://moslmon.own0.com/t68-topic.
13. IT Research Center for the Holy Quran and Its Sciences (NOOR), 2013. http://www.nooritc.org.
14. Dubolia R., Singh R., Bhadoria S.S, Gupta R., 2011. "Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR", 2011 International Conference on Communication Systems and Network Technologies, Page(s): 593 - 596.
15. Brunet D. Vrscay E. R., and Wang Z., 2012. "On the mathematical properties of the structural similarity index ", *IEEE Transactions on Image Processing*, vol. 21, no. 4, pp. 1488-1499.
16. Sheikh H.R., and Bovik A.C., *2006.* "Image information and visual quality", *IEEE Transactions on Image Processing,*Vol.15, no.2, pp. *430- 444.*
17. Wang Z. and Bovik A.C., 2002. "A Universal Image Quality Index", *IEEE Signal Processing Letters,* vol. 9, no. 3, pp. 81-84.
18. Damera-Venkata N., Kite T.D., Geisler W.S., Evans B.L., and Bovik A.C, 2000. "Image Quality Assessment Based on a Degradation Model", *IEEE Transactions on Image Processing*, Vol. 9, No. 4.

5/24/2013