Information Sciences Letters

Volume 7
Issue 1 *Jan. 2018*

Article 1

2018

Secure Watermarking Algorithm based on DNA Sequence Using DWT-SVD

Marghny H. Mohamed
Computer Science, Faculty of Computer and Information, Assiut University, Egypt, nomail@naturalspublishing.com

Saad Z. Rida
Mathematics, Faculty of Science, South Valley University, Egypt, nomail@naturalspublishing.com

Basma Ahmed A. Hafez
Computer Science, Faculty of Science, South Valley University, Egypt, nomail@naturalspublishing.com

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/070101

Secure Watermarking Algorithm Based on DNA Sequence Using DWT-SVD

Marghny H. Mohamed[1], *Saad Z. Rida*[2], *Basma Ahmed A.Hafez*[3,*]

[1] Computer Science, Faculty of Computer and Information, Assiut University, Egypt
[2] Mathematics, Faculty of Science, South Valley University, Egypt
[3] Computer Science, Faculty of Science, South Valley University, Egypt

Received: 22 Oct. 2017, Revised: 22 Nov. 2017, Accepted: 24 Dec. 2017.
Published online: 1 Jan. 2018.

Abstract: Due to the continuous development of information technology and the widespread use of digital media, such as text, videos, and digital images, the digital watermark has become one of the most important methods to protect digital media from tampering. DNA sequence-based image has been used as a biometric watermark for copyright protection and authentication, where the DNA sequence is a unique biometric feature and difficult to copy or duplicate. We have been presented a watermarking algorithm that based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD), in order to achieve imperceptibility. The quality of the watermarked image has been measured using peak signal to noise ratio (PSNR), at different DNA sequence-based images. This algorithm can be used for authentication and data hiding purposes.

Keywords: Digital Watermarking, DNA, Discrete wavelet transformation, Singular value decomposition.

1 Introduction

The evolution of the Internet and the augmentation availability of multimedia applications development of technologies have led to the emergence of copyright issues, as a result, the concept of digital watermark become a branch of information hiding [1]. Information hiding is a technique to protect information from any modification, steganography and watermarking one of its sections, and each has its own algorithms [2].

A digital watermark is a technique of inserting information such as a number, text, image within a digital object like image, text, audio file and digital video file to protect the rights of the owner and authentication. Because of the clone of digital content which can be distributed with less quality differ from original version this illegal duplication results in material damage to content providers [3].

Watermarking technique should have two main characteristics: the first one is the imperceptibility which means that the digital watermarking should be perceptually invisible to prevent the deterioration of the original image and no one can see and determine where the watermark is inserting and it is difficult to change or modify it [4,5]. The second characteristic is the robustness, where the embedded watermarking information must resist processing of the image, such as compression, cropping, resizing, rotation and others attacks. For images, this means that the pixel value modification should be invisible [6,7]. There are many applications of digital watermarking like ownership verification, broadcast monitoring, copyright protection, content authentication, medical purpose and copy control.

Digital watermarking can be categorized according to the processing domain into two classes: spatial-domain and frequency-domain. In spatial-domain, the image is treated directly by changing its pixels. In frequency-domain, the watermark inserted by alteration the frequency bands. The frequency domain is more accurate than the spatial domain because it analyzes the image to lower coefficients [8,9].

Biometric characteristics can be used in copyright protection and authentication like face, retina, ear features, iris, a fingerprint image and DNA codes, i.e. personalized watermarking which is suitable for security systems, where it is unique and difficult to copy or duplicate.

A blind digital watermarking algorithm based on DNA sequence-based image (as a watermark), singular value decomposition, and discrete wavelet transform have been proposed. The proposed algorithm is robust where it uses SVD approach, and secure where it uses DNA sequence which is one of the most uniquely biometric features. The proposed algorithm uses high-frequency sub-

*Corresponding author e-mail: basma_hafez@sci.svu.edu.eg

band to embed watermark in order to achieve high imperceptibility [10].

Two algorithms have been proposed in [11], content-based watermark algorithm using DNA sequence (CBDNA) and user specified watermark algorithm using DNA sequence (USDNA) based on digital images watermarking by using DNA sequence. An algorithm has been introduced in [12] for watermarking of digital images by using biometric human voice as the original watermark which is embedded in the image. In [13], video watermarking algorithm by using biometric fingerprints based on two-level DWT has been proposed. DNA watermarking for DNA copyright protection by encoded DNA sequence and insert it in DNA based on DWT transformation was introduced in [14]. A digital watermarking method based on DWT and SVD with high accuracy and resistant to attacks for copyright protection has been discussed in [15].

The paper is organized as follows. Section 2 presents the DNA review. Section 3 shows the proposed discrete wavelet transform (DWT). Singular value decomposition SVD is explained in section 4. The proposed algorithm is presented in section 5.The experimental results proposed in section 6 and the conclusion of the paper is described in Section 7.

2 DNA Review

DNA carries the genetic characteristics of the organism; every cell in a person's body has the same DNA. Most DNA is found in the cell nucleus but mitochondria contain a small Quantity of DNA [16, 17].

DNA consists of simpler structures called nucleotides. One part of DNA consists of thousands or millions of nucleotides. Each nucleotide consists of a sugar, and phosphate and base. These bases are adenine (A), guanine (G), cytosine (C), and thymine (T). Chemically DNA is similar in all living organisms and what distinguishes these organisms is a sequence of characters. The DNA code consists of different letters in the nucleotides, the cell reads the instructions that appear on the DNA of different letters. Every 3 letters consist of a word called "codon", for example, ATC TCA GGA AAT GCC CAG.

Although there are only four different letters, DNA molecules consist of thousands of letters. This allows for billions of different combinations. Due to the nature of the DNA in the form of large sequences of nucleotides and the possibility of conversion into numbers used in the field of hiding information such as encryption, watermarking and Steganography [18].

3 Discrete Wavelet Transform (DWT)

In the image processing, an image can be converted from spatial domain into frequency domain using mathematical transformation like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), etc.

Wavelet conversion from time domain to frequency domain has been widely used in the fields of signal processing and image compression, because of using multi-resolution decomposition which divides the image into four sub-bands:(HH, LH, HL, LL)as shown in figure1.

LL	HL
LH	HH

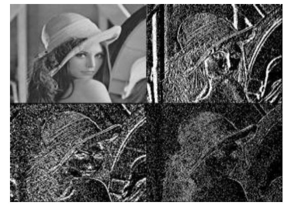


Figure (1), 1-level of discrete wavelet transform

To achieve image robustness, embedding must be done in the low-frequency domain LL [19,20].The segment with the high frequencies is mainly the edge components of the signal. The segment with the low-frequencies is divided again into two parts of high and low-frequencies. The two levels decomposition of DWT appears in figure 2. This process is repeated a number of times, depending on the application used.

<table>
<tr><td>LL1</td><td>LH1</td><td rowspan="2">LH</td></tr>
<tr><td>HL1</td><td>HH1</td></tr>
<tr><td colspan="2">HL</td><td>HH</td></tr>
</table>

Figure(2), 2-level of discrete wavelet transform

4 Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is a mathematical technique which decomposes a given matrix into three component matrices. SVD has many applications, in image processing field for example image hiding, noise reduction, and image watermarking because the singular values of an image do not change greatly when a small chaos is added to an image [21-23].

In linear algebra, the image can be considered as a matrix with positive values. If A is a square matrix, A $\in R^{n*n}$ since R is the set of real numbers, the SVD of the matrix A is:

$$A = USV^T.$$

Where U is an orthogonal matrix, S is a diagonal matrix containing the singular values A, and V is an orthogonal matrix. Using the SVD in digital image processing does not affect image quality by adding a little confusion.

Inf. Sci. Lett. 7, No. 1, 1- 6 (2018) / http://www.naturalspublishing.com/Journals.asp

5 Proposed Algorithm

In the proposed watermarking algorithm, DNA sequence converted into an image as a watermark, then using DWT transformation and SVD decomposition in the frequency domain. The image in frequency domain split into four sub-bands(HH, HL, LH, LL) in the proposed algorithm We choose HH sub-band to include the watermark because the edges of the image are concentrated in the high-frequency sub-bands HH and the Human Visual System (HVS) is less sensitive to changes in these sub-bands, so this sub-bands used for watermarking, this results that the watermarking algorithm is imperceptible, the proposed algorithm uses DNA sequence which is one of the most uniquely biometric features for this the algorithm is more secure.

5.1 Watermark Embedding Algorithm

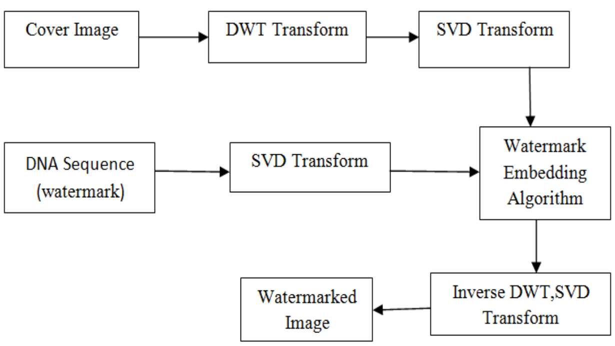


Figure (3), the block diagram of watermark embedding process.

The flowchart of the proposed algorithm for embedding a DNA watermark is shown in figure 3 and the algorithm can be summarized in the following algorithm.

Step 1: Read DNA sequence and convert DNA sequence to DNA digital image W.
Step 2: Read cover Image.
Step 3: Read DNA image (watermark)W.
Step 4: Apply SVD to decompose watermark W by $A_W = U_W S_W V_W^T$.
Step 5: Use DWT transformation to decompose cover image into four sub-bands(HH,HL,LH,LL).
Step 6: Apply SVD to HH sub-band by $A_{HH} = U_{HH} S_{HH} V_{HH}^T$.
Step 7: Modify singular values of HH sub-band with watermark W.
Step 8: Apply inverse SVD as $A_{HH'} = U_{HH} S_W V_{HH}^T$.
Step 9: Obtain the watermarked image by using inverse DWT.

5.2 Watermark Extraction Algorithm

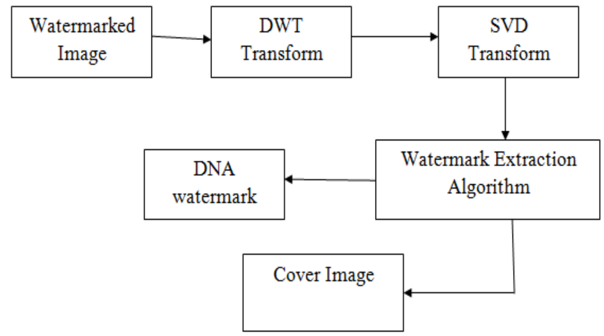


Figure (4), the block diagram of watermark extraction process.

The flowchart of the proposed algorithm for extraction a DNA watermark is shown in figure 4 and the algorithm can be summarized in the following algorithm.

Step 1: Read watermarked Image.
Step 2: Use Discrete Wavelet transform to decompose watermarked image into four sub-band(HH,HL,LH,LL).
Step 3: Apply SVD to HH sub-band $A_{HH} = U_{HH} S_{HH} V_{HH}^T$
Step 4: Obtain the singular values from HH sub-band.
Step 5: Extract the DNA watermark $A_{W'} = U_W S_{HH} V_W^T$.

6 Experimental Results

The algorithm performance investigated using three different digital cover images; these are Lena, Madril, and Peppers with size 512×512. As watermark, three different DNA watermark images are used, DNA1-image of size 178×128 was created using DNA1 sequences (locus: AM263178) gene ID:118122736, DNA2-Image of size 187×128 was created using DNA2 sequences (locus: ASY31260) gene ID:1240568788, and DNA3-Image of size187x128 was created using DNA3 sequences (locus: NP_001342071) gene ID:1240431728.The aforementioned DNA sequences were obtained from the National Center for Biotechnology Information (NCBI) database [24].

The qualities of the watermarked images were evaluated by using peak signal to noise ratio (PSNR). The signal-to-noise ratio of the image can be calculated using the mean square error(MSE). The value of MSE is estimated by the difference between the cover image and the watermarked image as:

$$\text{MSE} = \frac{1}{MN}\sum_{X=1}^{M}\sum_{Y=1}^{N}[T(x,y) - T'(x,y)]^2, \quad (1)$$

where $T(x,y)$ and $T'(x,y)$ give the pixel value at position $(x,y)$of the cover image and the watermarked image respectively. The larger value (PSNR) means an imperceptible watermark method and indicates less degradation. The equation that represents Peak signal to noise ratio (PSNR) can be written as follow:

$$PSNR = 10 * log_{10}\left[\frac{225^2}{MSE}\right]. \quad (2)$$

Table1, Obtained results using DNA1-image as a watermark.

Cover image name	Cover image	DNA watermark	Watermarked	PSNR	Extracted DNA watermark
Lena				**38.9046**	
Peppers				**37.4778**	
Madril				**30.7826**	

Table2, Obtained results using DNA2-image as a watermark.

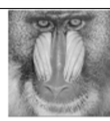
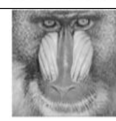
Cover image name	Cover image	DNA watermark	Watermarked	PSNR	Extracted DNA watermark
Lena				**38.7364**	
peppers				**37.1841**	
Madril				**30.7258**	

Table3, Obtained results using DNA3-image as a watermark.

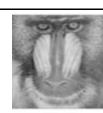
Cover image name	Cover image	DNA watermark	watermarked	PSNR	Extracted DNA watermark
Lena				**38.6858**	
Peppers				**37.2608**	
Madril				**30.8397**	

Table4, the PSNR value of V. Santhi and A. Thangavelu algorithm and our algorithm

Cover Image	Algorithm	PSNR
Cameraman 	V. Santhi and A. Thangavelu CBDNA algorithm	32.9448
	V. Santhi and A. Thangavelu USDNA algorithm	32.5267
	Our algorithm	41.9492

Generally, the obtained results show that the embedded DNA watermarks do not deform the quality of the watermarked cover image, as indicated in the fourth column with title "watermarked cover image", in tables 1, 2, and 3. It is clear from the tabulated results that the algorithm is imperceptible where the watermark inserted in HH sub-band.

By inspecting the third and sixth columns in tables 1, 2, and 3; the essential identical between DNA watermark and extracted DNA watermark emphasizes the robustness of the used algorithm.

In terms of the (PSNR) measure, it is clear that for example at Lena-cover image, the investigated algorithm provides almost the same PSNR values at DNA1, DNA2, and DNA3 watermarks. The same notice can be observed at both Peppers, and Madril-cover images tables in 1, 2, and 3. This illustrates an aspect of the robustness of the investigated algorithm at different watermarks. The proposed algorithm achieves high PSNR values, where the value of MSE which estimated by the difference between the cover image and the watermarked image is very small (equations 1, and 2) thus, the proposed algorithm indicates less degradation.

Table 4, shows a comparison between Santhi and A.Thangavelu [11] watermarking algorithm and our algorithm, where Cameraman-cover image used in the experiment, the results demonstrate that our algorithm has a higher PSNR where we have been used DWT, SVD transformation. The proposed digital watermarking algorithm that depends on DNA watermarks achieves invisibility, imperceptibility and hence security.

7 Conclusion

In the current paper, a new blind digital watermarking algorithm was introduced. The proposed algorithm uses DNA sequence as a unique watermark. DWT and SVD have been employed in order to achieve both imperceptibility and security. Where the proposed algorithm is a blind watermarking technique, it does not need the original image in the process of watermark image recovering.

The experiment results of the proposed algorithm revealed a good imperceptibility, where it uses high-frequency sub-band to embed a watermark and a great improvement in security. The proposed algorithm was investigated in the cases where there are not any types of attacks. Attacks presence and its effects on the performance of the proposed technique will be considered.

References

[1] H. Marghny. Mohamed, M. N. Al-Aidroos, and A. M. Bamatraf, "Data hiding technique based on LSB matching towards high imperceptibility," MIS Review, pp. 57-69, 2012.

[2] M. Mohamed, F. Al-Afari, and M. A. Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation," Int. Arab J. e-Technol., vol. 2, pp. 11-17, 2011.

[3] H. Rawat and A. K. S. Kumar, "Robust Digital Image Watermarking Scheme for Copyright Protection," International Journal of Computer Applications, vol. 75, 2013.

[4] M. H .Mohamed and H. I. Abul-Kasim, "Data Hiding by LSB Substitution using Gene Expression Programming," extraction, vol. 10, p. 5, 2012.

[5] M.H. Marghny, S. E. El-Gendi, F. Al-Afari and M. El-Melegy, "Steganography for Secure Data Communication" Msc Thesis, Faculty of Science, Assiut University, pp. 120,2009.

[6] V. Bohara and S. Toshniwal, "A Review of Different Secret Image Watermarking," International Journal of New Technology and Research (IJNTR), ISSN: 2454-4116, Volume 3, Issue-1, January 2017 Pages 71-76.

[7] M. Mohamed, A. Al-Mehdhar, and M. Bamatraf, "SOM PAD: Novel Data Security Algorithm on Self Organizing Map," Computer Science and Information Technology (CS and IT), 2012.

[8] P. Sharma and S. Swami, "Digital image watermarking using 3 level discrete wavelet transform," in Conference on Advances in Communication and Control Systems, 2013, pp. 3-24.

[9] H. Marghny Mohamed, M. Naziha AL-Aidroos and A. Mohamed Bamatraf, "A combined image Steganography technique based on edge concept and dynamic LSB," International Journal of Engineering Research and Technology, vol. 1, 2012.

[10] M. H. Mohamed and L. M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method," Applied Mathematics & Information Sciences, vol. 10, p. 259, 2016.

[11] V. Santhi and A. Thangavelu, "A robust digital image watermarking algorithm using DNA

sequences," International Journal on Image and Video processing (ICTACT), vol. 1.

[12] R. Saxena, K. Shah, R. Chawla, and V. Santhi, "Biometric Watermarking for Copyright Protection of Digital Images," International Journal of Applied Engineering Research, vol. 9, pp. 23681-23688, 2014.

[13] S. Jung, D. Lee, S. Lee, and J. Paik, "Robust watermarking for compressed video using fingerprints and its applications," International Journal of Control, Automation, and Systems, vol. 6, pp. 794-799, 2008.

[14] S.-H. Lee, "DWT based coding DNA watermarking for DNA copyright protection," Information Sciences, vol. 273, pp. 263-286, 2014.

[15] A. K. Gupta and M. S. Raval, "A robust and secure watermarking scheme based on singular values replacement," Sadhana, vol. 37, pp. 425-440, 2012.

[16] J.D. Watson" Molecular Biology of the Gene, Fifth Edition 5th Edition"2004, 732 pp, hardcover/CD-ROM.

[17] M. Mohamed, A. A. Al-Mehdhar, M. Bamatraf ، and M. R. Girgis, "Enhanced Self-Organizing Map Neural Network for DNA Sequence Classification," Intelligent Information Management, vol. 5, p. 25, 2013.

[18] A. Mendez, R. James" A Comparative Study of Robust Blind Image Watermarking Scheme for Image Authentication Using DNA Encoding, Optimal Wavelet Basis& Discrete Wavelet Transform" International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 9, September 2015.

[19] M. H. Mohamed, Y. B. Mahdy, and W. A. E.-W. Shaban, "Confidential Algorithm for Golden Cryptography Using Haar Wavelet," arXiv preprint arXiv:1501.03617, 2015.

[20] X.-G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," in Image Processing, 1997. Proceedings., International Conference on, 1997, pp. 548-551.

[21] L. Rajab, T. Al-Khatib, and A. Al-Haj, "Video watermarking algorithms using the SVD transform," European Journal of Scientific Research, vol. 30, pp. 389-401, 2009.

[22] K. A. Al-Afandy, E.-S. M. EL-Rabaie, F. E. A. El-Samie, O. S. Faragallah, A. ELmhalaway, and A. Shehata, "Robust Color Image Watermarking Technique Using DWT and Homomorphic based SVD," in The International Congress for global Science and Technology, 2016, p. 9.

[23] M. H. Mohamed, N. M. Al-Aidroos, and M. A. Bamatraf, "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference".

[24] The National Center for Biotechnology Information https://www.ncbi.nlm.nih.gov/

Marghny H. Mohamed is a Professor of Computer Science, Vice Dean of Faculty of Computers and Information, Assiut University. He received his Ph.D. degree in computer science from the University of Kyushu, Japan, in 2001, his M.Sc. and B.Sc. from Assiut university, Egypt, in 1993 and 1988, respectively. His research interests include data mining, text mining, information retrieval, web mining, machine learning, pattern recognition, neural networks, evolutionary computation, fuzzy systems and information security. Dr. Marghny is a member of the Egyptian mathematical society and Egyptian syndicate of scientific professions.

Saad Z. Rida is a Professor of Mathematics, Mathematics Department, Faculty of Science, South Valley University. Ph. D. of Mathematics, Fachbereich Mathematik und Informatik, Freie Universität Berlin, Germany, in 1996. M. Sc. in Mathematics, Faculty of Science (Assiut), Assiut university, Egypt, in 1989. He is referee and Editor of several international journals in the frame of pure and applied mathematics. His main research interests are: Mathematical analysis, Fractional Calculus, Differential equations, Mathematical modeling, Soliton theory, Bio-Mathematics.

Basma Ahmed A. Hafez is a Demonstrator in the Department of Mathematics, Faculty of science, South Valley University. Received her B.SC.in Computer Science from faculty of Science, South Valley University, in 2009.