USING DIGITAL WAVELET TRANSFORM WITH COLORED IMAGES TO HOST SECRET SIGNATURES FOR ENSURING THE INTEGRITY OF CONTENT

[1]ABDALLAH S.N. AL-TAHAN AL-NUAIMI, [2]ABDULLAH.M.F.AL_ALI

[1,2]Faculty of Information Technology, Isra University
E-mail: [1]abdstn@iu.edu.jo, [2]Abdulla.Alali@iu.edu.jo

Abstract- Handwritten signatures were used over hundreds of years to prove the identity of certain person. Moreover, handwritten signatures were used to prove the content integrity of certain document. This work gives a new procedure of hiding digital signature in digital colored images that solves the challenge of identity and integrity. The proposed procedure depends on changing the digital colored image from spatial domain to discrete wavelet transform domain and hiding the digital signature secretly in the transformed image. Then, the resultant image is retransformed to the spatial domain. The human visual system cannot differentiate between the original image and the image that carrying the secrete signature. The used procedure gives the signature strength and stiffness sufficient to overcome different types of attacks.

Keywords- Digital Signature, Identity, Content Integrity, Digital Wavelet Transform, Watermarking.

I. INTRODUCTION

Handwritten signatures were used in most countries hundreds of years to define the identity of the writer of any document. Also, handwritten signatures were used to give the originality and integrity of written contents. Now days, the digital world depends on transferring information using different kinds of multimedia. This gives more importance for images than words and writing. So, digital signature appears as a new concept of writing signatures using computers. But, the digital signature can be attacked from unauthorized persons who try to delete it or to change its contents.

The most robust way of using digital signature is to hide it in certain digital colored image to be invisible for the human visual system. This can be done using different types of hiding procedures. In [1-5], certain numerical data was hidden in digital images to identify the owners. In spite of the success of hiding these types of digital signatures invisibly, the hidden data is very little and does not give rich information and it could be attacked easily. Amplitude modulation was used in [6] to hide certain numbers for identifying the owner. The hidden data represents certain numerical information without any visual information.

Regarding the domain that is used for hiding the secret information, the well-known ways of hiding the secret information in digital images were divided into two main types. The first way, which is simpler and direct, uses the spatial domain of the image to directly carry the secret information invisibly [7-15]. This way is not complicated and it needs fewer calculations. It gives good results regarding the invisibility of the secret information, the security and the robustness of the hidden information against attacks. The second way depends on transforming the digital image to certain transform domain then hides the secret information in the transformed copy of the image [16-20]. This way is more complicated and needs more calculations. But, it is more secure and has better ability than the first way to overcome the dangerous types of attacks.

In this work, the digital colored image will transformed firstly to the discrete wavelet transform, which represents the transform domain that will be used, and then the discrete information that represents the digital signature will be hidden in the transformed version of the image.

The coming sections of this paper were organized as follows. Section two contains the hiding and the extraction processes of the digital signature. Section three contains the experimental results visually and numerically. In section four, the conclusions were highlighted and the future work was suggested.

II. SIGNATURE HIDING AND REMOVING

2.1. Signature Hiding

The procedure of hiding the digital signature in this proposed work has many successive steps to ensure high degree of security. The original Red, Green and Blue (RGB) colored image is transformed to another type of color format (YIQ).

This type of color format separates the colored image into three layers, one of them contains the visual intensity information and the other two contain the visual colors information. The intensity layer is transformed into discrete wavelet transform (DWT) domain. At the other hand, the digital signature is designed using direct writing using any proper computer software or takes a scanned version of handwritten signature. The resultant signature image will be a black/white image.

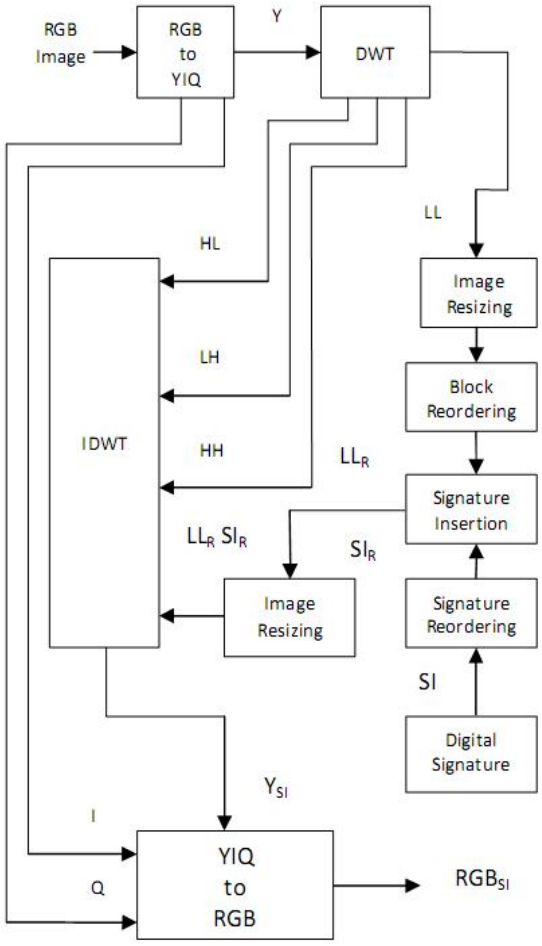


Fig. 1. Signature hiding process

The pixels of this image are reordered using certain secret key to get a new version of the signature without visual meaning.

The low-low (LL) part of the discrete wavelet transformed layer of the colored image is divided into blocks. These blocks were reordered using another secret key. Each pixel of the modified version of the signature is inserted in one block of the modified version of the (LL_R) part of the image. The resultant version of (LL_RSI_R) that is carrying the modified signature is combined with the other three parts of the image by using inverse discrete wavelet transform to change the image to the spatial form to get (Y_{SI}). Then, the color layers (I) and (Q) are combined with (Y_{SI}) and transformed to RGB color format to get (RGB_{SI}). The complete block diagram that explains the process is seen in figure 1.

The insertion process of the signature pixels in the (LL_R) part of the image depends on both the signature pixel value and the pixel values of the (LL_R) part [21]. If the signature pixel value is zero, all the pixels of the odd rows of (LL_R) part changed to take the minimum value of each row. While, all the pixels of the even rows of (LL_R) part changed to take a new value by subtracting certain adjustable value from each pixel value. In contrast, if the signature pixel value is one, all the pixels of the even rows of (LL_R) part changed to take the maximum value of each row. While, all the pixels of the odd rows of (LL_R) part changed to take a new value by adding certain adjustable value to each pixel value.

The values that are added to or subtracted from the pixel values represent the digital signature itself. These changes do not affect the quality of the image. The presence of the signature in the image is invisible for the human visual system.

2.2. Signature Extraction

The signature can be obtained by extracting it from the colored image that carries it. The procedure of extraction has several successive steps similar to the hiding process in reverse order. First of all, the colored image that carries the signature (RGB_{SI}) is transformed from (RGB) color format to (YIQ) color format. Then, the intensity layer (Y_{SI}) is transformed from spatial domain to discrete wavelet transform (DWT) to get the (LL_RSI_R) part that contains the signature. After that, the values of the pixels of each block of the (LL_RSI_R) part are added together. If the result is greater than the addition of the pixel values of the same block of the original image, the value of the signature pixel is one. In contrast, if the result is less than the addition of the pixel values of the same block of the original image, the value of the signature pixel is zero. Finally, the pixels of the resultant image for the signature are reordered using the same secret key to get the original signature.

2.3. Attacks Against Signature

The hidden digital signature maybe suffers from several types of attacks. Some of the attackers just want to see the signature. Others want to destroy the signatures. Some of the others attackers want to exchange the signature by another one. This proposed procedure of hiding signatures can overcomes most of the strong attacks.

II. EXPERIMENTAL RESULTS

To examine the proposed procedure, several colored images were used with several types of digital signatures. Also, several types of attacks were used to examine the robustness of the signatures hidden in the images. Figures 2, 3, 4 and 5 give good examples of visual experimental results. The original image appears in Fig. 2. (a). The image that carries the signature appears in Fig. 2. (b). The visual difference between the two images appears in Fig. 2. (c). There is no difference between the image before and after carrying the signature.

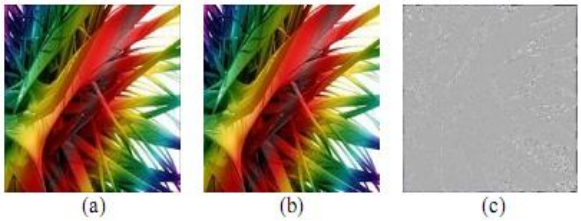


Fig. 2. The Imagery Results for IM1 and signature 1, (a) The original Image, (b) The Image Carrying the Signature, (c) The difference Between (a) and (b)

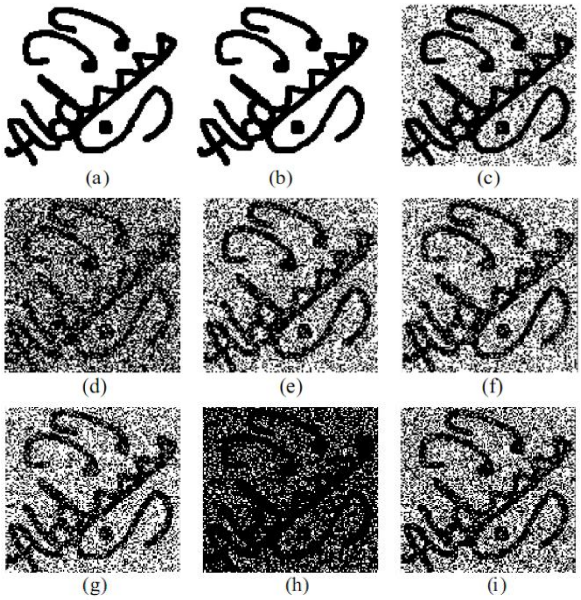


Fig. 3. The Imagery Results for the extracted signature for IM1 and Sig1, (a) The original signature image, (b) The signature image after extraction without any attack, (c) The extracted image after facing low pass filtering attack, (d) The extracted image after facing median filtering attack, (e) The extracted image after facing scale down attack, (f) The extracted image after facing JPEG compression attack, (g) The extracted image after facing cropping attack, (h) The extracted image after facing rotation attack.

Figure 3 represents the extracted signature after the image that carries the signature faced several types of attacks. Fig. 3. (a) represents the original signature before hide it in the image. Fig. 3. (b) represents the extracted signature when the image does not face any type of attack. Fig. 3. (c)-(h) represents the extracted signature after the image faced low-pass filtering, median filtering, scaling, JPEG compression, cropping and rotation attacks respectively. It is obvious that the hidden signature overcomes all the strong attacks. Besides that, the hiding of the signature does not affect the image quality. Moreover, the signature itself is invisible and the human visual system cannot see it.

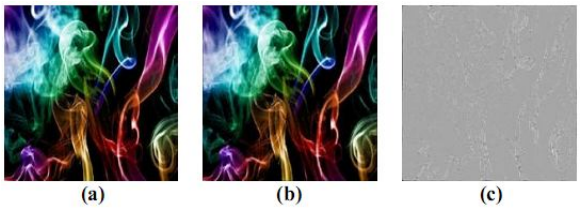
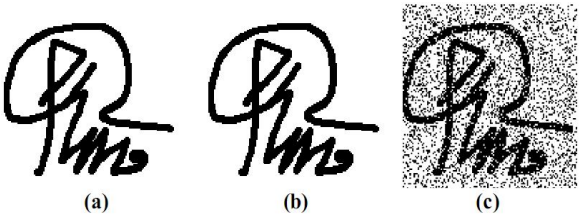


Fig. 4. The Imagery Results for IM2 and signature 1, (a) The original Image, (b) The Image Carrying the Signature, (c) The difference Between (a) and (b)



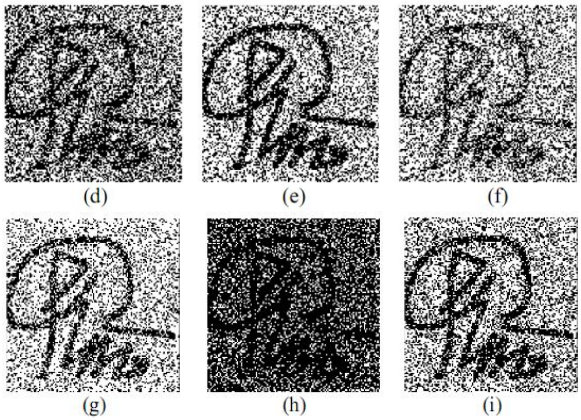


Fig. 5. The Imagery Results for the extracted signature for IM1 and Sig1, (a) The original signature image, (b) The signature image after extraction without any tampering violation, (c) The extracted image after facing low pass filtering attack, (d) The extracted image after facing median filtering attack, (e) The extracted image after facing scale down attack, (f) The extracted image after facing JPEG compression attack, (g) The extracted image after facing cropping attack, (h) The extracted image after facing rotation attack.

Figures 4 and 5 are similar to figures 2 and 3 respectively but with different image and different signature.

The invisibility and image quality can be computed numerically by using the measurements of peak signal to noise ratio (PSNR) which is calculated using the following equation [20]:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} = 20 \log_{10} \frac{255}{\sqrt{MSE}} \quad (1)$$

Where MSE represents the mean square error of the original image and the image that carrying the signature. The average (PSNR) for 20 test images is 36 dB. This high value represents the high similarity between the two images before and after carrying the signature.

In comparing these results with the results in [6], the proposed procedure in this work is more active with better capacity to carry more information. Moreover, the visual signature gives more information than that of [6]. In comparing the results with the results of [21], the visual results appeared to be the same. The (PSNR) measurements of this work is slightly below the (PSNR) calculated in [21], 36dB versus 38dB, the signature in this work is more secure, since the signature was hidden in the discrete wavelet transform domain instead of directly hide the signature in the spatial domain. The visual results seems to be the same for the human visual system and in all cases the signature is invisible.

CONCLUSIONS

The proposed procedure in this work proves the ability of hiding secret digital signature within colored image to prove the identity and the content

integrity. The visual and numerical results that were obtained using experimental tests prove that the signature hiding does not affect the quality of the image. The signature can hold valuable visual information with large payload and the capacity of the colored image is very high to carry large signatures. Several colored images, several types of digital signatures and several types of strong attacks were used to examine the proposed procedure of hiding signatures and the results for all were very good. The future work suggested in this work is to use colored digital signatures that maybe hidden in the colored images.

REFERENCES

[1]. S. Burgett, E. Koch, and J. Zhao, "A novel method for copyright labeling digitized image data", IEEE Transactions on Communications, September 2004.

[2]. W. Bender,D. Gruhl, and N. Mormoto, "Techniques for data hiding," in SPIE, vol. 2420, February 1995.

[3]. I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Technical Report 95-10, NEC Research Institute, 1995.

[4]. K. Matsui, and K. Tanaka, "Video-steganography: how to secretly embed a signature in a picture ," Journal of The Interactive Multimedia Association Intellectual Property Project, 1(1): 187-206, January 1994.

[5]. R. Van Schyndel, A. Torkel, and C. Osborne. "A digital watermark," in IEEE International Conference on Image Processing, vol. 2, 86-90, 1994.

[6]. M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," Storage and Retrieval for Image and Video SPIE 3022, vol. 518, pp. 518-526, January 1997.

[7]. A. Mohammad, A. Alhaj, S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership, signal processing, Elsevier, vol. 88, 2158-2180, 2008.

[8]. C. Lu, and H. Liao, "Multipurpose watermarking for image authentication and protection. (IEEE) Transaction on Image Processing, vol. 10, 1579-1592, 2001.

[9]. W. Zeng,and B. Lio, "A statistical watermark detection technique without using original images for resolving rightful ownership of digital images, Transaction on Image Processing, IEEE, vol. 8. 1534-1548. 1999.

[10]. M. Celik, G. Sharma, , E. Saber, and A. Teklap, "Hierarchical watermarking for secure image authentication with localization, IEEE Transaction on Image Processing, vol. 11, no. 6, 585-595. 2004.

[11]. J. Tzeng, , W. Hwang, and I. Chern, " Enhancing image watermarking methods with/without reference images by optimization on second-order statistics. IEEE Transactions on Image Processing, vol. 7, 771-782. 2002.

[12]. I. Pitas, " A method for watermark casting on digital image. IEEE Transactions on Circuits System and Video Technology. vol. 8,775-780, 1998.

[13]. A. Al-tahan Al-nu'aimi, and R. Qahwaji, "An adaptive watermarking technique for digital colored images. IEEE 2nd International Conference on Information & Communications Technologies: From Theory to Applications, vol. 1, 729-732, 2006.

[14]. J. Hernandez, , M. Amado, and F. Perez-gonzalez, "DCT-domain watermarking techniques for still images, detector, performance analysis and a new structure. IEEE Transactions on Image Processing, vol. 9, 55-68, 2000.

[15]. X. Xia, , C. Bancelet, and G. Arce, "Multi-resolution watermarking based on wavelet transform for digital images. Proc. International Conference on Image Processing, vol. 3, 26-29, 1997.

[16]. Y. Wang, , J. Doherty, and R. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions on Image Processing, vol. 11 (2), 77-88, 2002.

[17]. A. Latif, A. Nachsh-nilchi, "Digital image watermarking based on parameters amelioration of parametric Slant-Hadamard transform using genetic algorithm", International Journal of Innovative Computing, Information and Control, vol. 8 (2), 1205-1220, 2012.

[18]. T. Chen, G. Horng, and S. Wang, "A robust wavelet-based watermarking scheme using quantization and human visual system model". Pakistan Journal of Information and Technology, 2 (3), 213-230, 2008.

[19]. R. Anderson, F. Petitcolas, "On the limits of steganography, (IEEE, Ed). Journal of Selected Area in Communications, 16 (4), 474-481, 1998.

[20]. A. Al-tahan Al-nu'aimi, R. Qahwaji, "Digital colored images watermarking using YIQ color format in discrete transform domain. The Fourth Saudi Technical Conference and Exhibition, 383-388. Riyadh. 2006.

[21]. A. Al-tahan Al-nu'aimi, "Digital Secure Signature Using Digital Colored Images As A Communication Carrier", ICCTE2015, 2nd International Conference on Computing, Technology and Engineering, 23-24 Nov. 2015. Dubai.

★★★