ISSN 2278-3083

International Journal of Science and Applied Information Technology (IJSAIT), Vol.4 , No.5, Pages : 40-43 (2015)
Special Issue of ICCTE 2015 - Held during 23 – 24 November, 2015 in Hotel Crowne Plaza, Dubai
http://warse.org/IJSAIT/static/pdf/Issue/iccte2015sp07.pdf

Digital Secure Signature Using Digital Colored Images as a Communication Carrier

Abdallah Al-Tahan Al-Nu'aimi
Department of Computer Multimedia Systems
Isra University
Amman, Jordan
abdstn@iu.edu.jo

Abstract **- Signature was used several hundreds of years as a proof of identity and integrity of intent. In now days, computers and computer-like devices take the lead of communication processes between peoples. Therefore, digital signature proved to be the new generation of signatures. In this work, a new technique of hiding a digital signature in colored images and transmit it as secret information to intended receiver. The proposed technique is very secure and robust enough to protect the secrete information that the digital signature carries. Moreover, the digital signature here invisible and the human visual system cannot detect it and any illegal viewer cannot extract the signature from the image that carries it. All these advantages were proved visually and numerically.**

Keywords – Signature, security, robustness, integrity.

INTRODUCTION

The first generation of signature stays hundreds of years at the same procedure. Any person wants to sign certain document he just use his own handwritten signature and write it directly using pencil. Recently, several types of digital signatures appeared and solved the problem of identity proofing and intent integrity. One of these types is using digital images to carry the digital signatures invisibly.

In literature, there are several articles that give a solution to sign digital colored images. In [1], amplitude modulation was used to hide certain information as a digital signature. Certain owner-related numbers were used to identify the owner without visual meaning. Several articles can be seen in literature used similar scenarios. However, most of these proposed ways depend on hiding random numbers or certain numbers with certain information related to the person who writes the signature [2-6].

Other ways of hiding certain random numbers or meaningful numbers in digital gray or colored images depend on transform the image into other domain and used the transformed image to carry the information [7-12]. This scenario is very useful to protect the secret information from violation. But, this scenario adds more computations for the process in comparing with the direct insertion of secret information in digital images [13-19]. The former way is called transform domain insertion and the latter way called spatial domain insertion.

In this work, spatial domain is used. The digital signature is inserted in digital colored images invisibly. The digital image format is changed to another colored format the separate the gray part of the image from the colored parts. The gray part of the image is used to accept the additional information which is the digital signature because it is the richest part of the image that can contain the added part. After implementing this technique and used several types of test images and signatures, good results were achieved and this technique is proved to be successful in carrying out this task.

The remained sections of this article are structured as follows. Section 2 explains the process of insertion the signature in the image and extraction it. In section 3 the implementation of the technique is applied and the results were extracted. In section 4 the conclusions were written and the future work was suggested.

SIGNATURE INSERTION AND EXTRACTION

A. *Signature Insertion.*

The first step in this technique is making a digital signature by writing the signature directly using imagery software or by scanning handwritten signature. After that, the pixels of the signature image are reordered so as to make a new version of it. The resulted new version has pieces of cut lines that are independent and have no connections with each others. This version has no visual meaningful information. This is done to make the digital signature secure enough to be not predictable by any parasitical. Then, the digital colored image, which is the carrier of the signature, is transferred from the original Red, Green, Blue (*RGB*) color format to any color format that separates the gray part and the colored parts like *YIQ*. After that, the gray part of the carrier image is divided into blocks of pixels. These blocks are reordered to raise the degree of security. Then, each pixel contents of the signature image are inserted in certain block of the digital gray part of the carrier image. The gray part now is carrying the signature information. So, the next step is reordering the blocks of the gray part to the original order. Finally, the colored parts are mixed with the gray part to get the final colored image that carrying the signature. This technique is seen in Fig. 1 below.

The RGB represents the digital colored image which will be the carrier of the digital signature. Y represents the gray part of the carrier image. SI represents the signature image. I and Q represent the colored parts of the carrier image. Y_S represents the gray part of the carrier image after its pixels where reordered. SI_S represents the signature image after its pixels where reordered.

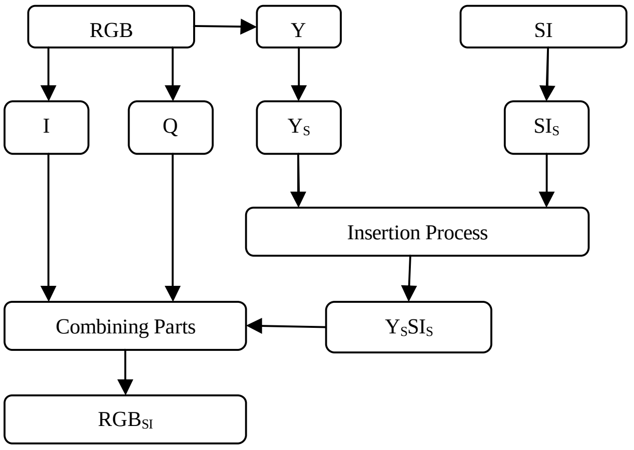

Fig. 1 Block diagram of the proposed Technique.

Y_SS_{IS} represents the gray part after carrying the signature image. RGB_{SI} represents the final version of the carrier colored image after combining the colored parts with the gray part.

The previously mentioned reordering processes for the signature image and the gray part of the digital colored image are similar to the encryption processes that need keys to encrypt and decrypt certain information. The goal of that is to raise the security of the information and prevent any parasitical from predicting, understanding or tampering the information that are secretly inserted in the image.

The insertion process depends on the value of each pixel in the signature image and the values of the pixels in the gray part of the carrier image. If the pixel value in the signature image is zero, the pixel values of the odd rows of the related block in the gray image will change to take the minimum value of those rows. While the pixel values of the even rows will decrease by certain adjustable value. In the contrary, if the pixel value in the signature image is one, the pixel values of the even rows of the related block in the gray image will change to take the maximum value of those rows. While the pixel values of the odd rows will increase by certain adjustable value.

B. *Signature Extraction*

The signature extraction process has the same steps as the steps of the signature insertion process but in reverse order. Namely, the colored carrier image will be separated to gray part and colored parts. The gray part will be encrypted using the same previously used encryption key. The values of the pixels of each block is added and compared with the addition of the same block in the original image. If the addition of the former is greater than the addition of the latter, the resulted pixel value of the signature is one, otherwise it is zero. Finally, the pixels of the resulted signature image will be reordered to get the extracted signature image which represents the legal signature.

C. *Tampering attempts*

The digital colored image that carrying the digital signature may be suffered from certain types of tampering attempts. The goal of the parasitical who try to tamper the digital colored image that contains the digital signature maybe is to know if there is a signature or not, to see the signature, to delete the signature, to change the signature, to take a copy of the signature or to destroy it. This proposed technique is solid enough to robustly withstand against several types of tampering attempts.

IMAGERY AND NUMERICAL RESULTS

Tenths of digital colored images were used as carriers. These images are of different nature and contents. Tenths of different types of digital signatures were used as well. Different image sizes where used for both the carrier colored image and the signature image. The colored images have full pixel resolution that is 24 bit per pixel. The visual results for certain image (IM1) and certain signature (Sig2) that represents the insertion process are seen in Fig. 2 and Fig. 3.

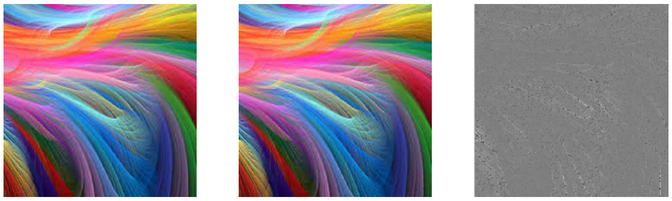
(a) (b) (c)

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

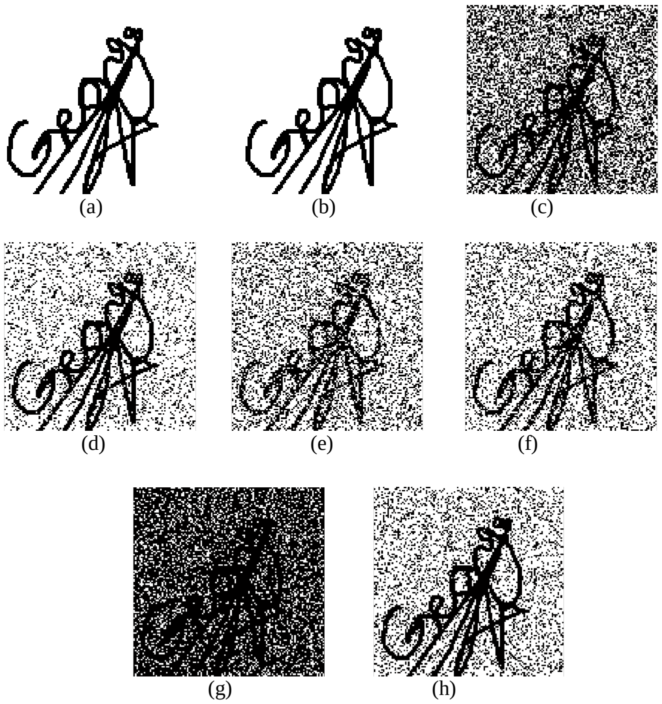

Fig. 3. The Imagery Results for the reconstructed signature for IM1 and Sig1, (a) The original signature Image, (b) The signature Image after reconstruction without any tampering violation, (c) The reconstructed image after facing low pass filtering violation, (d) The reconstructed image after facing median filtering violation, (e) The reconstructed image after facing scale down violation, (f) The reconstructed image after facing JPEG compression violation, (g) The reconstructed image after facing cropping violation, (h) The reconstructed image after facing Rotation violation.

Fig. 2 shows good results for the proposed technique in putting secret signature in digital image. The carrier image that contains the signature remains visually the same likes the original one and no one can differentiate between the two images. Fig. 3 shows the visual results of the reconstructed signature that resulted by the extraction process. The reconstructed signature is fully similar to the original signature without any change. Furthermore, Fig. 3 shows the visual results of the reconstructed signature after the carrier image faced several types of dangerous violets like compression, filtering and cropping. The results show that in spite of facing several violets, the proposed technique ensures the security of the signature to be still existed and could be understood.

Fig. 4 and Fig. 5 show also good results for the proposed technique in putting another secret signature (Sig1) in another digital image (IM2). Using this technique of signature insertion in images, the signature will be secure and robust.

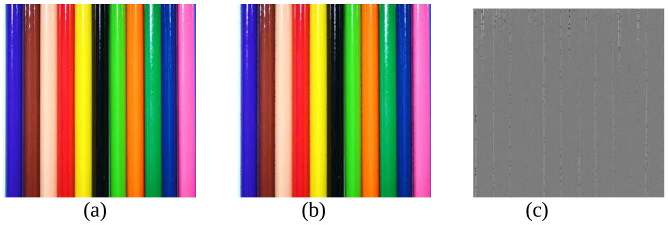

Fig. 4. The Imagery Results for IM2, (a) The original colored Image, (b) The Colored Image Carrying the Signature, (c) The difference Between (a) and (b)

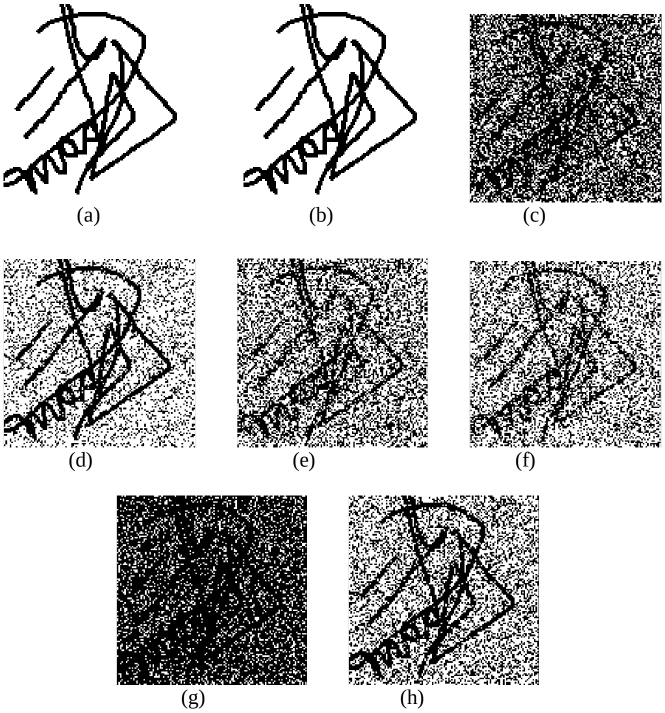

Fig. 5. The Imagery Results for the reconstructed signature for IM2 and Sig2, (a) The original signature Image, (b) The signature Image after reconstruction without any tampering violation, (c) The reconstructed image after facing low pass filtering violation, (d) The reconstructed image after facing median filtering violation, (e) The reconstructed image after facing scale down violation, (f) The reconstructed image after facing JPEG compression violation, (g) The reconstructed image after facing cropping violation, (h) The reconstructed image after facing Rotation violation.

On other hand, the invisibility and quality of the carrier image after signature insertion could be computed numerically. The peak signal to noise ratio (PSNR) is a numerical way of inspection the invisibility and quality of the carrier image [20]. The (PSNR) value for the carrier image is computed using the following equation:

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

Where, MSE is the mean squared error between the carrier image that resulted from carrying the signature and the original coloured image. The average PSNR for 100 different coloured images is 38dB. This large number ensures the invisibility of the signature and the image integrity of noise that may be resulted from the signature insertion process.

In comparing this proposed technique with the amplitude modulation in [1], it is found that this technique is more powerful and large size signature could be used and very large number of bits could be contained. In [1], the digital signature contains 32 bits while in this proposed technique the digital signature contains 16384 bits. This means that much visual meaningful information could be inserted securely in the carrier image.

CONCLUSIONS

Very solid technique is proposed in this work. Digital signature could be inserted in digital colored image which represents the carrier to the secrete information that the signature carries. The inserted signature will be invisible and does not affect the quality of the carrier image. The technique is very robust in respect to sustaining dangerous types of violets. Several types of colored images and several types of signatures were used and with all of them the results were very good. The proof of identity and the integrity of intent using digital signature with visual information were proved through this technique.

REFERENCES

[1] 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.

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

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

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

[5] 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.*

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

[7] 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.

[8] 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.

[9] 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.

[10]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.

[11]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.

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

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

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

[15]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.

[16]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.

[17]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.

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

[19]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.

[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.