International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 5, pp 29-33, May-2022

https://doi.org/10.47001/IRJIET/2022.605003

Digital Secure Signature Using Image Edge Energy

Abdallah Altahan Alnuaimi

Faculty of Information Technology, Isra University, Jordan
Email ID: abdstn@iu.edu.jo

***Abstract* - Digital signature is very important to support electronic business. Hundreds of procedures were proposed regarding digital signatures. One of the most successful procedures is to use digital images to carry secret signature. In this work, a novel digital signature procedure is submitted. It depends on choosing the image color layer with the maximum edge energy to host the digital signature. The results of the experiments prove the success of this procedure and the superiority of it in comparison with several older procedures.**

Keywords: Edge, image, layer, signature.

I. INTRODUCTION

After the invention of computers and computer networks, electronic transactions appeared and the business sector do many operations electronically. The need of proofing the identity is a big challenge in electronic transactions. So, many research articles were submitted in literature to overcome this risk. Most of the procedures submitted depend on different types of encryption techniques. This requires the encryption of the document completely.

Modern techniques are suggested for digital signatures. These techniques suggest using digital images to carry digital signatures secretly. Any digital image that carries digital secret signature could be sent electronically via several types of networks. Thus, there is no need to encrypt the file because the digital signature is inserted invisibly in the image and human visual system cannot detect it.

In [1]-[6], the authors used random numbers or certain user-dependant numbers as a secret signature hidden in the image. Besides the proofing of identity, these numbers may represent useful meaning. But, there is no visual meaning for these types of signatures. In [7]-[10], the authors hide real digital signatures belong to their owners in the digital images. In [11]-[16], the authors convert the digital image to a new transform. Then, they hide the real signature in the image. After that, they convert the image back to its spatial nature.

In [1], the authors used amplitude modulation to insert certain numbers in the image. They insert 32 bits that identify the identity of the user. The author in [9] used 16384 bits to make real digital signature that has a visual meaning as the traditional hand written signature. In this proposed work, the technique used in [9] is modified via the insertion of digital signature in the image color layer that has the maximum edge energy. Since, the edges in any image can accept additional information without affecting the quality of the image. In general, the human visual system cannot detect the additional information in the edges of the image if it is small in size. The following sections are divided as follows. Section two contains the signature hiding process and retrieval process.

Section three contains the experiments and results. Section four contains the conclusions.

II. SIGNATURE HIDING AND RETRIEVAL

Hiding Stage

The digital signature may be acquired using handwritten and then scanned it. Also, any drawing program could be used to do that. This signature is belonged to certain user and represents the identification of him. Also, it contains visual information. To make this signature secure enough, the pixels that represent the signature is reordered to make a new signature without visual meaning. After that, the digital colored image that will carries the signature is split into its three main color layers (R, G & B). The edge energy of the three layers is computed. The color layer that has the maximum edge energy is chosen to carry the secret signature. Before doing the hiding process, the maximum edge energy layer is divided into certain number of blocks. Every block of them will carry the information of one pixel of the signature. The blocks are reordered to make a new version of this layer without visual meaning to add additional security for the technique used. Now, the selected color layer is ready to carry the secret signature. This procedure is very secure. Since, the first reordering process of the signature pixel represents the first secret key. The second reordering process of the colored image represents the second secret key. The third key is represented by the choosing process of the selected color layer. Fig. 1 below represents the hiding process. The colored image represents the original colored image before carrying the secret signature. The R-layer, G-layer and B-layer represent the red color layer, the green color layer and the blue color layer, respectively. The block that contains maximum edge energy criterion represents the process of splitting the colored image into the three main color layers R, G and B.

The reordering blocks represent the process of reordering the signature pixels and the color layer blocks.

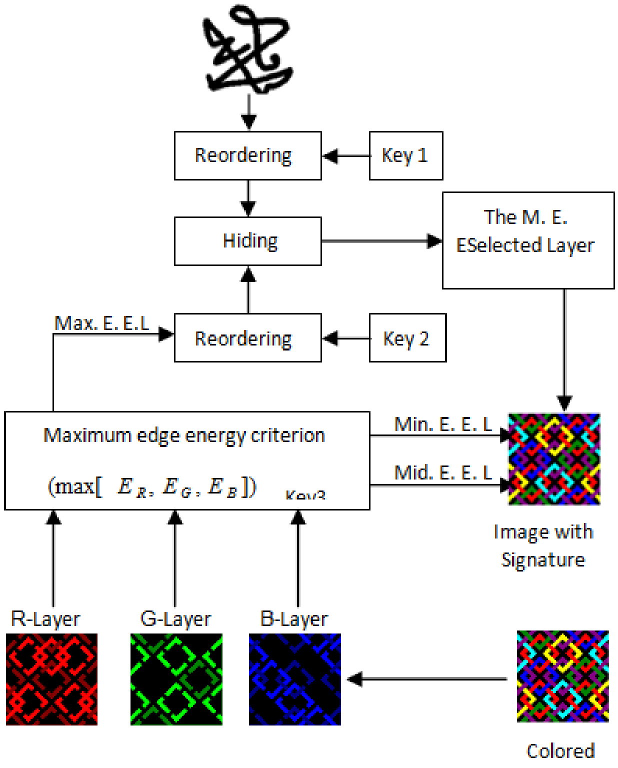

Figure 1: The hiding process

The hiding process takes several steps. First of all, the number of pixels of the signature and the colored image layer are computed. Then, the pixels number of the colored image layer is divided by the pixel number of the signature to get the number of pixels in each layer block that will carry every pixel of the signature. So, every single pixel of the signature is related to individual block of the image layer with certain number of pixels. After that, every image layer block is divided into four quarters and every quarter contains several pixels. Then, the values of each block quarter are changed depending on the value of the signature pixel. If the signature pixel has the value of zero, the pixels values of the related block will be decreased. The pixels values of the first quarter will be changed to take the minimum value in this quarter. Also, the pixels values of the third quarter will be changed to take the minimum value in this quarter. The pixels values of the second and the fourth quarters will be changed by subtracting certain fixed number from each pixel value. On the other hand, if the signature pixel has the value of one, the pixels values of the related block will be increased. The pixels values of the second quarter will be changed to take the maximum value in this quarter. Also, the pixels values of the fourth quarter will be changed to take the maximum value in this quarter. The pixels values of the first and the third quarter will be changed by adding certain fixed number to each pixel value.

Retrieval Stage

The retrieval stage depends on the opposite processes of the hiding stage. Specifically, the colored image that carrying the secret signature is split into its three main layers R, G and B. Then, the previously selected layer with maximum edge energy is taken. Using the second security key the pixels of this layer is reordered. After that, every block of this layer is compared with the related block of the same layer before that does not carry the signature. If the summation of the pixel values of the former block is bigger than the other, the value of the signature pixel is one, otherwise it is zero. Finally, using the first secret key, these pixels reordered to the original case of the signature that has visual meaning.

Attacking operations

This submitted technique is very secure and can overcome most types of attacks. It is not easy for anyone to know that certain colored image carries secret signature. If anyone knows that certain image carrying signature, he needs to know more information to have the ability to know and extract the signature. First of all, he needs to know the procedure of hiding process. Moreover, he needs to know three different keys that are used in this robust technique. The first key which is used to reorders the signature pixels. The second key which is used to reorders the block pixels. The third key which is determines which color layer is used to carry the secret signature. To test this technique, several experiments of attacking were used and the technique overcomes all and stands to be very robust.

III. EXPERIMENTAL RESULTS

Several digital-colored images and several secret signatures were tested using the proposed technique. The colored images used represent different types with different components and details. Also, different types of attacks were used to test the ability of the technique to overcome this risk. The objective of any attack is to detect and extract the secret signature. But, if this is not possible, the attack tries to destroy the signature.

Fig. 2 shows the visual results for the colored image IM1 and the signature SI. Fig. 2 (a) represents the original image before use it to carry the signature. Fig. 2 (b) represents the image after carrying the secret signature. The two images (a) and (b) are the same for the human visual system and no one can differentiate between them. The used signature could be seen in (c).

Fig. 3 shows the visual results for the signature S1 extraction from the image IM1 after several attacks. Fig. 3 (a) represents the extracted signature after the image facing low

ISSN (online): 2581-3048
Volume 6, Issue 5, pp 29-33, May-2022
https://doi.org/10.47001/IRJIET/2022.605003

pass filtering attack. While the parts (b), (c), (d), (e) and (f) represent median filtering, scale down, JPEG compression, cropping and rotation attacks, respectively.

Fig. 4 shows the visual results for the colored image IM2 and the signature S2. Fig. 4 (a) represents the original image before use it to carry the signature. Fig. 4 (b) represents the image after carrying the secret signature. The two images (a) and (b) are the same for the human visual system and no one can differentiate between them. The used signature could be seen in (c).

Fig. 5 shows the visual results for the signature S2 extraction from the image IM2 after several attacks. Fig. 5 (a) represents the extracted signature after the image facing low pass filtering attack. While the parts (b), (c), (d), (e) and (f) represent median filtering, scale down, JPEG compression, cropping and rotation attacks, respectively.

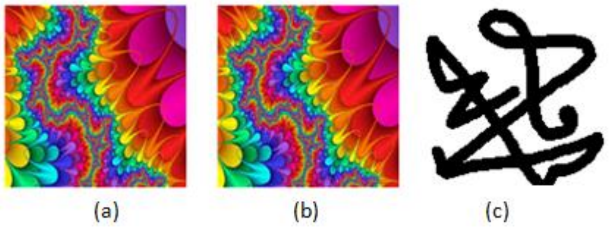

Figure 2: The visual results for image IM1, (a) represents the original-colored image before hiding the signature, (b) represents the image after carrying the signature, and (c) represents the secret signature

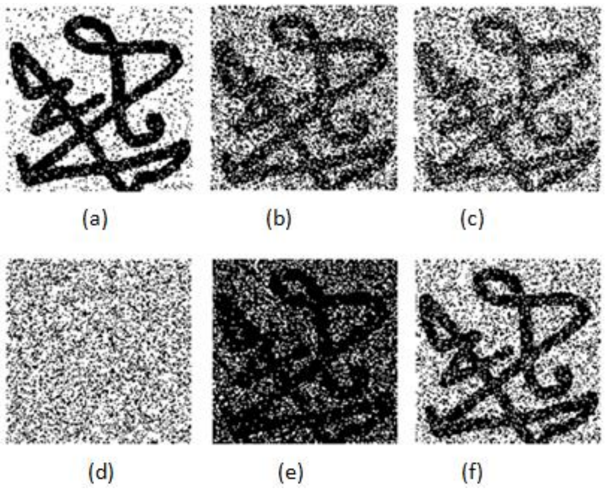

Figure 3: The retrieval visual results for the signature S1 with IM1 after several attacks, (a) low pass filtering attack, (b) median filtering attack, (c) scaling down attack, (d) JPEG attack, (e) cropping attack, (f) rotation attack

The experiments and the visual results give a clear indication for the success of the proposed technique. In usual cases, the extracted signature is the same as the original one. In the cases of facing certain attacks, the extracted signature still clear and represents the user signature. The technique has a big success in facing most of the dangerous attacks except its weakness in facing the JPEQ compression attack. The weak result for the JPEQ compression attack is seen in Fig. 3 (d) and Fig. 5 (d).

Using mathematical equations that can compute certain parameters in comparison between the original image and the same image after carrying the signature will support the visual results. The peak signal to noise ratio (PSNR) is a mathematical parameter that can check quality of the technique by comparing the two mentioned images [17]. The (PSNR) value depends on the value of the mean square error (MSE). The (PSNR) value can be 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 image that carrying the signature and the original image. The average PSNR for 10 images is greater than 35dB.

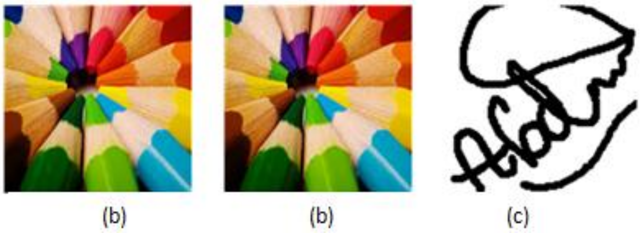

Figure 4: The visual results for image IM2, (a) represents the original-colored image before hiding the signature, (b) represents the image after carrying the signature, and (c) represents the secret signature

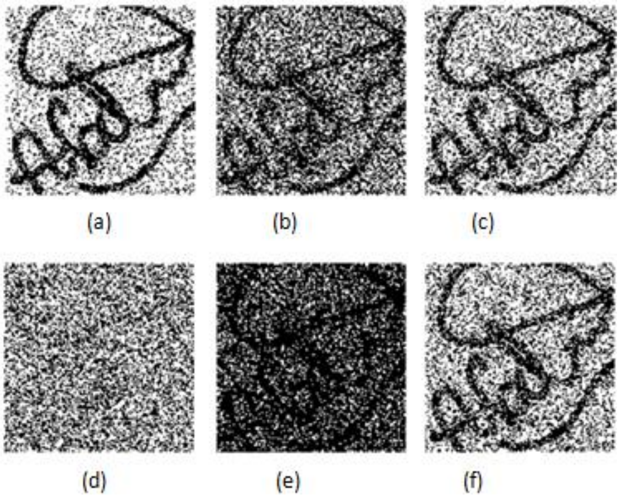

Figure 5: The retrieval visual results for the signature S2 with IM2 after several attacks, (a) low pass filtering attack, (b) median filtering attack, (c) scaling down attack, (d) JPEG attack, (e) cropping attack, (f) rotation attack

This means that, the image that carries the signature is very similar to original one and the signature does not affect the quality of the image.

Moreover, it means that the similarity between the two images is very high and the differentiation between them is not possible.

This technique is compared with that in [1]. In this proposed technique, the signature reaches 16384 bits with the image of 512×512 pixels. While in [1], the signature contains only 32 bits. Also, in the proposed technique, the signature has visual meaning. But, in [1] the signature is just certain numbers.

This technique is also compared with that submitted in [9]. The visual results of extracting the signature after facing several attacks is better in this work except for JPEG compression which better in [9]. Moreover, in both works the signature has a big size with a visual meaning.

IV. CONCLUSION

In this work, a high quality and secure technique for digital signature is proposed. Different colored images were used to carry digital signatures. The experiments that used to test the technique prove the robustness of it in facing several types of strong attacks. The technique is superior in most of the criteria that support the success of digital signatures regarding the security and robustness. The comparison between this technique and others gives it a good rank. The weakness in facing JPEG compression will be treated in future work.

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] A.Al-Tahan Al-Nu'aimi, "Digital secure signature using digital colored images as a communication carrier", *International Journal of Information Technology and Web Engineering*, Dubai, 2015.

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

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

[13] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

Citation of this Article:

Abdallah Altahan Alnuaimi, "Digital Secure Signature Using Image Edge Energy" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 5, pp 29-33, May 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.605003

****