مجلة العلوم البحتة والتطبيقية

Journal of Pure & Applied Sciences

www.Suj.sebhau.edu.ly ISSN 2521-9200

Received 19/04/2019 Revised 19/08/2019 Published online 17/11/2019

The Mechanism of Secure Watermarking based on Encryption and Attached Frame with Image

*Fatma A. Ibrahim[a], Mabroukah A. Amarif[b]

[a]Computer Department, Faculty of Science/Sebha University, Libya

[b]Computer Department, Faculty of Information Technology/Sebha University, Libya

*Corresponding author: fat.ibrahim1@sebhau.edu.ly

Abstract Watermarking is the common techniques that have been used in information security. It's the way of hiding data or information within images in order to protect ownership and copyrights. Nowadays, many companies and enterprise apply watermarking to their products. With the increment and distribution of personal photos and photographs images around the world, the protection of ownership and copyrights becomes inevitable. Many algorithms and techniques have been developed in order to embed the watermark and implement the integrity of it. The simplest one is the LSB (Least significant bits) technique. This technique ensures that the quality of the image will not degrade but it's prone to cropping and scaling attacks. This paper proposes and provides an algorithm that can be used for protecting watermark image from damage or stolen by embedding the watermark into the frame of image instead of image itself. The frame should be invisible so any attack processes will not be able to destroy the watermark. The result shows that the watermark is still the same under cropping and scaling processes. This could really ensure the integrity of personal photo watermarks for a large wide range.

Keywords: Information security, Watermarking, Cryptography, LSB, Image processing.

آلية أمنية العلامة المائية بناءً على التشفير و الاطار الملازم للصورة

*فاطمة علي إبراهيم[1]و مبروكه علي امعرف[2]

[1] قسم علوم الحاسب–كلية العلوم–جامعة سبها، ليبيا

[2] قسم علوم الحاسب–كلية تقنية المعلومات–جامعة سبها، ليبيا

*للمراسلة: fat.ibrahim1@sebhau.edu.ly

الملخص تُعتبر العلامة المائية أحد أهم التقنيات الشائعة المستخدمة في أمن المعلومات. إنها طريقة إخفاء البيانات أو المعلومات داخل الصور لحماية الملكية وحقوق التأليف والنشر. في الوقت الحاضر، تُطبق العديد من الشركات والمؤسسات علامات مائية على منتجاتها. مع زيادة وتوزيع الصور الشخصية والصور الفوتوغرافية في جميع أنحاء العالم، تصبح حماية الملكية وحقوق التأليف والنشر أمراً لا مفر منه. العديد من الخوارزميات والتقنيات تم تطويرها من أجل تضمين العلامة المائية و سلامتها. أبسط احد هذه التقنيات هي تقنية البت الاقل أهمية LSB. تضمن هذه التقنية عدم تدهور جودة الصورة، ولكنها عرضة لهجمات الاقتصاص والتحجيم. هذه الورقة تقترح وتقدم خوارزمية يمكن استخدامها لحماية صورة العلامة المائية من التلف أو السرقة عن طريق تضمين العلامة المائية في إطار الصورة بدلاً من الصورة نفسها. يجب أن يكون الإطار غير مرئي حتى لا تتمكن أي عمليات هجوم من تدمير العلامة المائية. تظهر النتيجة أن العلامة المائية لا تزال كما هي في ظل عمليات الاقتصاص و التحجيم و توسيع نطاقها. يمكن لكل هذا أن يضمن فعلاً سلامة علامات الصور الشخصية على نطاق واسع.

الكلمات المفتاحية: أمنية المعلومات، العلامة المائية، التشفير، LSB، معالجة الصور.

Introduction

Information security is a way for ensuring that the private information is still secure without lost or stolen. The common categories of Information security are Cryptography, and Steganography [1, 2]. Cryptography is the art of secret writing. It is defined as the process of encoding secret information in a way that unreadable by a third party, only the authorized persons can decode and read the message [3,4]. The main aim of cryptography is providing many of security related goals like confidentiality, authentication, integrity, availability and access control [4,5].

In addition, the art of hiding data or the secret information within cover files is related to Steganography. The process of hiding should ensure that no one can change or damage it or even observe it [6,7]. The technique of hiding data inside digital multimedia isoften known as the watermarking and the watermark itself is that hiding data which could be text, date, serial number, logo or any other type of identification marks [8]. In fact, the watermarkis able tobe extracted or disclosed for different purposes such as authentication, owner identification, copyrights, content protection, or any other identification improvement [9,10]. Based on that, A digital watermarking has been defined as a set of bits which are embedded in a data file (as images) to show features such as IPM (Intellectual Property Management) and proof of ownership.

The Watermarking must be used to hide the information in a way that can't be easily extracted by the third party[9]. Watermarking is very closely linked to cryptography if the hiding data or information is encrypted before embedding as a watermark for a second layer of protection[3].

Currently, watermarking techniques work on two domains: spatialandfrequency domains. Spatial domain concerns with embedding of the watermark data value into original image by modifying pixels value using an appropriate algorithm. The most used simpletechniques in spatial domain is LSB (lest significant bits) [6,11,12]. Its works by embedding the watermark bits into the least significant bits of each pixel of original image. This technique is easy to perform and understand. It provides High perceptual transparency and low computational complexity for both embedding and detection of the watermark. This technique ensures that the quality of the image will not degrade[11,13,14].

In the other side, frequency domain, which is also known as transform domain, concerns with embedding the watermark by modifying the coefficients of the converted image using one of the suitable transform methods such as DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) [15,16]. Although the transform domain is more secure and effective than the spatial domain, but it suffers from computational complexity, slow embedding and extraction processes. In fact, using of transform domain methods require more experience and expert skill, hence it's more suitable for medical images [17,18].

Spatial domain methods and algorithm are more easy to use and implement, but theylack of the robustness especially during scaling and cropping image operations [11,13,16,19]. This motivates us to propose and suggest the design of an algorithm that supports the technique of watermarking within classification of the spatial domain using the LSB. The idea of the proposed algorithm is to attach and fit the watermark with the image so no one can remove or change it. This could be extremely worked with personal image protection especially for personal photos and drawing panel. The following section explains the design method of the proposed algorithm and section III describes the analysis. Results and discussion are provided in section IV. The paper is concluded with section V.

II. Algorithm Description

The purpose of this research is to design and develop an algorithm that can be able to embed the watermark into any image edges. These edges are represented as a frame. This process ensures the integrity of image contents from any change or confusion. Based on this concept, the proposed algorithm works by adding frame to original image, then, embed the watermark in this frame, which is represent the image edges. Whatever the process that is performed on it, the image frame is out of that process. The proposed algorithm steps aredescribed in figures 1, 2, 3, and 4 as givenbelow:

Stage1: Watermark Embedding Process

In this stage, the original image is convertedto grayscale image.

Input

The input is the watermark data.

Algorithm

i. Take Watermark and encrypt it by using one of the symmetric key cryptography algorithms. The output of this step is Encrypted watermark.
ii. Add a frame to a grayscale image; the result is a framed image.
iii. Embed Encrypted watermark in the framed image using LSB technique. The output image is Watermarked image.

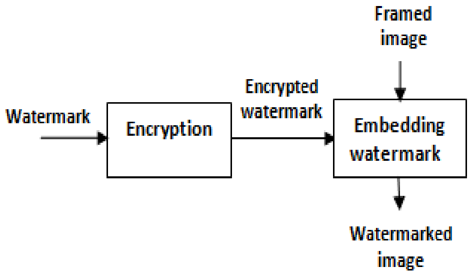


Figure1: Block Diagram of Watermark Embedding Process

Output

Watermarked image.

Stage2: Process of Attacks

In this process, some attacks such as scaling and cropping are performed on a watermarked image in order to consider the effect of these attacks on the integrity of watermarked image and the encrypt watermark. Figure2 showsthe inputs and outputs of this process.

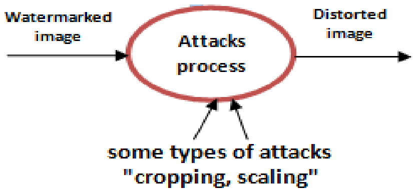


Figure2: Block Diagram of attacking process

Stage3: Watermark Extraction Process

Input

The input to this stage is the distorted image.

Algorithm

i. Extract encrypted watermark and separate it from the watermarked image using LSB technique. Output of this step is both extracted image and encrypted watermark.
ii. Decrypt encrypted watermark using the sameencryption algorithm. The output of this step should be an extracted watermark and image.

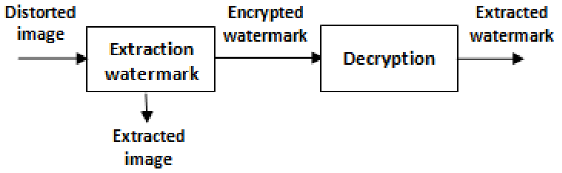


Figure3: Block Diagram of Watermark Extraction Process

Output

Extracted image – an image recovered from the watermarked image.

Extracted watermark – a watermark recovered from the watermarked image.

Stage4: Evaluation Process

In this stage, the comparison between each of extracted image and original image, as well as the comparison between the extracted watermark and the watermark are performed using performance measures [20] as shown in Figure 4:

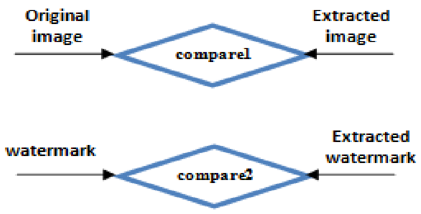


Figure4: Block Diagram of Evaluation Process

The PSNR and the MSE is calculated according to the values of the given original image and extracted image. The descriptions of these two measurements are given below:

- **Peak Signal to Noise Ratio (PSNR):**it is used to measure the similarity between two images, as well as to test the image quality of a watermarked image, it is also used to compare the original watermark and extracted watermark. The equation is:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\max^2}{\mathrm{MSE}}\right)$$

Where max = 255 in grayscale image

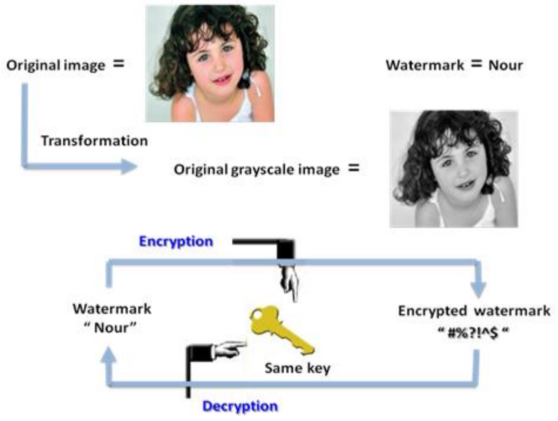
- **Mean Square Error (MSE):**it's used to find similarity between original image and watermarked image andthe equation is:

$$\mathrm{MSE} = \frac{1}{mn}\left(\sum_{i}^{m}\sum_{j}^{n}[\,(W(i,j) - O(i,j)\,]^2\right)$$

Where m,n = size of original image
W(i,j) = pixel values in watermarked image
O(i,j) = pixel values in original image

III. Analysis and results

The developed algorithm has been applied to the personal and photographic image to explain and measurethe algorithm performance using metrics PSNR, MSE. Figure 5 describes the algorithm steps according to the given image.



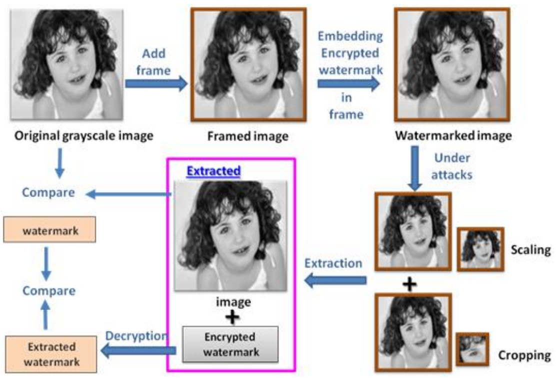


Figure5:Work the proposed algorithm

In this section, we use the data "Nour" as a watermark. We have applied both the image and watermark to the developed algorithm. The embedding image is in the original grayscale image with file of extension jpg (Nour.jpg) and the size is 56x56.

According to the proposed algorithm, the watermark characters are converted into its binary format 01001110, 01101111, 01110101, 01110010, and then the grayscale image are converted into binary format. Each byte from the watermark will be embedded in 2 pixels only, in the 4-bits at less significant bit in the grayscale image. Based on the proposed algorithm, it needs to add frame for grayscale image to embed the watermark in the frame. We use frame size of (4x56), and calculate PSNR to test image quality. According to our calculation, the PSNR is 14.8129. If the watermarked image is cropped or scaled, the frame is still the same because it's out of the image domain. The frame should be invisible so no one can attack or destroyed. This feature is included in the algorithm by excluding the image frame outside of the image array size. The result shows that it's difficult to attack the image frame. It's also improves the integrity of watermarking during the cropping and scaling attacks to the watermarked image.

IV. Discussion and Conclusion

We have designed and developed an algorithm which adopts the feature of attached frame in order to protect the watermark from changed or stolen. A case study of personal photo image with size of 56x56has been applied to the algorithm. We have justified that our proposed algorithm works better if the watermark have been embedded in the image frame.

It has been observed that the biggest image is better than small one to fit the watermark to the attacked image. Actually, the designed algorithm is able to embed the watermark around the given image as possible if the given image size is applicable. This algorithm could protect the watermark of personal photos images. It also determine whether the photographs images has been changed or not during scaling and cropping operations.

REFERECE

[1]- W. Stallings, *"Cryptography and Network Security: Principles and Practices"*, 5th, Upper

Saddle River, NJ: Prentice Hall, ISBN:978-0-13-609704 -4, 2006.

[2]- Hardikkumar V.Desai (B.Sc., MCA), *"Steganography, Cryptography, Watermarking: A Comparative Study"*, Journal of Global Research in Computer Science, Volume 3, No. 12, ISSN: 2229-371X, December 2012.

[3]- S.M.Mousavi, A.Naghsh, S. A. R. Abu-Bakar, *"Watermarking Techniques used in Medical Images: a Survey"*, Society for Imaging Informatics in Medicine, 29 May 2014.

[4]- G. Yadav, A. Majare, *"A Comparative Study of Performance Analysis of Various Encryption Algorithms"*, International Conference On Emanations in Modern Technology and Engineering, ISSN:2321-8169, Vol.5, Issue 3, 70 - 73, March 2017.

[5]- A. J.Amalraj, J. J. R. Jose, *"A Survey Paper On Cryptography Techniques"*, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, pg. 55-59, August-2016.

[6]- A. N. Senarathne, K. De Zoysa, *"ILSB: Indexing with Least Significant Bit Algorithm for Effective Data Hiding"*, International Journal of Computer Applications, Volume 161 – No 5, (0975 – 8887), March 2017.

[7]- S. Almuhammadi, A. Al-Shaaby, *"A Survey on Recent Approaches Combining Cryptography and Steganography"*, Sixth International Conference on Information Technology Convergence and Services, pp. 63– 74, February 2017.

[8]- M.Manivannan, G.Suseendran, *"A Review of Watermarking Requirements, Techniques, Documents, Human Perception and Applications for Medical Images"*, International Journal of Innovative Research in Applied Sciences and Engineering, Vol. 1, Issue 2, ISSN: 2456-8910, August 2017.

[9]- S. Kumar, T. P. Singh, *"A Review of Digital Watermarking, Applications and its Techniques"*, International Journal of Computer & Organization Trends, Vol.4 Issue 4, July to August 2014.

[10]- O P Singh et al, *"Study of Watermarking Techniques Used in Digital Image"*, International Journal of Scientific and Research Publications, Vol. 2, Issue 10, ISSN 2250-3153, October 2012.

[11]- N. Tiwari, Sharmila, *"Digital Watermarking Applications, Parameter Measures and Techniques"*, International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017.

[12]- P. Gaur, N. Manglani, *"Image Watermarking Using LSB Technique"*, International Journal of Engineering Research and General Science, Vol.3, Issue 3, May-June, 2015.

[13]- P. Parashar, R.k. Singh, *"A survey: Digital Image Watermarking Techniques"*, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.7, No.6, pp. 111-124, 2014.

[14]- M. Patel, P.S. Sajja, R. K. Sheth, *"Analysis and Survey of Digital Watermarking Techniques"*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue10, ISSN: 2277 128X, October 2013.

[15]- N.Mahajan, C.Marwaha, Sonam, *"Review on the various Watermarking Techniques Based on Medical Images"*, International Journal Of Engineering And Computer Science, Vol.6 Issue 4, ISSN:2319-7242, Page No. 21165-21170, April 2017.

[16]- G.Cetinel, L.Cerkezi, *"Wavelet Based Medical Image Watermarking Scheme for Patient Information Authenticity"*, International Journal of Applied Mathematics, Electronics and Computers, Page NO. 220–223, ISSN: 2147-8228,2016.

[17]- Balamurugan.G, K.B.Jayarraman, Arulalan.V, *"A Survey on Medical Image Watermarking Techniques"*, International Journal of Computer Science and Network, Vol.3, Issue 5, ISSN: 2277-5420, October 2014.

[18]- Kavitha K J, Reshma M, *"Survey on Digital Watermarking on Medical Images"*, International Journal of Advanced Computer Research, Vol.3 Number4 Issue-13, ISSN: 2277-7970 December 2013.

[19]- Bal, S.N., et al, *"On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching"*, Journal of King Saud University– Computer and Information Sciences, 13 April 2018.

[20]- P. Dabas, K. Khanna, *"A Study on Spatial and Transform Domain Watermarking Techniques"*, International Journal of Computer Application, Vol.71, No.14, (0975 – 8887), May 2013.

[21]- A. Bamatraf et al, *"Digital Watermarking Algorithm Using LSB"*, International Conference on Computer Applications and Industrial Electronics, December 5-7, 2010, Kuala Lumpur, Malaysia.

[22]- C. Deepak Naidu et al, *"Crystography Based Medical Image Security with LSB-BLOWFISH Algorithms"*, ARPN Journal of Engineering and Applied Sciences, VOL. 9, NO. 8, ISSN 1819-6608, August 2014.

[23]- M. M. Emam, A. A. Aly, F. A. Omara, *"An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection"*, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3, 2016.

[24]- P. Singh, R S Chadha, *"A Survey of Digital Watermarking Techniques, Applications and attacks"*, International Journal of Engineering and Innovative Technology, Vol. 2, Issue 9, ISSN: 2277-3754, March 2013.