International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: http://doi.org/10.31695/IJERAT.2018.3352

E-ISSN : 2454-6135

Volume.4, Issue 12
December -2018

Image Authentication Subject Review

Khalid Kadhim Jabbar

Mustansiriyah University

Computer Science Department

Baghdad – Iraq

ABSTRACT

Image authentication is the process of proving image identity and authenticity by embedding a secure data in the secure way called embedding process. In embedding, an algorithm is used to combine watermark (binary) and host data (original image), the watermark bits are embedded into the original data under transform domain or transform domain to produce the watermarked signal(data). To protect the authenticity of an image, several approaches have been proposed. Nowadays image authentication techniques have recently gained great attention due to its importance of multimedia applications.

Key Words: *Authentication, Identity, Transform domain.*

1. INTRODUCTION

The massive distribution and development of digital multimedia and with the aid of image processing software, which is easily available in the modern day market, make editing and inappropriate distribution of digital content a problem. Consequently providers of intellectual property are naturally concerned with intellectual rights. Therefore watermarking and cryptographic systems have been developed for those issues [1]. Digital Image Watermarking is used for copyright protection of digital information. With the widespread of internet, the intellectual properties are accessible and manipulated easily. It demanded to have different ways to protect data. Digital watermarking provides a viable and promising solution. In this paper, we have described about the three different watermarking techniques (LSB, DCT, DWT) along with the various performance parameters required to evaluate the best technique out of them. This can help us to propose and implement new technique to achieve maximum robustness against various attacks. The watermarking schemes can be broadly classified into three types [2]: robust watermark, fragile watermark and semi-fragile watermark. Robust watermark is generally used for copyright protection and ownership verification since it is robust to nearly all kinds of image processing operations such as lossy compression, spatial filtering and geometric distortions [3]. Fragile watermark is mainly applied to content authentication since it is easy to be destroyed by any manipulation [4]. Between these two extremes lies what is called semi-fragile watermarking. It could tolerate acceptable modifications to the watermarked image whilst it is sensitive to all other malicious manipulations and capable of localizing tampered regions [5]. Image watermarking methods can be grouped into spatial domain methods and transform domain methods. In spatial domain, we embed the watermark by directly modifying the pixel values of the original image. In transform domain, a transformation is first applied to the original image and then embedding the watermark into transform coefficient. There are three main transform methods generally used, i.e. Discrete Cosine Transform (DCT), Wavelet Transform (DWT), and Fourier Transform (DFT). Embedding the watermark into the transform-domain can increase the robustness, when the watermarked image is tested after having been subjected to common image processing [6].

2. AUTHENTICATION REQUIREMENTS

1. Sensitivity: The authentication system must be able to detect any content modification or manipulation. For any authentication algorithms, detection of any manipulation is required and not only content modification.
2. Robustness: The authentication system must tolerate content preserving manipulations.
3. Localization: The authentication system must be able to locate the image regions that have been altered.
4. Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered.
5. Security: The authentication system must have the capacity to protect the authentication data against any falsification attempts.

3. IMAGE AUTHENTICATION TECHNIQUES

Digital watermarking is the art and science of embedding copyright information in the files; the information which is embedded in files is called watermarks. Digital watermark is one of the signals which are added to a document to authenticate it and to prove the ownership. Two approaches for watermarking data authentication are possible fragile watermarking and robust watermarking.

❖ **Advantages of watermarking**

- Uniquely identify the author of copyright work.
- Implementation on pc platform is possible.
- Embedding watermarks is easy.
- Image tampering detection.

❖ Disadvantages of watermarking

- Doesn't prevent image copying.
- Watermark vanishes if someone manipulates the image.
- Resizing, compressing images from one file type to another may diminish the watermark and it becomes unreadable [7]. The major techniques for authenticating an image are as follows:

- Image authentication based spatial domain.
- Image authentication based frequency domain.

3.1 Watermarking based spatial domain

Least Significant Bit LSB [8] is a spatial domain technique which is a very simple and straight forward. It takes less time to embed image (watermark).The watermark is embed into the least significant bits of the original image. This technique has many drawbacks, even simple attacks can remove or destroy watermark but sometime it may survive against some of the transformations. Various improvements on LSB substitution has also been proposed in recent times like embed watermark at single bit rate, multi bit rate or using a pseudo-random number generator. Pixel can also be selected with help of key. Any addition of noise [9] and performing lossy compression can easily degrade the image quality or remove or destroy or disrupt watermark. It lacks the basic robustness. In case, if the algorithm is discovered, it becomes easy for attacker to change or remove watermark, the following figure illustrate this technique:

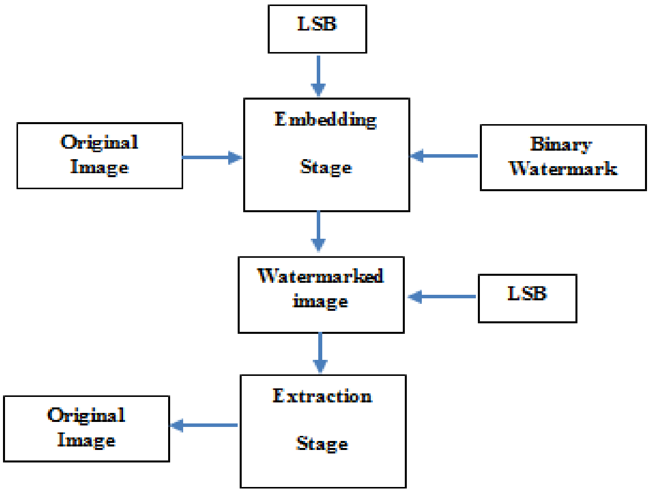


Figure 1: Image Authentication Under Spatial Domain

DOI : 10.31695/IJERAT.2018.3352

3.2 Watermarking based frequency domain

Transforming the signal from spatial to frequency domain is more appropriate for watermarking because of its following properties.

A. Statistical independence between pixels is obtained.

B. Inverse transformation evenly spreads the watermark over host image giving tough times to attackers.

C. it takes the Humane Visual System (HVS) into consideration.

D. Watermark can be embedded into significant area of host image, thus providing robustness against several attacks.

E. Cropping a serious threat to spatial domain hardly impacts in transformation domain.

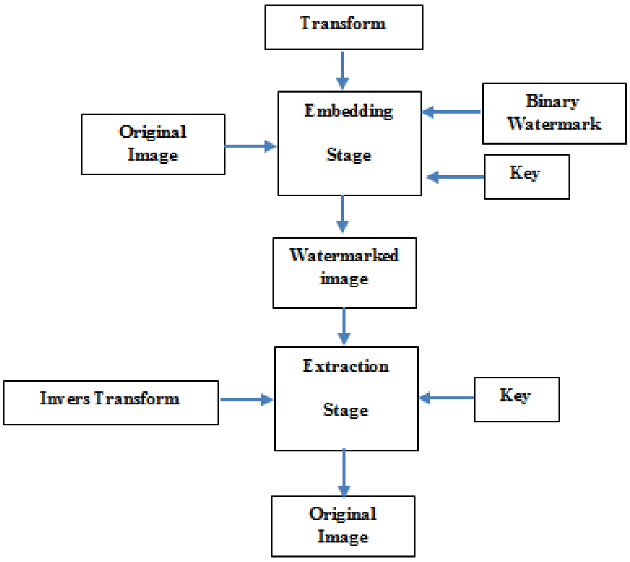


Figure 2: Image Authentication Under Transform Domain

3.2.1 Discrete Cosine Transformation (DCT)

DCT [10] is a very popular transform domain watermarking technique. In this technique, an image is divided into different frequency band as low (FL), medium (FM) and high (FH). It allows selecting the band to embed data or watermark into the image. Figure 2 represents Discrete Cosine Transform Frequency 8X8 block, where low frequency band FL appears at upper left corner, if modification performed here, the watermark can be caught by human eyes. High frequency band FH lies at lower and right edges, if modification performed here, it may lead to local distortion along with edges. Medium frequency band FM is considered best region for modification, it cannot affect the image quality. Thus, a middle frequency band is the best band to embed watermark. DCT is a faster technique [11], with complexity O (n log n). This technique can survive attacks like compression, noising, sharpening and filtering. This technique is considered to be better than spatial domain watermarking technique. The following steps involved in any technique which is based on DCT are as follows [12].

1. Divide the entire image into 8x8 sized non-overlapping blocks, see fig 3.

2. Take the DCT of each block of size 8x8.

3. Apply a block selection criteria based on the knowledge of Human Visual System (HVS).

4. Use some coefficient selection criteria for embedding.

5. Embed the watermark by modifying the selected coefficients.

6. Take the inverse DCT of each block.

DOI : 10.31695/IJERAT.2018.3352

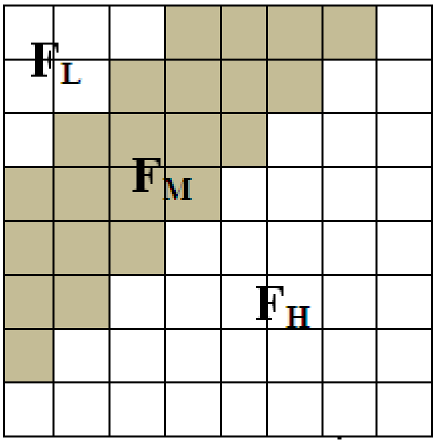


Figure 3: Discrete Cosine Transform Frequency 8X8 block

3.2.2 Discrete Wavelet Transformation

The basic concept behind DWT is that of wavelets. Wavelets are small waveforms with an average value of zero which can start and stop at any point on the axis where we wish. Wavelet analysis breaks the original signal into shifted and scaled versions. It has been found that any image formed on the retina of eye splits into separate frequency bands. Each band of frequency is then separately processed by the Human Visual System. Similarly multi-resolution decomposition of an image by DWT divides the image into separate frequency bands of approximately equal bandwidth. Hence the independent processing of these bands by DWT makes the process of imperceptible marking very effective. DWT applied on an image divides it into four sub-images, 1 approximation component and 3 detail components. The approximation component as LL and detail components as LH, HL, and HH. LL contains the information about low frequency components of an image like smooth areas, while HH component contains high frequency parts of an image like sharp edges. LH and HL bands contain intermediate frequency bands of an image. LL band can be further decomposed to get the next level wavelet coefficients and the process of decomposition continues till the desired fine details about the image are obtained [14], the following figure shows two levels decomposition under DWT domain:.

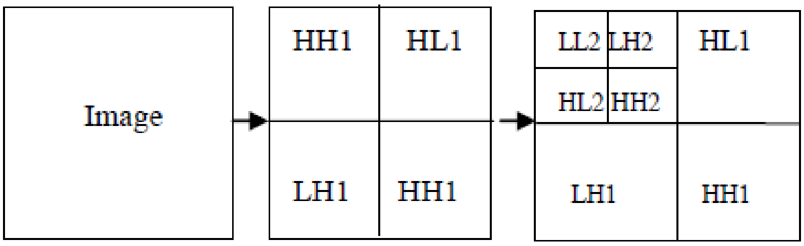
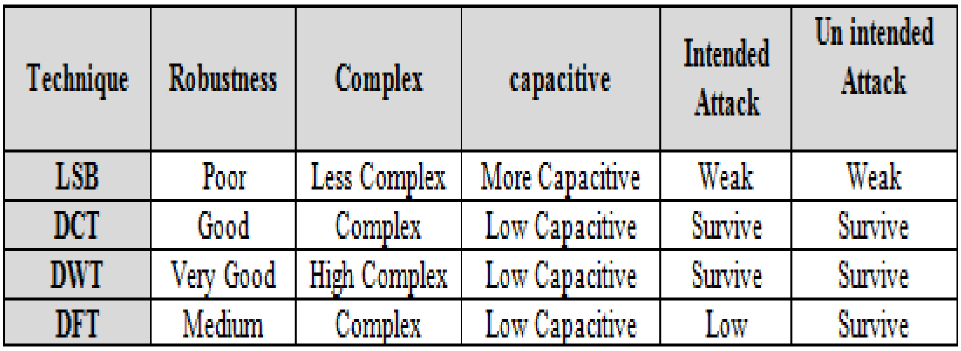


Figure 4: 2-level decomposition of an image by DWT

3.2.3 Discrete Fourier Transform (DFT)

The Fourier transform provides a representation of functions defined over an infinite interval and having no particular periodicity, in terms of a superposition of sinusoidal functions. The DFT of a function provides a quantitative picture of the frequency content in terms of magnitude and phase. Furthermore, □it is robust against various geometric attacks like rotation, translation, cropping and so on. Scaling of a signal in spatial domain causes inverse scaling in Fourier domain. It means as spatial scale expands, the frequency scale contracts and amplitude increases to keep area constant [13]. After a simple review of the set of techniques commonly used in the field of image authentication, we need to compare the techniques above between of them. The following table illustrates the comparison between the commonly techniques that used in the field of image authentication:

Table 1: Compare Between the Common Techniques



Technique	Robustness	Complex	capacitive	Intended Attack	Un intended Attack
LSB	Poor	Less Complex	More Capacitive	Weak	Weak
DCT	Good	Complex	Low Capacitive	Survive	Survive
DWT	Very Good	High Complex	Low Capacitive	Survive	Survive
DFT	Medium	Complex	Low Capacitive	Low	Survive

4.CONCLUSION

In this paper, the major image authentication techniques discussed. Spatial domain techniques apply directly on the original image by manipulating the pixel value during the embedding process based on LSB technique, and it was found with this type of image authentication technique is less complex, easy to implement, more capacitive and it has poor robustness, it can be easily attached with intended or unintended attack. Furthermore, the watermark can be removed or destroyed easily by applying common mild processing operations like data compression, copy past, transmission, rotate, and resize. Characteristics of human perception are not taken into consideration. While the transform technique are more efficient than spatial domain technique, it was found that the frequency domain more robustness with embedding process than spatial domain, the watermarked image has good objective and subjective characteristics such as: the hiding watermark bits is invisible, the watermarked image robustness for some type of intended attack (compression, copy past, and transmission), it has ability to survive the watermarked image during intended attack. Furthermore, the tampered image based on frequency domain has ability to localize the tampering area(s). On the other hand, it can be found that Wavelet Transformation is better for embedding process as compared with DCT or DFT transformation because of its efficient multi-resolution decomposition and Human Visual System (HVS) characteristics of DWT, between intended attack and unintended attack, and it provides selective authentication. The watermarked image that produced under transform domain is imperceptibility and robustness of watermarked digital images rather than the watermarked image that produced under spatial domain, while the technique that implanted in spatial domain is simple, need few requirements, but frequency domain technique has more computational requirements, and some type is so complex.

ACKNOWLEDGMENTS

The Authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Bagdad-Iraq for its support in the present work.

REFERENCES

[1] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, “Perceptual Watermarks for Digital Images and Video”, Proceeding of the IEEE, vol. 87, no. 7, pp.1108-1126, July 1999.

[2] C. K. Ho and C. T. Li. “Semi-Fragile Watermarking Scheme for Authentication of JPEG Images”, International Conference on Information Technology: Coding and Computing (ITCC 04), vol. 1 pp.7-11, 2004.

[3] M. Barni, F. Bartolini, V. Cappellini and A. Piva, “A DCT-Domain System for Robust Image Watermarking”, Signal Processing, 63(3), pp.357-372, 1998.

[4] P. W. Wong and N. Memon, “Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification”, Image Processing IEEE Transactions, 10(10), pp. 1593-1601, 2001.

[5] X. Q. Li and X. Y. Xue, “Fragile Authentication Watermark Combined with Image Feature and Public Key Cryptography”, 7th International Conference on Software Process (ICSP 04), Aug, pp.2286-2289, 2004.

[6] Rinaldi M., Bambang R., Sarwono S., and Wiseto P.,"An Asymmetric Watermarking Method in the DCT Domain Based on RC4-Permutation and Chaotic Map",Telekomunikasi Indonesia, Jl. Gegerkalong, Bandung, Indonesia, 2010.

DOI : 10.31695/IJERAT.2018.3352

[7] S.Jothimani1, P.Betty2," A Survey on Image Authentication Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 4- Jan 2014.

[8] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[9] J. L., Dugelay, S. Roche, C. Rey, G. Doërr, "Still- image watermarking robust to local geometric distortions," IEEE Trans. on Image Proc., vol. 15, no. 9, pp. 2831-2842, 2006

[10] M. Bami, F. Bartolini, V. Cappellini, A. Piva., "A DCT Domain System for Robust Image Watermarking", Signal Processing, Issue 3, Vol. 66, pp. 357-372, 1999.

[11] J.R. Hemandez, M. Amado, "DCT domain watermarking techniques for still images as detector performance analysis and a new structure," in IEEE Transactions on Image Processing, vol. 9, pp. 55-68, 2000.

[12] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, , "Secure spread spectrum watermarking for multi-media," IEEE Trans. on Image Processing 6, 1673-1687, 1997.

[13] K.F. Riley, M.P. Hobson and S. J. Bence, Mathematical Methods for Physics and Engineering, Third Edition Cambridge University Press, 2006.

[14] Shahid Bashir Dar1, Aasif Bashir Dar2," Watermarking in Frequency Domain A Review", International Journal Of Engineering And Computer Science ISSN: 2319-7242, volume 3 Issue 11 November, Page No. 9215-9218, 2014.

DOI : 10.31695/IJERAT.2018.3352