ISSN (Online): 2230-7893
www.IJCEM.org

Image Authentication Scheme using Digital Signature and Digital Watermarking

Seyed Mohammad Mousavi

Industrial Management Institute, Tehran, Iran

Abstract

Usual digital signature schemes for image authentication encode the signature in a file separate from the original image, so this process require extra bandwidth to transmit it. Meantime, watermarking is an information hiding sub-discipline that embeds some information into host image. In this paper a joined digital signature and digital watermarking scheme for image authentication is proposed which is based on signature generation method purposed by [4] and combined DWT-DCT watermark embedding procedure [3]. The scheme extracts signature from the original image and embeds them back into the image as watermark which leads to avoiding additional signature file.

Keywords: *Image Authentication, Watermark, DWT, DCT, Digital Signature, watermarking.*

1. Introduction

People have been always tried to develop innovative methods for secret communication, and today's rapid growth of networked multimedia systems has created one urgent need to protect digital information against illegal duplication and manipulation. In order to be successful, we should use the security systems such as cryptography and information hiding methods.

There are three techniques which are interlinked; steganography, watermarking and cryptography as it has been shown in figure 1 presented by [6].

1.1 Digital Signature

Digital signature which is some sort of cryptographic is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. They also act as checksums which are depended on the time period during which they were produced [1].

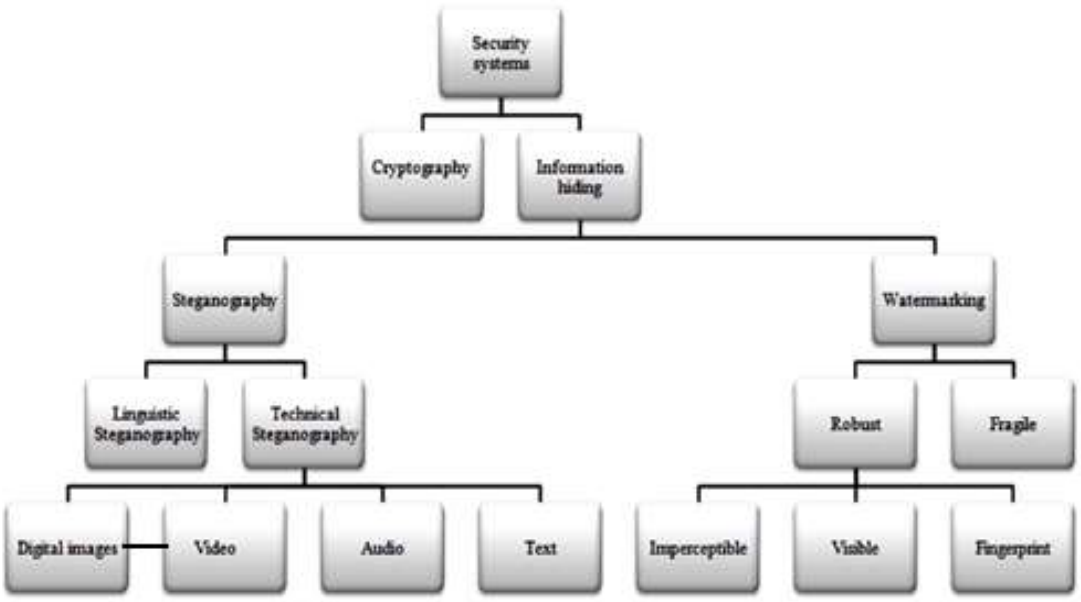

Fig 1. The different embodiment disciplines of security systems [6].

1.2 Watermarking

Digital watermarking is the process of embedding information, call digital signature or watermarking, into a digital signal in a way that is difficult to remove. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks, digital watermarks are only perceptible under certain conditions.

To find the balance among the aspects such as robustness to various attacks, security and invisibility is the main point of digital watermarking. A watermark is a hidden signal added to images that can be detected or extracted later to make some verification about the host image [2].There are different sorts of watermarking as shown in figure 2.

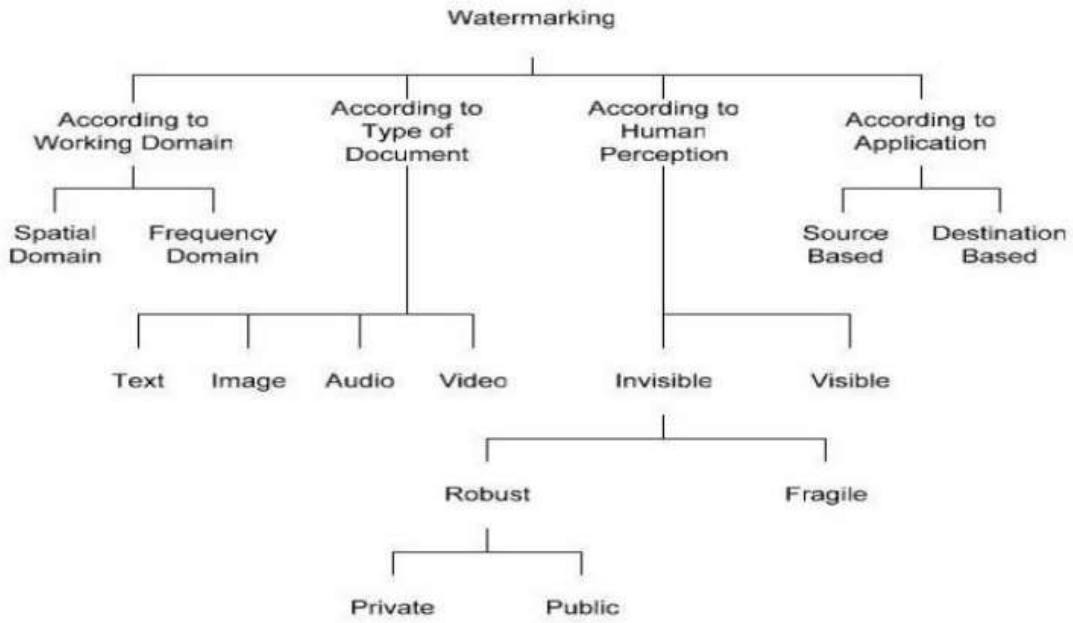

Fig 2. Different sorts of watermarking studies.

As it has been explained by [3], the compression, filtering, rotation, scaling, cropping, collusion attacks among many other digital signal processing operations are common image manipulations, where a digital watermarking method should be effective enough to be undetectable and robust to them. Some watermarking attacks are mentioned in the figure blow.

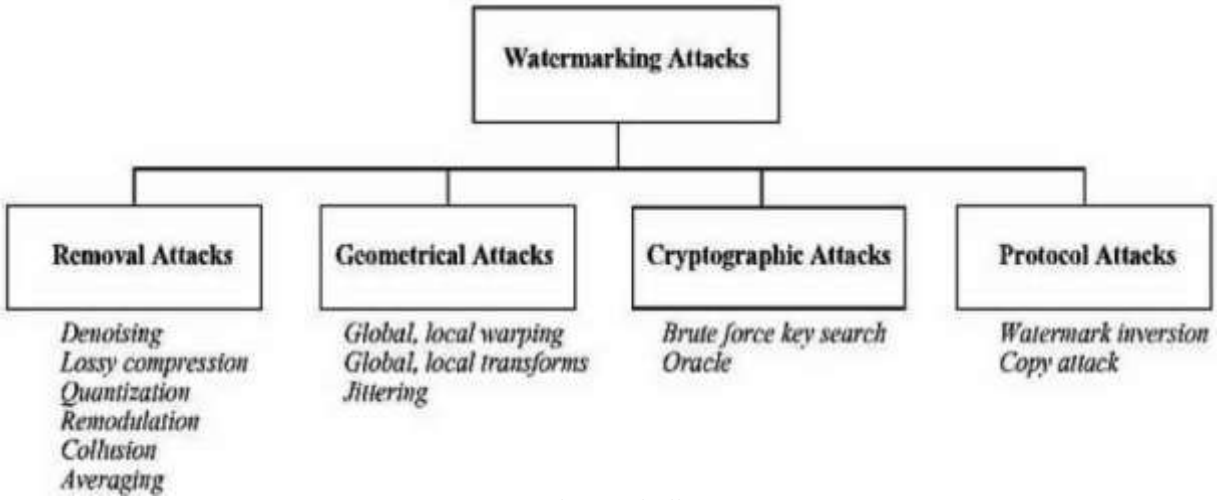

Fig 3. The classification of different watermarking attacks

ISSN (Online): 2230-7893
www.IJCEM.org

2. The proposed scheme

2.1 Digital Signature Generation

The signature generation method purposed by [4], the content dependent robust bits are extracted from the original image. In this method an image is divided into blocks of 16x16 pixels (for large images, larger size could be used). A secret key ***K*** (a number uniquely associated with an author, movie distributor, or a digital camera) is used to generate ***N*** random matrices with entries uniformly distributed in the interval [0, 1]. Then, a low-pass filter is repeatedly applied to each random matrix to obtain ***N*** random smooth patterns. After subtracting the mean from each pattern considering the block and the pattern as vectors, the image block ***B*** is projected on each pattern $\boldsymbol{P_i}$, $1 \leq \boldsymbol{i} \leq \boldsymbol{N}$ and its absolute value is compared with a threshold *Th* to obtain ***N*** bits b_i *:*

$$b_i = \begin{cases} 0, \text{If } |B.pi| < Th \\ 1, \text{If } |B.pi| \geq Th \end{cases}$$

The projections do not depend on the mean gray value of the block and only depend on the variations in the block itself because of patterns $\boldsymbol{P_i}$ have zero mean. The distribution of the projections is image dependent and should be adjusted accordingly so that approximately half of the bits b_i are zeros and half are ones. This will guarantee the highest information content of the extracted N-tuple. This adaptive choice of the threshold becomes important for those image operations that significantly change the distribution of projections, such as contrast adjustment. Experiments in [4] showed that these extracted bits are robust to some image processing operations. In this paper these bits considered content dependent digital signature and will be embed back into the original image as watermark.

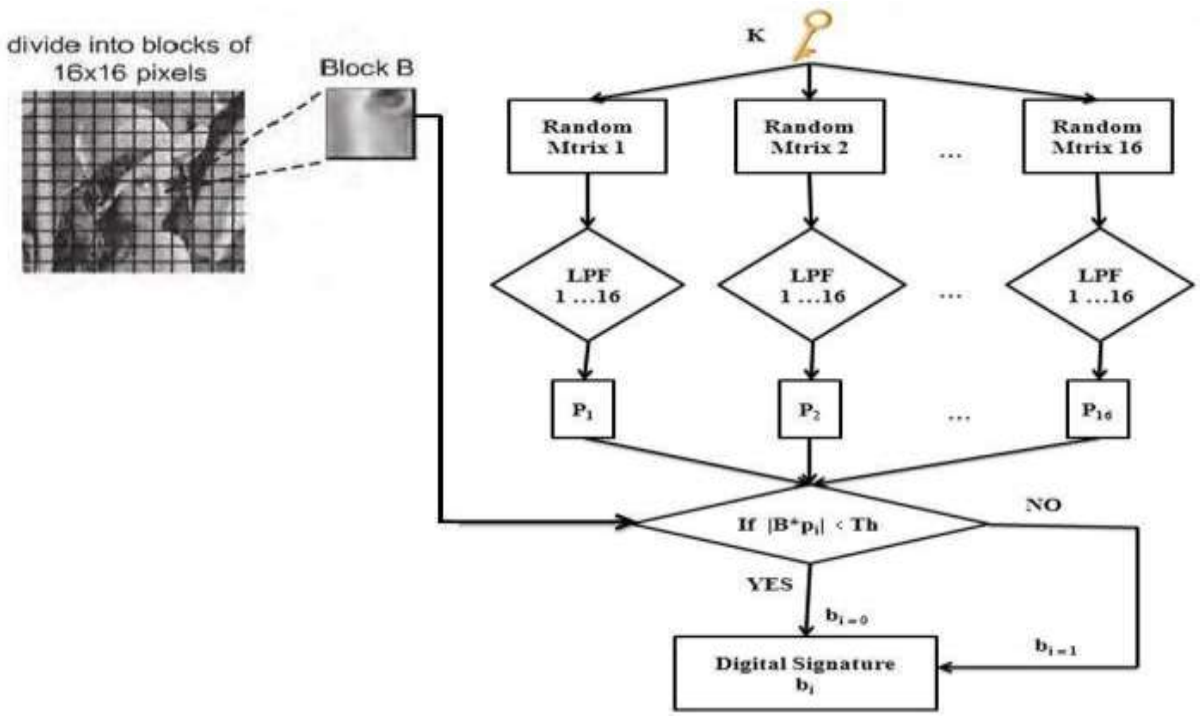

Fig 4. Digital Signature generation

2.2 Digital Watermark Insertion and Detection

There are many watermark insertion and detection algorithms in the literatures. The foremost requirement of image authentication is blind detection. Blind detection means watermark must be extracted from the watermarked image without referring to the original one. Also, the watermark can be neither too robust to be insensitive to content modification, nor to fragile to be easily corrupted bye reasonable compression[7]. In this procedure a frequency domain method is used [5] which is based on the joint DWT-DCT scheme.

The watermark which is our extracted digital signature is scrambled by Arnold cat map and embedded in certain coefficient sets of a 3-level DWT transformed of a host image. Then, DCT transform of each selected DWT sub-band is computed and the PN-sequences of the watermark bits are embedded in the middle frequencies coefficients of the corresponding DCT block.

ISSN (Online): 2230-7893
www.IJCEM.org

In extraction procedure, the watermarked image, which maybe attacked, is pre-filtered by combination of sharpening and Laplacian of Gaussian filters to increase distinction between host image and watermark information. Subsequently, the same procedures as the embedding process is used to extract the DCT middle frequencies of each sub-band. Finally, correlation between mid-band coefficients and PN-sequences is calculated to determine watermarked bits. More details can be found in [5].

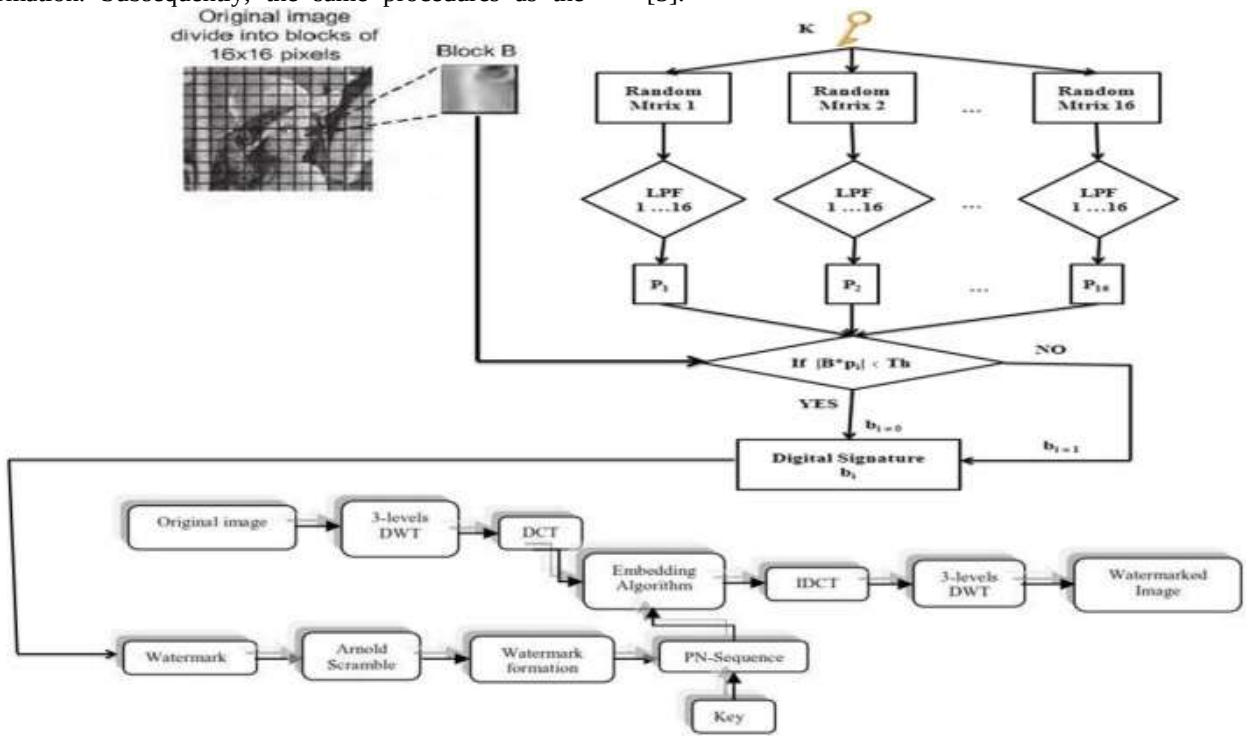

Fig 5. The proposed watermark embedding procedure.

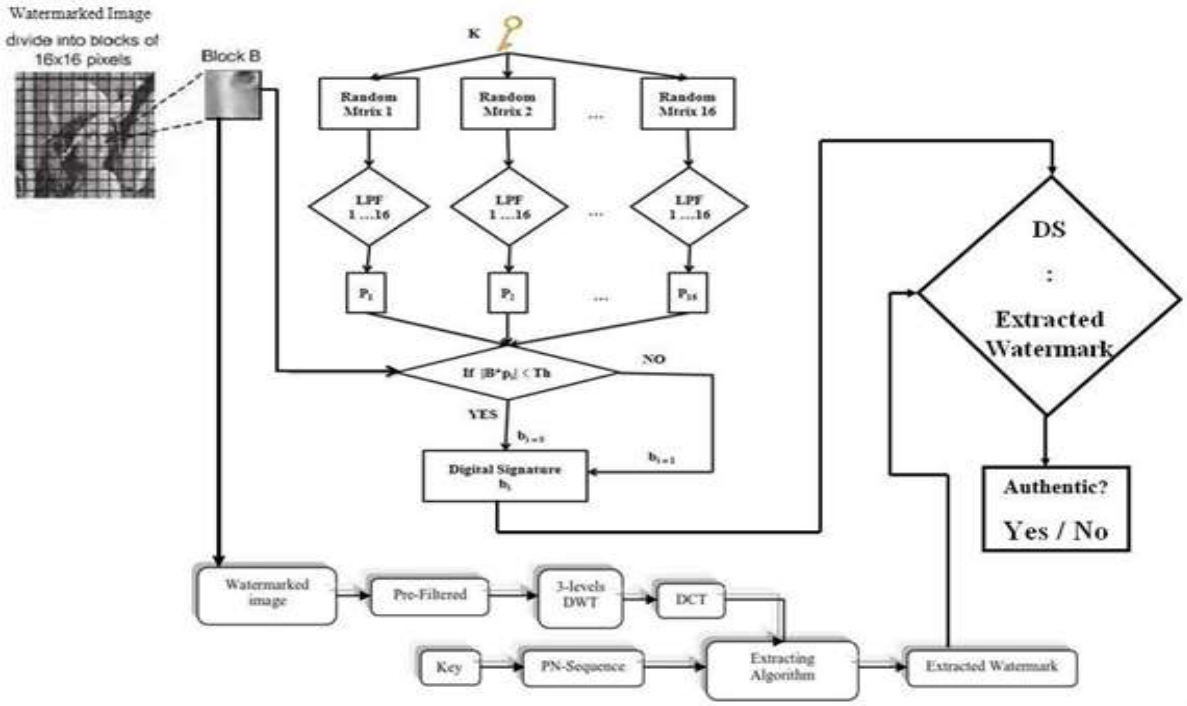

Fig 6. The proposed watermark extraction and verification procedure.

2.3 Verification

In the receiver's side, the same robust bits extraction and watermark detection methods are performed threshold, the correspondent block is regarded as being modified by others. Otherwise, the image is considered as integrity. Block based verification techniques is quite useful if the image is distributed in the Internet. If only some blocks are undesirably modified, just these blocks need to be re-transmitted, which reduces the burden of the network. This is very efficient when the Internet is in congestion.

3. Experimental Results

The experiment result in [4] shows that the purposed algorithm will find applications in many oblivious Watermarking schemes including secure data embedding into videos and watermarking images for tamper detection. And according to experiments and results in [5] the performance of the watermarking methods under consideration is investigated by measuring their imperceptible and robust capabilities. For the imperceptible capability, a quantitative index, Peek Signal-to-Noise Ratio (PSNR), is employed to evaluate the difference between an original image O and a watermarked image O. The watermarked is almost invisible to human visual system if PSNR value is greater than 35dB the watermarked image is within acceptable degradation levels.

4. Conclusion

Digital signature and digital watermark are two techniques used for copyright protection and authentication, respectively. In this paper, a combined digital signature and watermarking scheme is proposed for image authentication. The highest advantage of this combination besides the digital signature robustness and the watermark image imperceptibility, is that is not necessary an additional band width to transmit the digital signature, since this is embedded in the host image as a watermark. Experiments show our scheme is robust against common signal processing attacks like blurring, noising, cropping, scaling, JPEG compression and so on.

References

[1] M.Sreerama Murty, D.Veeraiah, Bernito A, A.Srinivas Rao,(2011) "Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis",Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, June 2011.

[2] Dr.M.Mohamed Sathik, S.S.Sujatha, (2010) "An Improved Invisible Watermarking Technique for Image Authentication", International Journal of Advanced Science and Technology, Vol. 24, November, 2010.

[3] Ali Al-Haj, (2007) "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3 (9): 740-746, 2007.

[4] J. Fridrich, (1999) "Robust Bit Extraction from Images", in Proceedings of IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), Vol. 2, 1999, pp. 536-540.

[5] Saeed K Amirgholipour, Ahmad R. Naghsh-Nilchi, (2009) "Robust Digital Image Watermarking based on joint DWT-DCT", International Journal of Digital Content Technology and its Applications, Vol. 3, No. 2.

[6] A. Cheddad , J. Condell, K. Curran and P. Mc Kevitt, (2010) "Digital Image Steganography: Survey and Analysis of Current Methods," Journal of Signal Processing, 90(3)(2010) 727-752.

[7] Neha Chauhanm Akhilesh A. Waoo, P. S. Patheja,"Information Hiding Watermarking Detection Technique by PSNR and RGB Intensity" International Journal of Computational Engineering and Management IJCEM, Vol. 15 issue 6, Nov. 2012.

Seyed Mohammad Mousavi recived his Associate's Degree in Computer Software from Amir Kabir Technical Academy, Arak, Iran and his Bachelor Degree in Hardwar Engineering Technology from Bahmanyar Higher Education Institute, Kerman, Iran. He is employed in Indusrial Management Institute - Qom Representative as IT Manager. His research intrests icludes Cryptography, Digital Watermarking and E-Commerce Security.