IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

An Extensive Survey of Image Integrity Approaches and Its Perspectives

Amit Bhagat[1] and Rajshree Dubey[2]*

[1,2*] *MANIT,Bhopal,India*

www.ijcseonline.org

Received: Apr/28/2015 Revised: May/09//2015 Accepted: May/20/2015 Published: May/30/ 2015

Abstract— The Storage of digital information is increasing day by day and at the same time new multimedia broadcasting services has also been developed. This development motivated research on copyright-protection and authentication schemes to be applied to these services. One Possible solution is to apply labelling which is a low level system that works upon the bit-stream. Another one is a high level, graphically inlaid, non-deletable system i.e. watermarking. This paper focuses on authentication and watermarking and presents methods that are proposed for the particular cases of still images. The effects of these methods to JPEG and other image formats are to be analyzed, as well as its sensitivity to image manipulations, are expounded and evaluated.

Keywords—Image integrity, image cropping, watermarking.

I. Introduction

There are new concerns rising about maintaining image integrity-ensuring that images and their associated metadata files match. If mismatches occurs, one could face considerable risks with significant financial and customer trust/public relations consequences. Speakers will present the challenge today's financial institutions are facing in maximizing image integrity, a critical component of quality assurance.

Watermarking is a technique used to hide data or identifying information within digital multimedia.

Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information.

A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each, or be common to multiple copies. In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting, where the original file remains intact and a new created file 'describes' the original file's content [1].

The digital watermarking process embeds a signal into the media without significantly degrading itsvisual quality. Digital watermarking is a process to embed some information called watermark into differentkinds of media called Cover Work [2][3].

Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

The major technical challenge is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection algorithm. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark. The literature survey explains robustness is the resistance of an embedded watermark against intentional attacks such as noise. Capacity is the amount of data that can be represented by an embedded watermark.

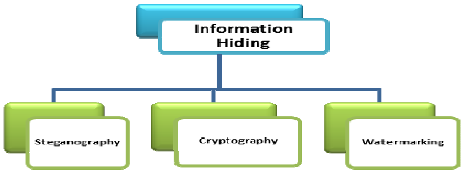

Figure 1: Tyes of Information hiding approaches

II. CLASSIFICATION

Visible watermark: The watermark that is visible in thedigital data like stamping a watermark on paper, (ex.) television channels, like HBO, whose logo is visibly superimposed on the corner of the TV picture.

Invisible watermarking: There is technology availablewhich can insert information into an image which cannot be seen, but can be interrogated with the right software. You can‗t prevent the theft of your images this way, but you can prove that the image that was stolen was yours, which is almost as good.

Image watermarking: This is used to hide the specialinformation into the image and to later detect and extract that special information for the author‘s ownership.

Video watermarking: This adds watermark in the videostream to control video applications. It is the extension ofimage watermarkingand needs real time extraction and robustness for compression.

Audio watermarking: This application area is one ofthe most popular and hot issue due to internet music, MP3.

Text watermarking: This adds watermark to the PDF,DOC and other text file to prevent the changes made to text.The watermark is inserted in the font shape and the spacebetween characters and line spaces.

Robust: Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossy compression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.

Fragile: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

Semi fragile: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression

Visual watermarking: It needs the original data in thetesting course, it has stronger robustness, but its application is limited.

Semi blind watermarking: It does not require an original media for detection.

Blind watermarking: It does not need original data, which has wide application field, but requires a higher watermark technology.

III. WATERMARKING TECHNIQUES

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information.

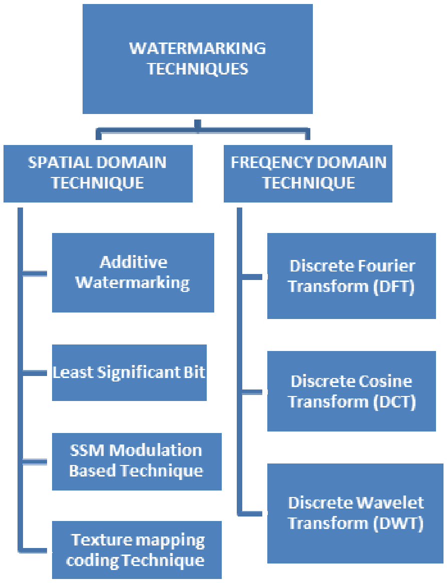
WATERMARKING TECHNIQUES
SPATIAL DOMAIN TECHNIQUE
FREQENCY DOMAIN TECHNIQUE
Additive Watermarking
Least Significant Bit
SSM Modulation Based Technique
Texture mapping coding Technique
Discrete Fourier Transform (DFT)
Discrete Cosine Transform (DCT)
Discrete Wavelet Transform (DWT)

Figure 2: Taxonomy of Watermarking techniques

III (A) SPATIAL DOMAIN TECHNIQUE

3.1.1 Additive Watermarking: It is the direct method used in spatial domain for embedding the watermark. It is done by adding pseudo random noise pattern to the intensity of image pixels. The noise signal may be integers like (-1, 0, 1) or floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of dif- ferent keys will be very low [14].

3.1.2 Least Significant Bit: Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks[20].A more sophisticated approach over conventional LSB method would be to use a pseudorandom number generator which determine the pixels to be used for embedding watermark based on a given key[13]. Security of the watermark would be enhanced greatly as the Watermark could now be no longer is easily viewable to the hackers or any other unintended user. Although this algorithm is still vulnerable to replacing the LSB's with a constant value.

3.1.3 SSM Modulation Based Technique: These technique are applied in the water marking algorithms with an linked information and attached to the original image with pseudo noise signal, its modulated by the watermark.

3.1.4Texture Mapping Coding Technique: This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [16], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture [20].

III(B) FREQUENCY DOMAIN TECHNIQUES

The target of this technique is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the -

- Discrete Cosine Transform (DCT),
- Discrete Fourier Transform (DFT),
- Discrete Wavelet Transform (DWT)

3.2.1 Discrete Cosine Transform (DCT): Discrete Cosine Transform is like as Discrete Fourier Transform. It is a technique for converting a signal into elementary frequency components [17]. The 2-dimentional DCT of given matrix gives the frequency coefficients in the form of another matrix. The left topmost corner of the matrix represents the lowest frequency coefficients while the right bottom most corner represents the highest frequency coefficients. Watermarking with DCT techniques are robust as compared to spatial domain techniques.

3.2.2 Discrete Fourier Transform (DFT): Transforms a continuous function into its frequency components [18]. It provides robustness against geometric attacks like scaling, cropping, rotation, translation etc.DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform. DFT is resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed [19].

3.2.3Discrete Wavelet Transform (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called Wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decompositionand is smaller for other bands (HH, LH, and HL) [20]. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution [21].

IV. USING THE TEMPLATE

This section attempts to provide a highlight regarding the most important image watermarking applications in recent pasts.

A. The survey of Rey et al. [4] identifies some of the emerging techniques of that time. They introduced the notion of image content authentication so that they can easily detect image tampering. They also highlighted the features about effective authentication scheme. They proposed an approach using feature based watermarking to show that an image is authentic even though the content has been modified.

B. Schneider et al. [5] proposed a scheme based on public key encrypted image block histogram for the purpose of authentication. The Euclidean distance between histogram of each block of the original image and the histogram of each block of the watermarked image is calculated. An authenticity measure is subsequently calculated by summing all the Euclidean distances over the entire image and compared against a pre-specified threshold for authentication. The major drawback of this scheme is twofold: First, 4 it is not secure enough because modifying an image without altering its histogram is trivial. Secondly, a large database of the public key encrypted histogram is required.

C. In this paper, Seo et al. [6] proposed a method forcontent based watermarking based on feature points ofan image. They embed watermark at each and everyfeature point after affine normalization according to thelocal characteristic scale. The proposed approach is robust enough against cropping, filtering, and affinenormalization and JPEG compression. It also supportsresilience against geometric distortions in watermarkdetection. Here, the original image is not needed for thewatermark detection. In this paper, the inaccuracy offeature point is overcome by using the local search. Theproposed method is computationally demanding thannormal watermarking and can easily handle geometric distortions.

D. To detect any manipulations on the gray level and re-sizing of a watermarked image, Wong [7] proposed a secret key watermarking scheme which is used in conjunction with a cryptographic hash function. The watermark can only be verified bythe user possessing the secret key. However, the requirement for transmitting the secret key to the user through a separate securechannel may jeopardize the security of the scheme.

E. To overcome this problem, Wong extended the secret key verification method into a public key scheme [8]. The value of the least significant bits (LSBs) of the original image are first set to zero, and the LSB-zeroed image is then divided into blocks of the same size as that of a watermark block. The image size together with each LSB-zeroed image block are then provided as inputs to a hash function and the output together with the watermark block are subjected to an exclusive-or (XOR) operation. The result of the XOR operation is then encrypted using a private key and embedded in the least significant bits of the original image. To verify the integrity of the received image, the receiving side must have the prior knowledge about the size of the transmitted image. This is the main drawback of their scheme because either the sender has to transmit this information via a separate secure channel, which may compromise the security of the scheme, or the scheme can only work on the images of fixed size.

F. Wu and Liu proposed in [9] an image authentication scheme by inserting a binary watermark into the DCT coefficients via a table look-up. In the first step of their scheme, a look-up table specific to the original image or a digital camera is generated, which maps all possible values of DCT coefficients randomly to either 1 or 0 with the constraint that the run-lengths of 1 and 0 are limited. Subsequently, a binary watermark pattern is embedded. At the receiver side, the extraction of the watermark is simply by looking up the table. Although, this scheme does not require the original image for watermark extraction, however, the same look-up table used in the embedding stage is necessary in the watermark extraction stage, which has to be transmitted through a secure channel and may compromise the security of the scheme.

G. Among the proposed fragile watermarking techniques, Yeung and Mintzer's scheme [10]is one of the most cited. In [20], watermark embedding is conducted by scanning each pixel and performing the watermark extraction function based on a look-up table. If the extracted watermark bit is equal to the authentic watermark bit, the pixel is left unchanged; otherwise, the value of the pixel is adjusted until the extracted watermark bit is equal to the authentic one. However, due to the lack of inter-relationship among neighboring pixels during the watermarking process, the look-up table and the binary logo can be easily inferred when the same look-up table and logo are reused for multiple images.

H. Attempting to counter this attack, Fridrich et al. proposed in a recent work [11] to inter-relate neighboring pixels during the watermark embedding process. Unfortunately, this technique is not able to detect the cropping on the right and from the bottom of the watermarked image

V. CONCLUSION

Watermarking can improve information protection from the information side. It allows a security layer the nearest as possible to the data because of its property to associate protection data with information to be protected in single object: a watermarked document.

Nevertheless, confidentiality and reliability are the main objectives that watermarking has been proposed for, considering applications like e-diagnosis or medical image sharing through PACS (Picture Archiving and Communication System). The expected outcome of the research would be a set of techniques that identify the image is modified or altered in some way, provide audit trail of changes done to the original image, and identify conversion from one format to another (jpeg to gif etc.) and will prevent alteration in the original image

REFERENCES

[1] Dr. Joachim von zur Gathen , Mahmoud El-Gayyar "Watermarking Techniques Spatial Domain Digital Rights" Seminar Media Informatics University of Bonn Germany May 06

[2] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518

[3] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011

[4] C. Rey, J.L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication", EURASIP

Journal on Applied Signal Processing 2002:6, pp. 613 – 621, Hindawi Publishing Corporation.

[5] M. Schneider and S. F. Chang, "A robust content based digital signature for image authentication," 12 in Proc. IEEE Intl. Conf. On Image Processing, vol. III, Lausanne, Switzerland, September 1996, pp. 227- 230.

[6] J.S. Seo, C.D. Yoo, "Image Watermarking based on scale space representation", Security, Steganography, and Watermarking of Multimedia Contents, VI, SPIE vol. 5306 2004, pp. 560 – 570

[7] P. W. Wong, "A watermark for image integrity and ownership verification," in Proc. IS & T PICConference, Portland, USA, May 1998.

[8] P. W. Wong, "A Public Key Watermark for Image Verification and Authentication," in Proc. IEEEIntl. Conf. On Image Processing, vol. I, Chicago, USA, October 1998, pp. 455-459.

[9] M. Wu and B. Liu, "Watermarking for Image Authentication," in Proc. IEEE Intl. Conf. On Image Processing, vol. II, Chicago, USA, October 1998, pp. 437-441.

[10] M. Yeung and F. Minzter, "Invisible Watermarking for Image Verification," Journal of Electronic Imaging, vol. 7, no. 3, pp. 578-591, July 1998.

[11] J. Fridrich, M. Goljan and A. C. Baldoza, "New Fragile Authentication Watermark for Images," in Proc. IEEE Int. Conf. Image Processing, vol. I, Vancouver, Canada, Sept. 2000, pp. 446-449.

[13] Frank Hartung, Martin Kutter(July 1999), "Multimedia Watermarking Techniques", proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[14] Lu, C-S., Liao, H-Y., M., Huang, S-K., Sze, C-J., " CombinedWa- termarking for Images Authentication and Protection" , in 1st IEEE- International Conference on Multimedia and Expo, vol. 3, 30 July-2Aug. 2000 pp. 1415 – 1418

[16] Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", 2010 International Conference on Intelligent Computation Technology and Automation

[17] Wu, C. and W. Hsieh, 2000, "Digital watermarking using zero tree of DCT", IEEE Trans. Consumer Electronics, vol. 46, No. 1, pp. 87-94.

[18] Ms.Jalpa M.Patel,"A brief survey on digital image watermarking techniques" ,International Journal For Technological Research In Engineering Volume 1, Issue 7, March-2014

[19]Vinita Gupta, "A Review on Image Watermarking and Its Techniques" International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 1, January 2014.

[20] Prabhishek Singh "A Survey of Digital Watermarking Techniques, Applications and Attacks" ,International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[21]Xiao Jun Kang Li Jun Dong, "Study of the Robustness of Watermarking Based on Image Segmentation and DFT", IEEE International Conference on Information Engineering and Computer Science, ICIECS, 2009, pp1-4.

AUTHORS PROFILE

Amit Bhagat is Assistant Professor in Department of MCA at Maulana Azad National Institute of technology, Bhopal. He has keen interest in Big data Analytics and Data Mining.

Rajshree Dubey is puruing Ph. D. from Maulana Azad National Institute of technology, Bhopal. She has keen interest in image mining and processing area.