A Survey of Blind & Non-Blind Watermarking Techniques

Shruti Sharma
Department of Computer Science & Engineering
Oriental College of Technology
Bhopal, India
sharma_shruti19@yahoo.com

Asst. Prof. Vivek Kumar
Department of Computer Science & Engineering
Oriental College of Technology
Bhopal, India
vivek_ndls@yahoo.co.in

Abstract — Watermarking is a term used for the hiding of some secrete information behind the images so that the attacker can't access the secrete or useful information from it. Since various watermarking techniques are already implemented for the information hiding. Here various blind and non-blind watermarking techniques are implemented and analyzed here and hence on the basis of their various advantages and limitations an efficient technique is implemented in future.

Keywords— Watermarking, fragile watermarking,

I. INTRODUCTION

The aim of watermarking is to include subliminal information (i.e., imperceptible) in a multimedia document to ensure a security service or simply a classification application. It would be then probable to improve the embedded message at any time, even if the document was changed by multiple nondestructive attacks, whether malevolent or not. In anticipation of now, the preponderance of publications in the area of watermarking mostly tackle the patent of still images. Other security services, such as image content verification, are still insignificant and many primary questions remain open. It may surprise, for instance, whether it is preferable to utilize a robust watermark, a fragile watermark, or still apply a entirely diverse technique. moreover, an validation service incompletely calls into question the settings generally recognized in watermarking copyright security, principally in conditions of the amount and nature of hidden information (for copyright or petent, the mark is autonomous of the image and is frequently a 64-bit identifier), as well as in terms of robustness[1].

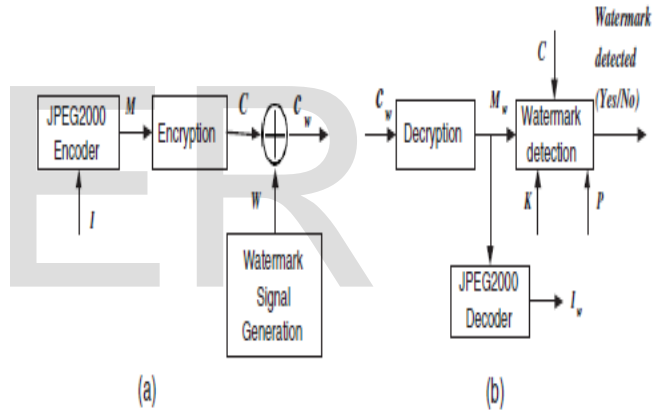

Figure 1: (a) Watermark embedding (b). Watermark extraction

Unfortunately this distinction is not always clear; it partly depends on the type of image and its use. Indeed the integrity criteria of an artistic masterpiece and a medical image will not be the identical. In first case, a JPEG compression will not affect the insight of the image, while in second case it may remove some of the fine details which would render the image totally useless. Even if the scope of this paper is the authentication of multimedia images for general purpose, it is interesting to notice that there exist methods dedicated to very specific integrity services, such as the authentication of medical and military images. Certainly such images should be customized by no means (including watermarking) and a strict definition of integrity is then required.

The first class of these methods is invertible watermarking scheme [2], in the sense that, if the image is deemed authentic,

the distortion due to the watermarking process can be removed to obtain the original image. Another approach [3] consists in separating the image into two zones: a region of interest (ROI) which is the part of the image used for the investigative, where data reliability must be severely restricted, and a region of noninterest (where distortions are allowed) used to embed the authentication data.

Various formulations have been proposed by Wu and Liu [4] and Lin and Chang [5]. However, we propose a generic image validation system. To be efficient, a system must assure the following criteria:

(1) **Sensitivity:** the system must be sensitive to malicious manipulations (e.g., modifying the image meaning) such as cropping or altering the image in specific areas.

(2) **Tolerance:** the system must tolerate some loss of information (originating from lossy compression algorithms) and more generally no malicious manipulations (generated, e.g., by multimedia providers or fair users).

(3) **Localization of modified regions:** the system should be able to locate precisely any malicious alteration made to the image and verify other areas as authentic.

(4) **Reconstruction of altered regions:** the system may need the capacity to reinstate, even incompletely, distorted or shattered regions in order to allow the user to know what the original content of the manipulated areas was. In addition, some technical features must be taken into account.

(i) **Storage:** authentication data should be embedded in the image, such as a watermark, rather than in a separate file, as is the case with an external signature.

(ii) **Mode of extraction:** depending on whether authentication data is dependent or not on the image, a full-blind or a semi blind mode of extraction is required. It is quite obvious that a non blind mode of extraction does not make sense for a verification service, since the unique image is compulsory.

(iii) **Asymmetrical algorithm:** contrary to classical security services such as copyright protection, an authentication service requires an asymmetrical watermarking (or encryption) algorithm (i.e., only the author of an image can secure it, but any user must be able to check the content of an image).

(iv) **Visibility:** authentication data should be invisible under normal inspection. It is a inquiry of making confident that the visual impact of watermarking is as weak as possible so that the watermarked image remains faithful to the original. Recently, a new approach based on invertible algorithms [2] has been proposed. The basic idea is to be able to remove the distortions due to the watermarking process to obtain the actual image data. Observably perfect in conditions of visibility, it is important to note that such an approach could create a very attractive context for attackers.

(v) **Security and Robustness:** it should not be feasible for authentication data to be forged or manipulated.

(vi) **Protocols:** protocols are an important aspect of any image authentication scheme; in exacting avoid defensive a despoiled picture. It is obvious that any algorithm alone cannot guarantee the security of the system. It is necessary to define a set of scenario and specifications describing the operation and rules of the system like the administration of the keys or the communication protocols between owner, seller, client, and so forth.

Most methods currently proposed for providing image authentication are based on a fragile watermark in opposition to robust watermark classically used for copyright protection. The basic idea underlying these techniques is to insert a specific watermark (generally independent of the image data [6]) so that any attempt to alter the content of an image will also alter the watermark itself (Figure 1). Therefore, the authentication process consists of locating watermark distortions in order to locate the regions of the image that have been tampered with. The major drawback of these approaches is that it is difficult to distinguish between malicious and non-malicious attacks (e.g., most fragile methods consider a lossy compressed image as a tampered image, whereas the semantic of the image is unchanged).

One of the first techniques used for image tampering detection was based on inserting check-sums into the least significant bits (LSB) of the image data. The algorithm proposed by Walton [7] in 1995 consists in selecting, according to a secret key, pseudorandom groups of pixels. The check-sum value is obtained by summing the numbers determined by the 7 most significant bits (MSB) of elected pixels. Then the check-sum bits are entrenched in the LSB. The basic version of this algorithm can be summarized as follows.

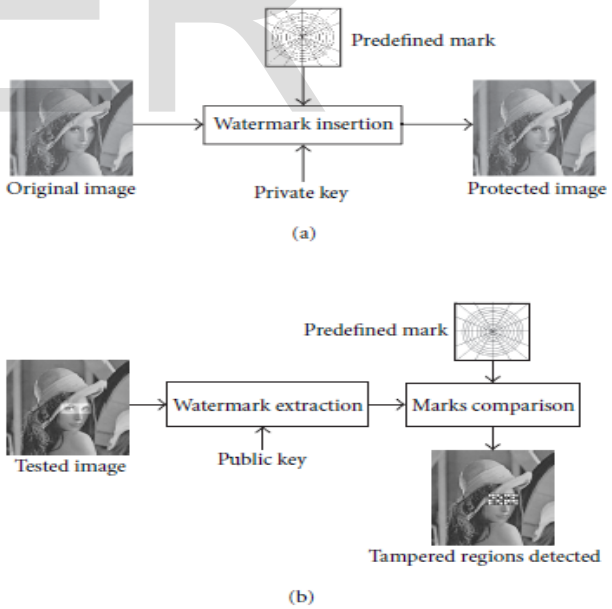

Figure 2: Generic fragile watermark scheme: (a) Security of Image. (b) Authenticity confirmation.

One of the drawbacks of this technique is that it is possible to swap homologous blocks (that are blocks of the same position) from two authenticated images protected with the same key. A

simple solution to this type of attack is to make the watermark dependent on the image substance. This could be attaining using the robust bit extraction algorithm proposed by Fridrich [8].

II. LITERATURE SURVEY

S. No.	Paper	Author	Technique used	Advantages	Issues
1.	A Robust Watermarking Technique Resistant JPEG Compression [9].	C. Hungfan, H.Yuhuang, A.Hsinghsu.	Quantization index modulation (QIM) and JPEG compression.	Can survive JPEG high compression ratios with good invisibility and robustness.	Results restrained by the embedding capacity.
2	Extracting Spread-Spectrum Hidden Data From Digital Media [10].	M. Li, M. K. Kulhandjian , D. A. Pados,Stella N. Batalama and M. J. Medley.	Multicarrier iterative generalized least squares andSpread spectrum embedding.	Can achieve recovery probability of error close to results known with embedding carriers and host autocorrelation matrix.	Less PSNR and more Error rate.
3	Compressed Encrypted Domain JPEG2000 Image Watermarking [11].	A. V. Subramanyam, Sabu Emmanuel, and Mohan S. Kankanhalli.	JPEG2000 Watermarking, Compressed and Encrypted Domain Watermarking.	Technique performs well against attacks like additive Gaussian noise, filtering and amplitude scaling.	Doesn't provide efficient watermarking.
4	A New Approach to Commutative Watermarking-Encryption [12].	R. Schmitz, S.Liy, Christos Grecosz and Xinpeng Zhang.	Commutative watermarkingencryption (CWE).	Using permutation cipher to encrypt the multimedia data leaving global statistics of the multimedia data intact, Watermark can be successfully extracted fromencrypted marked image or from marked encrypted image.	Generalization of the proposed CWE scheme to the compressed domain.

5	An Invisible Watermarking Technique for Image Verification[13].	Rashel Sarkar , Hemavathy R. and Dr. Shobha G.	Embedded watermark.	Low power spectral density,Interference limited operation,Privacy due to unknown random codes, Resistance to Interception,Resistance to multi-path effects.	The processing needs to be done pixel by pixel.
6	Shift Recompression-Based Feature Mining for Detecting Content-Aware Scaled Forgery in JPEG Images [14].	Q. Liu, X. Li, Peter A. Cooper and X. Hu.	Shift recompression, Ensemble classifier.	Steganalysis methods effective in detecting context-aware-based JPEG forgery.	Not identified the forged area and by adopting detectorcaused the error of out of memory.
7	Hiding Digital Watermarks Using Multiresolution Wavelet Transform [15].	Ming Shing Hsieh, Din Chang Tseng and Yong Huai Huang.	Discrete wavelet transform, Qualified significant wavelet tree.	Robust to signal distortions, such as JPEG, image cropping, sharpening, median filtering and incorporating attacks.	Not defined in applications of combining wavelet based digital watermarking, Image compression, progressive transmission and lost data reconstruction.
8	Anonymous Fingerprinting with Robust QIM Watermarking Techniques [16].	J. P. Prins, Z. Erkin, and R. L. Lagendijk.	Quantization index modulation (QIM), Fingerprinting.	Increased the robustness of the embedded fingerprints, while preserving the anonymity of the Fingerprinting protocol.	Uses the concept of modulation hence takes more time.
9	Efficient and Secure Encryption Schemes for JPEG2000 [17].	Hongjun Wu and Di Ma	Format compliant encryption scheme	Efficient and introduce d only small amount of Extra-computation, Highly secure.	Lossless compression technique.
10	A Survey of Watermarking Algorithms for Image Authentication [18].	Christian Rey and Jean Luc Dugelay.	Image content authentication.	Designed effective authentication scheme can detect whether image tampering has taken place.	Complementary counterattack methods to the classical cryptographic methods and No perfect solution for image data integrity.

11	A joint digital watermarking and encryption method [19].	M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale, and A. Neri.	Joint watermarking and ciphering key dependent domain, Tree structured haar transform.	Increased security of overall system, Authenticity of transmitted data.	Less secure and image gets tamper.
12	Tamper-Proof Image Watermarking using Self-Embedding [20].	Anamitra Makur and Nikhil Narayan S.	Fragile watermarking with self-embedding, Block based embedding and DCT based compression.	Enhanced watermark extraction, Tamper detection and recovery of images using no authentication bit.	Image may get tampered.
13	Watermarking for Image authentication [21].	Min Wu and Bede Liu.	Data embedding and Image Authentication.	Can detect and localize alterations of the original image and the tempering of the marked image.	Inefficient authentication.
14	Constructing Secure Content Dependent Watermarking Scheme using Homomorphic Encryption [22].	Zhi Li, Xinglei Zhu, Yong Lian and Qibin Sun.	Novel CDWM scheme, Homomorphic encryption and dirty paper pre-coding.	Achieved cryptographic level of security by proposing novel CDWM scheme.	Not able to improving the robustness of the proposed scheme.

III. CONCLUSION

Here in this paper a survey of all the techniques implemented for watermarking are discussed and analyzed here, so that on the basis of various advantages and limitations used a new and efficient technique is implemented in future.

References

[1].Christian Rey Jean-Luc Dugelay "A Survey ofWatermarking Algorithms for Image Authentication" Multimedia Department, Eurecom Institute, 2229 route de Crˆetes, B.P. 193, F-06904 Sophia Antipolis, France , EURASIP Journal on Applied Signal Processing 2002:6, 613–621 ,, Hindawi Publishing Corporation 2002 .

[2] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in *Proc*. SPIE Conf. Security and Watermarking of Multimedia Contents *III*, vol. 4314, pp. 197–208, San Jose, Calif, USA, January 2001.

[3] G. Coatrieux, B. Sankur, and H. Maˆıtre, "Strict integrity control of biomedical images," in Security and Watermarking of Multimedia Contents *III*, vol. 4314 of *SPIE* Proceedings, San Jose, Calif, USA, January 2001.

[4] M.Wu and B. Liu, "Watermarking for image authentication," in *Proc*. IEEE International Conference on Image Processing, vol. 2, pp. 437–441, Chicago, Ill, USA, October 1998.

[5] C.-Y. Lin and S.-F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," in *Proc*. SPIE International Conf. on Security and Watermarking of

Multimedia Contents II, vol. 3971, San Jose, Calif, USA, January 2000.

[6] M. M. Yeung and F.Mintzer, "An invisible watermarking technique for image verification," in Proc. IEEE International Conference on Image Processing, vol. 2, pp. 680–683, Santa Barbara, Calif, USA, October 1997.

[7] S. Walton, "Information authentification for a slippery new age," Dr. Dobbs Journal, vol. 20, no. 4, pp. 18–26, 1995.

[8] J. Fridrich, "Robust bit extraction formimages," in Proc. IEEE International Conference on Multimedia Computing and Systems, vol. 2, pp. 536–540, Florence, Italy, June 1999.

[9] chi-Hung Fan, Hui-Yu Huang and Wen-Hsing Hsu," A robust technique resistant jpeg compression", Journal of Information Science & Engineering, 2011.

[10] Ming Li, " Extracting spread-spectrum hidden data from digital media", IEEE 2013.

[11] A.V Subramanyam, Sabu Emmanuel," Compressed-Encrypted Domain JPEG-2000 Image Watermarking", IEEE 2010.

[12] Roland Schmitz, Shujun Li, Christos Grecos," A New Approach to Commutative Watermarking Encryption", 2010.

[13] Rashel Sarkar, Hemavathy R.," An Invisible Watermarking Technique for Image Verification", IJETAE 2012.

[14] Q. Liu, X. Li, Peter A. Cooper and X. Hu.," Shift Recompression-Based Feature Mining for Detecting Content-Aware Scaled Forgery in JPEG Images", ACM 2012.

[15] Ming Shing Hsieh, Din-Chang Tseng and Yong-Huai Huang "Hiding Digital Watermarks Using Multiresolution Wavelet Transform", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 48, NO. 5, IEEE-2001.

[16] J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous Fingerprintingwith Robust QIM Watermarking Techniques", Hindawi Publishing Corporation EURASIP Journal on Information Security-2007.

[17] Hongjun Wu, Di Ma, "EFFICIENT AND SECURE ENCRYPTION SCHEMES FOR JPEG2000", 2002

[18] Christian Rey, Jean-Luc Dugelay "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing, Hindawi Publishing Corporation-2002.

[19] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale, and A. Neri, "A joint digital watermarking and encryption method", 2007

[20] Anamitra Makur and Nikhil Narayan S. "Tamper-Proof Image Watermarking using Self-Embedding", ISI-KDD'12, ACM-2012.

[21]-Min Wu and Bede Liu "Watermarking for Image authentication", 0-8186-8821-1/98, IEEE-1998.

[22] Z. Li, X. Zhu, Y. Lian, and Q. Sun, "Constructing secure content-dependent watermarking scheme using homomorphic encryption," IEEE Int. Conf. Multimedia and Expo, 2007.