Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

A Survey of Fragile Watermarking-based Image Authentication Techniques

Xiao-Long Liu

Department of Computer Science
National Chiao Tung University, Hsinchu, Taiwan, R.O.C
shallen548@gmail.com

Chia-Chen Lin*

Department of Computer Science and Information Management
Providence University, Taichung, Taiwan, R.O.C
*Corresponding Author: mhlin3@pu.edu.tw

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University,Taichung 40724, Taiwan, R.O.C
Department of Computer Science and Information Engineering
Asia University, Taichung 41354, Taiwan, R.O.C
alan3c@gmail.com

Shyan-Ming Yuan

Department of Computer Science
National Chiao Tung University, Hsinchu, Taiwan, R.O.C
smyuan@cs.nctu.edu.tw

Received August, 2014; revised July, 2016

Abstract. *Image authentication is a technique aimed at protecting digital image authenticity and integrity when it is illegally modified. In this review paper, a literature survey of the emerging techniques for fragile watermarking-based image authentication is presented. To present a detailed description of existing fragile watermarking-based image authentication schemes, several of the existing representative schemes are classified into three main types in the paper, namely, spatial domain, frequency domain, and compression domain. Each main type is divided into two subtypes, which depend on each existing scheme having either recoverable or unrecoverable features. A characteristic analysis for all introduced schemes and comparisons of them in terms of localization, reconstruction capacities and other criteria are also offered. Finally, the potential issues of fragile watermarking-based image authentication are pointed out in the conclusion.*
Keywords: Image authentication, Fragile watermarking, Tamper detection, Localization capability, Reconstruction capability, Reversibility.

1. **Introduction.** With the rapid development of the information-oriented society, an increasing number of digitalized images are being transmitted over the Internet. Meanwhile, digital images can be easily manipulated and modified by the wide availability of powerful digital image processing tools. Once the authenticity and integrity of important original digital images are infringed upon and that infringement cannot be detected,

financial losses would occur. The research into watermarking-based image authentication has been undertaken to maintain the full integrity of digitalized images. The first watermarking-based image authentication technique was proposed by Schyndel et al. [1] in 1994. The watermarking procedure modifies certain features of the original image and the resulted object remains a meaningful image. The distortion cannot be perceived by the human visual system most of the time, so it is not easy for malicious attackers to suspect these watermarked images. Moreover, if an image is suspected as a manipulated or modified one, the authenticity and integrity of that suspicious image can be easily verified by watermarking-based image authentication techniques. Moreover, when the image is declared not authentic, the tampered areas can be detected or even restored using the detection or recovery functions provided by authentication techniques.

In this paper, we focus on a survey of previous fragile watermarking-based image authentication techniques. Fragile watermarking-based image authentication is first divided into two types based on the two basic image domains which the cover images belong to: (1) techniques in the spatial domain and (2) techniques in the compression domain. In addition, for techniques in the spatial domain, they are further classified as recoverable or non-recoverable techniques according to their recovery capability. Since basically all previous fragile watermarking techniques implemented in the compression domain cannot recover the tampered regions, the recovery capability is not a criterion for techniques in the compression domain introduced in this paper. Several representative, fragile watermarking-based image authentication schemes which are based on solid theory and frequently referred to in the related literatures are detailed and described in the following sections. Furthermore, we provide a characteristic analysis of these schemes and the comparisons among them. Analyses and comparisons are based on eight criteria are expanded from five general criteria, e.g., complexity, sensitivity, localization, and recovery capacities defined by [2] and visual quality as defined here.

2. **Criteria and Classifications of the Watermarking-based Image Authentication Techniques.** There are several general capacities used to estimate the effectiveness of a watermarking-based image authentication system [2]:

(1) Visual quality: The watermark in the authentication system must be invisible, and the distortion of the watermarked image cannot be perceived by the human visual system.
(2) Complexity: The proposed watermarking algorithm in an authentication system must be efficient, and its computing should be neither complex nor slow.
(3) Sensitivity: The authentication system must be able to correctly detect whether the suspicious image has been altered or not.
(4) Localization: The authentication system must be able to locate the image regions that have been altered correctly.
(5) Recovery: The authentication system must be able to partially or completely restore the image regions that were altered.
(6) Robustness: The authentication system can tolerate specific content-preserving manipulations.

According to the robustness feature, watermarking-based image authentication techniques can be further classified as either semi-fragile [3] or fragile watermarking-based techniques [4]. The main objective of semi-fragile watermarking-based image authentication techniques also known as selective authentication is to provide robustness against content-preserving manipulations, such as additive-noise, brightening, and compressions, while still able to detect and locate malevolent alterations and then restore the altered image regions.

In addition to semi-fragile watermarking-based image authentication schemes, fragile watermarking-based image authentication techniques also known as strict authentication are designed to make the embedded watermark easily destroyed once the watermarked image is attacked by any kind of manipulation. The major difference between the authentication of fragile watermarking and semi-fragile watermarking is that no modifications in the protected image are allowed for fragile watermarking authentication, while semi-fragile watermarking authentication withstands content preserved modifications. Thus, fragile watermarking-based image authentication is useful for applications that require strict authentication. Especially for military, medical and quality control images to prevent major financial and human life losses. For such circumstances, Walton [4] proposed the first fragile watermarking- based image authentication technique in 1995. Since then, many fragile watermarking techniques have been presented by scholars, and it is still a research topic that attracts researchers' attention.

3. Fragile Watermarking-based Image Authentication Techniques in the Spatial Domain.

In this section, we present several typical fragile watermarking-based image authentication techniques used in the spatial domain. Since recovery capability is an important criterion to evaluate a watermarking-based authentication technique, non-recoverable techniques and recoverable techniques are described here in Subsections 3.1 and 3.2, respectively, to provide readers the sufficient references.

3.1. Non-recoverable fragile watermarking-based image authentication techniques in the spatial domain.

The basic idea of non-recoverable fragile watermarking technique is having a predefined watermark embedded into an original image during the watermarking embedding process. In the authentication process, the embedded watermark is extracted from the suspicious image or from the attacked image using the same technique used in the embedding process. The extracted watermark is then compared with the predefined watermark to locate the watermark distortions and then locate the tampered regions on the image. The main drawback of a non-recoverable technique is that it cannot restore the original image regions that were tampered with and changed.

In 1997, Yeung and Mintzer proposed a method [5], wherein a binary map of a watermark was embedded into an original image to produce a watermarked image. In their watermark embedding process, a secret key was used to generate a binary valued function f, that maps pixels from the interval 0, 1, 2,, 255 to either 1 or 0. This binary function was used to make sure the extracted watermark from the unaltered watermarked image was equal to the watermark W. Thus, if the watermarked image was altered or damaged, the extracted watermark would be different with the watermark W. The localization capability and the visual quality of watermarked image offered by Yeung and Mintzer's scheme are both good. However, [6] Fridrich et al.'s have pointed out if the same logo and binary function f are reused for multiple images; it becomes very easy to draw the wrong conclusion during the authentication process. To prevent the above scenario from happening, Fridrich et al. proposed a scheme [7] in 2000, in which they involved aXa pixels in the mapping instead of just one pixel used in [5]. The wrong estimation of an attack does not occur with Fridrich et al.'s scheme because a large number of possible combinations of values are used in the binary function f.

For all of the literature mentioned above, no matter whether a watermarked image is tampered with or not, the original cover images cannot be reconstructed after watermark extraction and authentication. Now, some scholars have joined together the reversible data hiding techniques and fragile watermarking to provide a reconstruction capability of an authentic image. The goal of the reversible fragile watermarking technique used

in image authentication is not just to detect the tampered areas, but also to restore the distortion caused by the watermark embedding functions of the original images. If a watermarked image has not been tampered with, the embedded watermark can be extracted, and the watermarked image can be successfully restored back to the original image. Nevertheless, the tampered areas still cannot be restored once a watermarked image is under attack by any kind of manipulation.

In 2014, Lo and Hu [8] proposed a reversible fragile watermarking scheme for image authentication by using the concept of prediction-based histogram shifting scheme (PBHS). The watermark bits were first generated by the pseudo random number generator (PRNG) with a predefined seed S. In the predictive coding process, an original image was divided into 4X4 non-overlapping blocks. The center pixel in each block was chosen as the basic pixel for the predictive coding. For each block, the difference between each pixel and the corresponding basic pixel was computed to generate the prediction error. Thus, 15 predicted error values were generated in the predictive coding process in a 4X4 -pixels block. After the predictive coding processing of all image blocks was completed, a residual image with predicted error values was derived. Then, the histogram of all possible predicted error values in a residual image was generated. The histogram shifting technique with n pairs of peak and zero points for the predicted error values for a given residual image was used to embed the watermark bits. If a predicted error value was located in one of the peak points in the generated histogram, this predicted error value was considered an embeddable predicted error value. If each block of residual image contained at least one embeddable predicted error value, this block was considered an embeddable block, and a same 1-bit watermark bit c was embedded into the embeddable residual values in each block. By sequentially embedding the watermark bits into the embeddable blocks of the residual image, the watermarked residual image was generated. Finally, the watermarked image was produced by performing the inverse predictive coding process on the watermarked residual image. Later, authentication could be easily performed by comparing the original watermark bits generated by the PRNG to the extracted watermark bits in the watermarked image. The localization capability in Lo and Hu's scheme is very satisfying, as almost all of the tampered areas can be localized, because the same 1-bit watermark bit can be embedded into an embeddable block several times to enhance the detection ratio (DR). Furthermore, if the watermarked image is authenticated as an authentic image, it can be recovered and returned back to the original image completely.

3.2. **Recoverable fragile watermarking-based image authentication techniques in the spatial domain.** Different from non-recoverable techniques, recoverable fragile watermarking techniques can restore the tampered regions when the target image is altered. The flowchart of generic recoverable fragile watermarking techniques in the spatial domain is summarized as Fig. 1. The basic idea is to embed the predefined watermark and the recovery data into an original image. The watermark is used for authentication while the recovery data is used for restoration of the tampered image. In the authentication process, the hidden watermark is extracted from the suspicious image using the same technique applied in the embedding process. The extracted watermark is compared with the predefined watermark to detect and locate the tampered regions of the suspicious image. If the suspicious image is tampered, the recovery data is extracted for image restoration, and the recovered image is obtained. The image quality of the recovered image is also another important criterion for estimating a recoverable fragile watermarking technique.

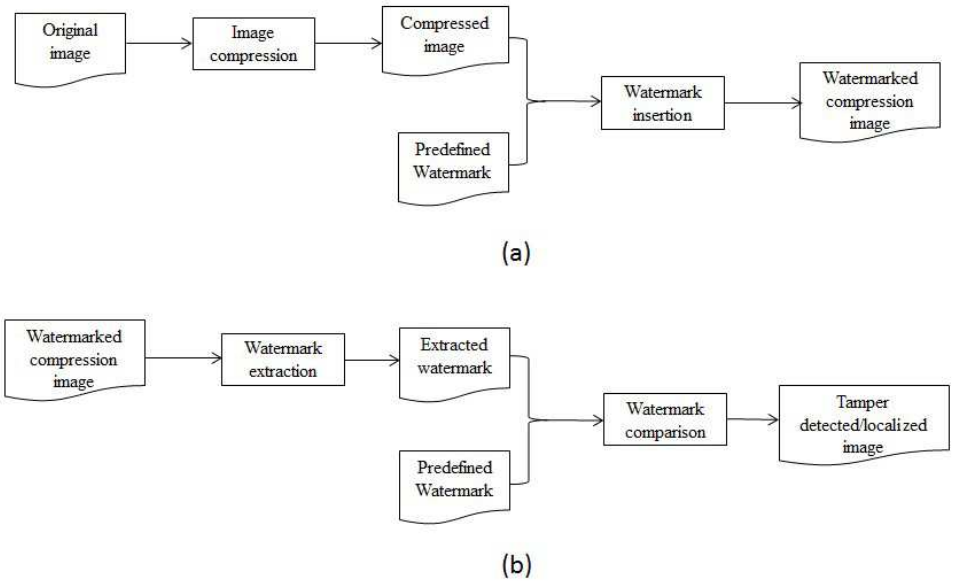

FIGURE 1. Generic recoverable fragile watermarking techniques in the spatial domain: (a) generation of authenticator; (b) verification of authenticity and restoration of tampered image

In 2005, Lin et al. [9] proposed a hierarchical fragile watermarking scheme for image tamper detection and recovery by using simple operations, such as parity check and comparison between the pixels average value of each block. In addition, they used 3 detection levels to ensure nearly 100% precision of tamper detection. However, if both of the two correlative blocks are tampered with, the image quality of recovered one will be significantly reduced. In 2008, Lee and Lin designed a dual watermarking scheme [10]. In their scheme, each block in an image contained recovery data of two other blocks, which means their scheme maintained two copies of information of the whole image and provided the second chance for block recovery in case one copy has been destroyed. Therefore, they provided a solution to overcome the drawback which existed in Lin et al.s method and ensured a higher image quality of recovered image even a watermarked image contains large tampered regions. To further enhance these recovery capacities while maintaining the high quality of localization and visual quality of a watermarked image, in 2010, Yang and Shen [11] proposed a tampered image recovery scheme by combining Wongs watermarking scheme [12] and the vector quantization (VQ) technique. If the watermarked image was judged as tampered, the altered pixels were recovered by replacing them with corresponding pixels in the VQ reconstructed-image. Since the VQ index table can be embedded into the cover image several times, an increased capability for image recovery is resulted. However, the visual quality of the watermarked image is still not so satisfying.

In 2013, a novel, chaos-based recoverable fragile watermarking approach was presented by Tong et al. [13] to provide enhanced visual quality of watermarked and restored images. First, an image was divided into non-overlapping 2X2 blocks. Then a chaotic map was applied to scramble blocks and their mapping blocks to enhance security. The average value (AVG) of each processing block X's four pixels was calculated, and 5 MSBs of block X's AVG were put into the mapping block Y's 3 LSBs of four pixels. The 5 MSBs(the most significant bits) of block X's AVG were regarded as recovery data. To improve the recovery capability, a sister block of Y was further generated to embed the 5 MSBs of block Xs AVG. In other words, the 5 MSBs information of each block have been embedded

into different blocks twice. To pad the 12-bits watermark section provided by the 3 LSBs of four pixels, two authentication bits m and n were appended. Authentication bit m was calculated by getting the number of "1" in this block and mod 2; the value of m was either 1 or 0. The other authentication bit was n=1-m. Here, m and n were used for tampering detection. During the detection procedure, the 12-bit watermark was retrieved from each block. The last two bits were indicated as m and n. Authentication bits m' and n'could be obtained by using the same approaches as embedding procedure. Two sets data were compared, if m not equal to m'or n not equal to n', the processing block was verified as invalid. During the recovery procedure, if a block X was invalid, its mapping block Y of this invalid block X was found. If block Y was valid, then the 5-bit of information of block X retrieved from block Y and assigned to block X's 4-pixels' 5 MSBs. Otherwise, the 5-bit of information of block X were retrieved from block Y's sister block and assigned to block X's 4-pixels' 5 MSBs, so that block X could be reconstructed. To improve the visual quality of recovered image, the remaining unrestored invalid blocks are recovered by being replacing with the average value for the valid blocks from their eight neighboring blocks. Scheme of Tong et al.'s tamper detection capability and the defense of attacks are improved by applying two authentication bits and a combination of the MSB and LSB mechanism. In addition, their recovery capability is improved by applying the sister block embedding and optimization method, which is used to find the average value of the valid blocks from their eight neighboring blocks and recover those unreconstructed blocks. In general, Tong et al.'s scheme has better performance on tamper detection and recovery even though the tampered area is relatively large.

4. **Fragile Watermarking-based Image Authentication Techniques in the Compression Domain.** Over the last three decades, diverse compression standards implemented on digital images have been developed by scholars, including JPEG, vector quantization (VQ)and block truncation coding (BTC), etc. As a result, the fragile watermarking-based image authentication techniques that can be implemented in the compression domain also draw the attention of many researchers. The flowchart of generic fragile watermarking-based image authentication techniques in the compression domain is summarized as Fig. 2. The watermark embedding procedure works on the compression image rather than the original image, and during the image compression procedure the original image may have occurred some distortion. Therefore, it becomes a crucial issue to maintain the image quality of the decompressed image during the watermark embedding procedure. In addition, the host data in the compression format does not provide sufficient space to carry the watermark, so it is also a challenge to locate the tampered area exactly while designing a watermarking technique. Therefore, tamper detection and localization capacities are the significant criteria for estimating a compression domain-based and fragile watermarking-based image authentication technique as well as the reconstructed image quality of a watermarked compression image. Basically, all the fragile watermarking-based image authentication techniques implemented in the compression domain and presented in the following paragraphs cannot restore the tampered regions when the targeted image has been altered. Thus, the recovery capability is not a criterion to use for a comparison of the techniques introduced in this section.

JPEG is a widely used compression standard for transmitting and storing digital images due to its outstanding compression rate and visual quality of the compression image. In 2004, Li [14] developed a fragile watermarking scheme for JPEG image authentication. The original image was first divided into non-overlapping 88 blocks. Then each block was transformed by DCT and quantized using a quantization table. The first binary map B1 was created to record the positions of the zero-valued coefficients. The second binary

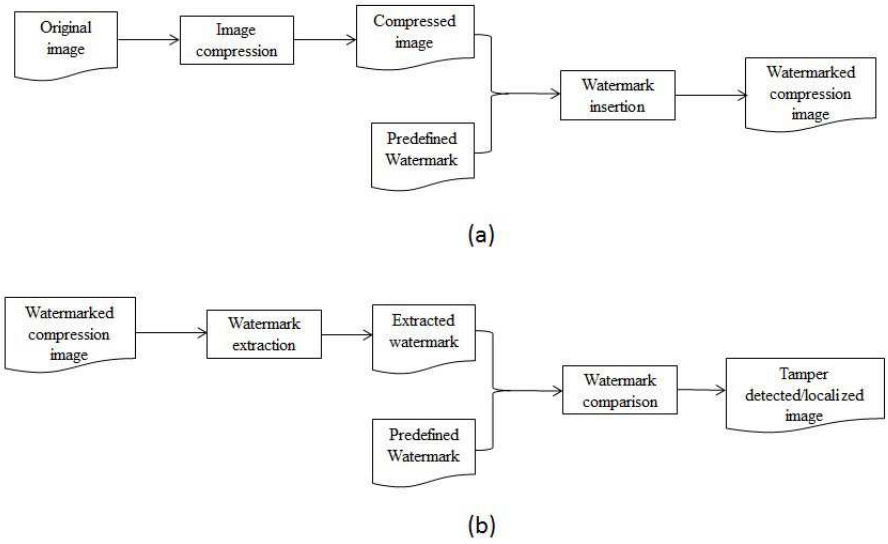

FIGURE 2. Generic flowchart of fragile watermarking-based image authentication techniques in a compression domain: (a) generation of authenticator; (b) verification of authenticity

sequence B2 with a length the same size as B1 was generated with a secret key. The watermark was then created by taking the result of the XOR operation on the binary sequences B1 and B2. For each DCT block, four non-zero coefficients whose frequencies were lower than or equal to a middle frequency h were chosen to embed the watermark. The four selected coefficients were justified based on their corresponding watermark bits and the non-zero coefficients of the 8 neighborhood coefficients. Li's scheme provides good localization capability, and the distortion after adding the watermark is unrecognized by the human visual system. However, the usage of eight neighboring coefficients may raise false alarms while the corresponding coefficients are manipulated. Therefore, the accuracy of the tamper localization in this scheme is not high. To provide the capability of tamper localization while minimizing the image distortion during watermark embedding, Zhang et al. [15] presented a reversible fragile watermarking for JPEG-compressed images in 2010. In this scheme, the watermark was generated by folding the hash results of quantized DCT coefficients in each block as a short bit-sequence. Each block was employed to carry two watermark bits using a reversible embedding method. Zhang et al.'s scheme provides a very satisfactory visual quality of a watermarked JPEG-compressed image due to its low degree of modification on the original image. Furthermore, if the watermarked JPEG-compressed image is not tampered, the watermark can be extracted, and the watermarked JPEG-compressed image can be recovered back to the original JPEG-compressed image.

Besides JPEG, VQ is another famous image compression technique and it is considered as a simpler and more efficient technique when compared to JPEG. In 2011, Chuang and Hu [16] proposed an adaptive fragile watermarking scheme for VQ-compressed images. The original image was first compressed into the index table with N indices. Then the index table was divided into several non-overlapping blocks made up of nXn indices. The total number of index blocks was calculated as T = N/(n*n). For each index block, parameters t needed to be predefined. It denotes the number of the indices in each block that will be selected to embed the watermark bit. Then, the total number of T*t predefined watermark bits were generated by the pseudo random number generator (PRNG) with a predefined seed. Let w present the watermark bits that were embedded into the selected index I. To embed w into the selected index I, the reminder r for I was

first computed as r = I mod 2. If r was equal to w, no change was made on the index I. Otherwise, the most similar index I'of I that satisfies I'mod 2 = w was found in the standard codebook and used to replace I. In Chuang and Hu's scheme, the number of selected indices t for each block was an important parameter for balancing the visual quality of watermarked compression image with the localization capability. When a large t was set to embed watermark bits, a better localization capability was obtained. On the contrary, the visual quality of the watermarked compression image was decreased when a large t was set. In general, the detection ratio is outstanding in Chuang and Hu's scheme while also maintaining an acceptable visual quality of the watermarked compression image.

In terms of BTC-compression, the fragile watermarking techniques for BTC-compressed images have also been proposed by scholars in recent years. In 2013, Hu et al. proposed a fragile watermarking technique [17] for BTC-compressed images, in which the watermark bits generated were based on the quantization values for each BTC block. The copies of watermark bits for each BTC block can be adaptively embedded into the bitmaps of other image blocks to attain a balance between the localization capability and visual quality of watermarked BTC-compression image. In the same year, an improved version of [17] was also presented by Hu et al. [18]. They jointed AMBTC and an image authentication scheme to process image compression and watermark embedding simultaneously. In this scheme, the watermark bits generated by a pseudo random number generator were still embedded into the bitmap of each AMBTC block. To improve the image quality of each AMBTC block further, two quantization values were justified based on the corresponding watermarked bitmap. Similar to [17], the number of embedded watermark bits for each bitmap is adaptable so as to reach a compromise between the image quality of the watermarked BTC-compressed image and the detection accuracy found in scheme [18].

5. **Comparisons and Summary.** In this section, certain performance comparisons among the above-mentioned fragile watermarking-based image authentication techniques are presented. The comparison is shown in Table 1. Eight criteria, as demonstrated in Table 1, are applied to compare the image authentication techniques. Difference with the six criteria mention in Section 2 which are used to estimate the effectiveness of general watermarking-based image authentication system (including semi-fragile and fragile watermarking-based techniques). The eight criteria illustrated as follows are specially designed for estimating the fragile watermarking-based techniques:

(1) Category: Three categories including non-recoverable techniques in the spatial domain (C1), recoverable techniques in the spatial domain (C2) or techniques in the compression domain (C3) are defined in this current review article. Here, we use "category" as a term to identify which type of each image authentication technique belongs to.
(2) Related technique: This term represents the kind of techniques used in each image authentication scheme.
(3) Domain: This term indicates which domain the image authentication scheme addresses.
(4) Watermarked PSNR: This term represents the visual quality of the watermarked image in each image authentication scheme. PSNR larger than 40dB is considered to be the threshold of a very good visual quality of the reconstructed image. While the PSNR lower than 30 dB would be considered as inadequate image quality.
(5) Reversible capability: The term represents whether the image authentication scheme is able to reconstruct an untampered watermarked image back to the original image
(6) Tamper Localization: The term represents the detection ratio for the location of tampered regions in the image authentication scheme.

(7) Tamper Recovery: It represents whether the authentication technique is able to restore the tampered image regions that have been tampered.
(8) Recovered PSNR: It represents the visual quality of the recovered image for tampered regions now restored using the authentication technique.

TABLE 1. Comparison of the fragile watermarking based image authentication techniques

Related Technique	Category	Basic Domain	Watermarked PSNR	Reversible Capability	Tampered Localization	Tampered Recovery	Recovered PSNR
Binary function [5, 7]	C1	Spatial	>40dB	No	Reasonable	No	N/A
Histogram [8]	C1	Spatial	>40dB	Yes	Good	No	N/A
Hierarchic [9]	C2	Spatial	>40dB	No	Good	Yes	>30dB
VQ [11]	C2	Spatial	30∼40dB	No	Good	Yes	>30dB
Chaos map [13]	C2	Spatial	30∼40dB	No	Good	Yes	25∼30dB
JPEG [14]	C3	Compression	30∼40dB	No	Reasonable	No	N/A
Hash& JPEG[15]	C3	Compression	30∼40dB	Yes	Good	No	N/A
VQ [16]	C3	Compression	25∼30dB	No	Good	No	N/A
BTC [17, 18]	C3	Compression	25∼30dB	No	Good	No	N/A

Note: N/A denotes recovered PSNR cannot be provided because this scheme does not have a tamper recovery capability

According to the above comparisons and summary table, the features of representative fragile watermarking techniques for image authentication offered over the last two decades have been clearly presented. All the image authentication techniques shown in Table 1 can detect any manipulation of the images. Several observations can be seen in Table 1. For the non-recoverable techniques in the spatial domains, scheme of Lo and Hu [8] presents the most outstanding performance compared to the others because it is the only one that provides reversible capability and maintains really good watermarked PSNR and tamper localization capability. For the recoverable techniques in the spatial domain, schemes of Yang and Shen [11] and Tong et al. [13] are relatively outstanding, and all provide very good watermarked PSNR, tamper localization capability, and recovery capability. For the techniques in the compression domain, scheme of Zhang et al. [15] provides reversible capability and really good watermarked PSNR and tamper localization capability. The other schemes have drawbacks in either visual quality of watermarked image or their detection ratio.

In terms of watermarked PSNR, the image authentication schemes designed in the spatial domain achieve a better visual quality of watermarked image than most of the

schemes that are implemented in the compression domain. That is because during the image compression procedure, the original image has already occurred some distortion, especially for those schemes which are based on BTC- or VQ-compressions. In terms of tamper localization capability, most of the schemes presented after 2000 satisfy this criterion, indicating that the research into image authentication schemes has achieved great improvement. However, the research into image authentication schemes for an image integrity protection purpose still has a large development potential. It was found that only schemes of Lo and Hu [8] and Zhang et al. [15] shown in Table 1 provide the enough capability of reversible watermarking. Furthermore, only a few image authentication schemes provided a good recovery capability up to now.

Both recovery capability and reversible capability are very important to have to protect image integrity. The latter can reconstruct the original image if it has not been tampered with and the former can restore tamper regions after an image has been under attack. Therefore, future research for relative watermarking-based authentication should focus on presenting a scheme that can provide outstanding reversible and recovery capacities while still maintaining good tamper localization capability and the visual quality of the watermarked image. In addition, the research into presenting efficient outstanding authentication schemes in the compression domain is still a critical issue for saving network bandwidth during the transmission of digitalized images.

6. **Conclusions.** Image authentication is the process of proving image integrity and authenticity. The literature survey presented in this paper has focused on fragile watermarking-based image authentication techniques. These techniques are further classified into non-recoverable techniques in the spatial domain, recoverable techniques in the spatial domain, and techniques used in the compression domain, according to the basic domain and recovery capability. For each category, several typical schemes were introduced and some criteria listed in this paper to evaluate the performance of each authentication technique. After a comparison and summary of previous literature, the importance of the future research for presenting authentication schemes that can deliver outstanding reversible and recovery capability while maintaining good tamper localization capability and the visual quality of watermarked images is further stressed.

REFERENCES

[1] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, A digital watermark, *Proceedings of the IEEE international conference on image processing*, vol. 2, pp. 86-90, 1994.

[2] A. Haouzia, and R. Noumeir, Methods for image authentication: a survey, *Multimedia Tools and Applications*, vol. 39, no. 1, pp. 1-46, 2008.

[3] L. Rosales-Roldan, M. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana, and B. Kurkoski, Watermarking-based image authentication with recovery capability using halftoning technique, *Signal Processing: Image Communication*, vol. 28, no. 1, pp. 69-83, 2013.

[4] S. Walton, Information Authentication for a Slippery New Age, *Dr. Dobbs Journal*, vol. 20, no. 4, pp.18 -26, 1995.

[5] M. Yeung, and F. Mintzer, An invisible watermarking technique for image verification, *Proceedings of the International Conference on Image Processing*, vol. 2, pp. 680-683, 1997.

[6] J. Fridrich, M. Goljan, and N. Memon, Further attacks on yeung-mintzer watermarking scheme, *Electronic Imaging. International Society for Optics and Photonics*, pp. 428-437, 2000.

[7] J. Fridrich, M. Goljan, and A. C. Baldoza, New fragile authentication/watermark for images, *Proceedings of the International Conference on Image Processing*, vol. 1, pp. 446-449, 2000.

[8] C. C. Lo, and Y. C. Hu, A novel reversible image authentication scheme for digital images, *Signal Processing*, vol. 98, no. 3, pp. 174-185, 2014.

[9] P. L. Lin, C. K. Hsieh, and P. W. Huang, A hierarchical digital watermarking method for image tamper detection and recovery, *Pattern Recognition*, vol. 38, no. 12, pp. 2519-2529, 2005.

[10] T. Y. Lee, and S. D. Lin, Dual watermark for image tamper detection and recovery, *Pattern Recognition*, vol. 41, no. 11, pp. 3497-3506, 2008.
[11] C. W. Yang, and J. J. Shen, Recover the tampered image based on VQ indexing, *Signal Processing*, vol. 90, no.1, pp. 331-343, 2010.
[12] P. W. Wong, and N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1601, 2001.
[13] X. J. Tong, Y. Liu, M. Zhang, and Y. Chen, A novel chaos-based fragile watermarking for image tampering detection and self-recovery, *Signal Processing: Image Communication*, vol. 28, no. 3, pp. 301-308, 2013.
[14] C. T. Li, Digital fragile watermarking scheme for authentication of JPEG images, IEE Proceedings-Vision, Image and Signal Processing, vol. 151, no, 6, pp. 460-466, 2004.
[15] X. P. Zhang, S. Z. Wang, and G. Feng, Reversible fragile watermarking for locating tampered blocks in JPEG images, *Signal Processing*, vol. 90, no. 12, pp. 3026-3036, 2010.
[16] J. C. Chuang, and Y. C. Hu, An adaptive image authentication scheme for vector quantization compressed image, *Journal of Visual Communication and Image Representation*, vol. 22, no. 5, pp. 440-449, 2011.
[17] Y. C. Hu, W. L. Chen, C. C. Lo, and C. M. Wu, A novel tamper detection scheme for BTC-compressed images, *Opto-Electronics Review*, vol. 21, no. 1, pp. 137-146, 2013.
[18] Y. C. Hu, C. C. Lo, W. L. Chen, and C. H. Wen, Joint image coding and image authentication based on absolute moment block truncation coding, *Journal of Electronic Imaging*, vol. 22, no. 1, pp. 013012:1-11, 2013.