Journal of Computer Science 5 (11): 831-837, 2009
ISSN 1549-3636

A Fragile Watermarking Scheme for Image Authentication with Tamper Localization Using Integer Wavelet Transform

P. MeenakshiDevi, M. Venkatesan and K. Duraiswamy
KS Rangasamy College of Technology, Tiruchengode, India

Abstract: Problem statement: In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Method for authenticating and assuring the integrity of the image is required. Image authentication is possible by embedding a layer of the authentication signature into the digital image using a digital watermark. In some applications tamper localization is also required. **Approach:** In this study, we proposed a fragile image authentication system with tamper localization in wavelet domain. In this scheme, secret data to be embedded is a logo. Watermark was generated by repeating logo image so that size of watermark matches with the size of HH sub-band of integer wavelet transform. To provide additional level of security, the generated watermark was scrambled using a shared secret key. Integer Haar wavelet transform was applied to obtain wavelet coefficients. Watermark was embedded into the coefficients using odd-even mapping. **Results:** Experimental results demonstrated that proposed scheme detected and localized tampering at pixel level. Proposed scheme was tested with images of various sizes and tampering of various sizes. It provided good results for tamperings ranges from single pixel to a block of pixels. **Conclusion:** Watermarking was done in wavelet domain; conventional watermarking attacks were not possible. The resolution of tamper localization was achieved at pixel level. The watermarked image's quality was still maintained while providing pixel-level tampering accuracy. Proposed scheme can be used in insurance, forensics departments.

Key words: Watermarking, authentication, tamper localization, integer wavelet transform

INTRODUCTION

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values[1]. There are many spatial and frequency domain techniques available for authentication watermarking[2-8].

In message authentication, only the image integrity is verified, but sometimes this is not sufficient in digital images and tamper localization is also required. The situations include forensics, crime, insurance. Tamper localization is used to identify the specific positions where the tamper has occurred.

To achieve tamper localization many existing schemes use block-based approach[9-12]. One of the first fragile watermarking techniques proposed for detection of image tampering was based on computing check-sums of gray levels which is determined from the seven most significant bits of the image. The check-sum is embedded into the Least Significant Bits (LSBs) of pseudo-randomly selected pixels[9]. One weakness of this scheme is that it is possible to swap blocks in an image without causing a detectable change. It is called as Vector-Quantization (VQ) attack or transplantation attack. But, VQ attack can be avoided by including the block position or block index to the image data before hashing[10]. The watermark can be calculated in a multi level hierarchy so that both VQ attack resiliency and high accuracy for tampering localization is achieved[11]. The watermark may include not only the block location but also a content-feature of another block and a Cyclic Redundancy Check (CRC) checksum[12]. The CRC checksum is used to authenticate the block inspected where as the block location and content-feature of another block are used for complicating the VQ

Corresponding Author: P. MeenakshiDevi, KS Rangasamy College of Technology, Tiruchengode, India

attack. The localization accuracy of this scheme is stated as 8×8.

Some schemes provide pixel-wise tampering localization[13-18]. One of the first pixel-wise authentication schemes was proposed in[13]. A secret binary function is used to map the value of each pixel to a preset logo bit. But, this scheme is vulnerable to many attacks[19-23] and it can be overcome by introducing the neighborhood dependency in mapping a pixel to a logo bit[14]. The pixel-wise schemes are vulnerable to oracle attack if the pixel scan order is public[24].

Recently, the researchers have focused on wavelet-based watermarking schemes for image authentication[25-31]. Some tamper localization schemes are proposed in wavelet domain[26,30]. In[26], the watermark is generated using DWT and embedded into the Least Significant Bits (LSB) of host image. In[30], a semi-fragile authentication scheme is proposed in which selective rounding of coefficients is carried out to embed the secret information. The techniques which uses transform domain are more complex and computationally expensive. Yet, they offer high degree of robustness against common image processing operations[30].

Almost all the pixel-wise schemes proposed in literature watermark pixels sequentially, one pixel at a time[13-18]. In these schemes, an image is scanned in a certain order to embed the watermark. The scan order may be public or secret. In[14] the image is scanned in a row-by-row scan order. In[15] the image is scanned in a zig-zag scan order. A neighborhood-dependent mapping function is used to map each pixel value to a desired logo bit. A special symmetry structure in the logo is used to authenticate the block content, while the logo itself carries information about the block origin (block index, the image index or time stamp, author ID).

In block-based approach, the image is divided into sub-blocks and the watermarking information is embedded into each and every block. Each individual block is authenticated by the successful retrieval of the watermark embedded in it. If the watermark of a particular sub-block is not retrieved successfully, then that sub-block alone is identified to be tampered and the remaining part of the image is authenticated. In these types of schemes, the localization resolution is based on the size of the sub-blocks. In[12], the size of the sub-blocks is 8×8 and hence the detection resolution is 8×8. The smaller sub-block size is required to increase the detection resolution. But this will lead to higher watermark payload. In[9], an image divided into non-overlapping blocks of W×H pixels. The watermarking is done for each block separately. Two versions of the algorithm have been proposed. In the private key version, the seven most significant bits of all pixels in the block are hashed using a secure key-dependent hash. The hash is then XORed with a chosen binary logo and inserted into the LSBs of the same block. Verification is done in the reverse order. Comparison with the logo indicates tampered blocks. In the public key version, the 7 MSBs are hashed using a fixed hash, XORed with the logo and then encrypted using a public key encryption method. The encrypted bit-stream is again inserted in the LSBs of the same block. During the verification process, first the hash of the 7 MSBs of all pixels in that block is calculated, XORed with the decrypted LSBs and the result is compared with the binary logo. The ability of this scheme to localize modifications is very satisfactory. The block size should be chosen so that the whole hash (128 bits) can be embedded. For example, block sizes of 8×16 or 12×12 pixels are possible. The logo can be either a binary picture with a graphical meaning or a randomly generated black and white pattern.

Since the block-based schemes embed watermark locally, they are vulnerable to local attacks. The major weakness of the block-wise schemes is VQ or transplantation kind of attack in which it is possible to swap blocks in an image without causing a detectable change. If an attacker has a database of images authenticated with the same key, it is possible to take an arbitrary image and modify it to make it authentic. One can divide the image into blocks and for each block perform a search through the blocks in the same position in all database images. The original block is then replaced with the closest match. This kind of VQ attack is applicable to schemes in which it is possible to identify disjoint groups of image elements that are modified without context. Consequently, most schemes that can localize changes are vulnerable to this attack[24]. This problem could be avoided by including the block position or block index to the image data before hashing[10]. In[24], VQ attack is overcome by XORing more block information such as block position, image index, camera ID.

There are few papers in tampering localization in wavelet domain[31-34]. In this model, DWT is applied to the original image to obtain the four sub-bands LL, HL, LH and HH. The watermark used here is usually a random binary string or a logo kind of image. The watermark bits are embedded in either of the sub-bands. Embedding data in high frequency sub-bands generates watermarked images with less distortion. The watermark bits are embedded in sub-bands by modifying the wavelet coefficients. To improve security, the coefficients can be selected in random order. Tamper localization model in wavelet domain overcomes the problems of the other two models. VQ attack and oracle attack are not possible in wavelet domain model. Hence, it is more secure than the other two models.

MATERIALS AND METHODS

The proposed scheme performs watermark embedding in wavelet domain. The image is decomposed by integer Haar wavelet transform. The watermark is embedded only in the HH sub-band. But, coefficients of all the sub-bands are considered in watermark embedding process. The proposed scheme finds tampering positions at pixel level.

Preprocessing: The following steps are carried out as preprocessing activity before embedding the watermark:

- Apply integer Haar wavelet transform to decompose the original image
- Rearrange the coefficients of sub-bands
- Permute the coefficients

The preprocessing steps are shown in Fig. 1. At first, the original image is decomposed by applying integer Haar wavelet transform to get LL, HL, LH and HH sub-bands. The coefficients of the sub-bands are combined together to form a new image. The coefficients in the sub-bands which corresponds to the same spatial location are grouped together to form a 4-coefficient block. Let C_{LL}, C_{HL}, C_{LH}, C_{HH} are the coefficients of LL, HL, LH and HH sub-bands respectively. The coefficients are rearranged as shown in Fig. 2.

The grouped coefficients form a new rearranged image (RImage) which is of the same size as the original image. The RImage is divided into sub-blocks of size 2×2. Each sub-block consists four coefficients where C_{LL} is placed at (0,0), C_{HL} is placed at (0,1), C_{LH} is placed at (1,0) and C_{HH} is placed at (1,1). Hence each sub-block represents the coefficients of all the sub-bands corresponding to the same spatial location.

Then these sub-blocks are randomly permuted by a secret key to obtain a permuted image (PImage). The original image is scrambled in wavelet domain but, the coefficients corresponding to same spatial location are preserved which enables easy tamper localization. Now, the PImage is ready for embedding the watermark in it.

To achieve statistical independency with respect to the image structure, the sub-blocks are permuted. The permutation can be viewed as a bijective mapping[2] of the sub-blocks indexes:

$$f : \{1,2,3....S\} \rightarrow \{1,2,3,....S\}$$

where, S is the total number of sub-blocks. Permutation is achieved by a two steps process. In the first step, S numbers of pseudo random numbers are generated by using Linear Congruential Generator (LCG). The second step is to sort the generated random numbers and identifying their index in the sorted list. The index list is nothing but the expected permuted list.

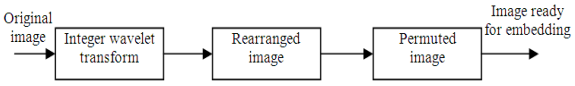

Fig. 1: Preprocessing

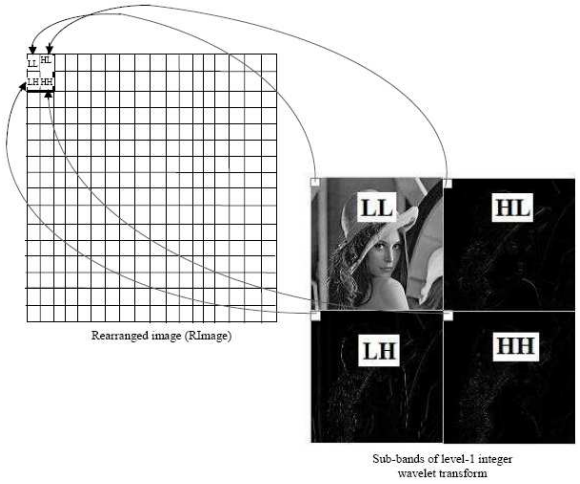

Fig. 2: Formation of rearranged Image (RImage)

LCG is one of the most popular methods for generating random numbers. The general formula used in LCG is:

$$I_k = (aI_{k-1} + c) \bmod m \quad (1)$$

Where the values a, c and m are pre-selected constants:
a = Known as the constant multiplier
c = The increment
m = The modulus

Given, $m \in Z^+$ the algorithm generates a sequence of random variables $X_n : Z^+ \rightarrow Z^+$ that are uniformly distributed in [0, m]. The LCG algorithm starts with a seed 's' and constants $a \geq 2, c, m \in Z^+$. Then the sequence of X_n is defined recursively as:

$$X_0(s) = s \quad (2)$$

$$X_{n+1}(s) = (aX_n(s) + c) \bmod m \quad (3)$$

When the increment c = 0, it is called as multiplicative congruential method. The seed plays an important role for the LCG. It determines the sequence, the LCG will generate. Hence, the permutation key shared between the sender and the receiver is used as the seed for LCG. At the receiving side, the same sequence of random numbers can be generated by giving the same permutation key as the seed for LCG.

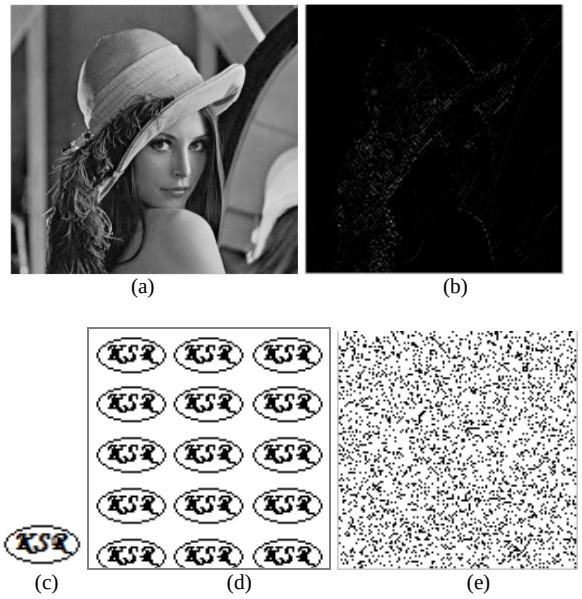

Fig. 3: Watermark generation for Lena image; (a) original image; (b) HH sub-band (c) original logo (d) generated watermark (e) scrambled watermark

Here, the 2×2 sub-blocks are shuffled and permuted order is generated randomly and the watermark is embedded in the permuted sub-blocks. The same shuffling needs to be performed at the receiver side also.

Watermark embedding: The watermark to be embedded is taken as a either a logo or a random sequence of predefined bits which is known to both the sender and the receiver. The advantage of using the logo is that cropping can be easily detected.

The watermark is generated by repeating the logo image so that the size of the watermark matches with the size of the HH sub-band of Integer Wavelet Transform. Figure 3 shows the watermark generation process for Lena image (256×256). The size of HH sub-band is 128×128 and the size of the logo is 42×27. The HH sub-band and the original logo are shown in Fig. 3b and 3c respectively. To provide additional level of security, the generated watermark is scrambled using a shared secret key. Figure 3d and e shows the generated and scrambled watermark.

The PImage is divided into sub-blocks of size 2×2. Let the sub-block is represented as F_i. As already stated, each sub-block consists four coefficients where C_{LL} is placed at (0,0), C_{HL} is placed at (0,1), C_{LH} is placed at (1,0) and C_{HH} is placed at (1,1). The coefficients are added to produce the sum of that sub-block. The sum is used to represent the embedded watermark bit.

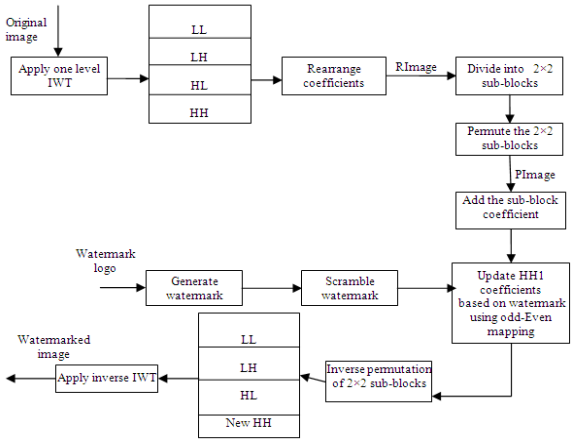

Fig. 4: Watermark embedding process

Odd-even mapping is the simplest and well known scheme in spatial domain. If the sum is an odd number, it is assumed that bit-1 is embedded, otherwise (even number) it is assumed that bit-0 is embedded. If the sum matches with the bit to be embedded then no change is made to the coefficients. Otherwise, the coefficient of HH sub-band ($[F_i]_{2,2}$) is either incremented or decremented to have the required value. Here, all the four sub-band coefficients are considered for computing the sum, but only the HH sub-band is modified to embed the watermark.

After the embedding process is over, inverse permutation is applied to get the rearranged form (RImage) of original image. Then, the coefficient values are separated from the 2×2 sub-block and restored back to LL, HL, LH and HH sub-bands. Now, inverse integer Haar wavelet transform is applied to get the final watermarked image. Figure 4 shows the watermark embedding process.

Watermark extraction: At the receiving side, the receiver does the same process as the sender for preprocessing step. At first, the watermarked image is decomposed by applying integer Haar wavelet transform to obtain LL, HL, LH and HH sub-bands. Then the coefficients of sub-bands of watermarked image are rearranged (WRImage) and permuted to obtain Watermarked-Permuted-Image (WPImage). The WPImage is divided into sub-blocks of size 2×2. Let the sub-block is represented as F_i^*. As already stated, each sub-block consists four coefficients each from the four sub-bands. The coefficients are added to produce the sum of that sub-block. If the sum is an odd number, it is assumed that bit-1 is embedded, otherwise (even number) it is assumed that bit-0 is embedded. One bit is retrieved from each of the 2×2 sub-blocks. The bits are retrieved from top left corner of the watermarked image. Figure 5 shows the watermark extraction process.

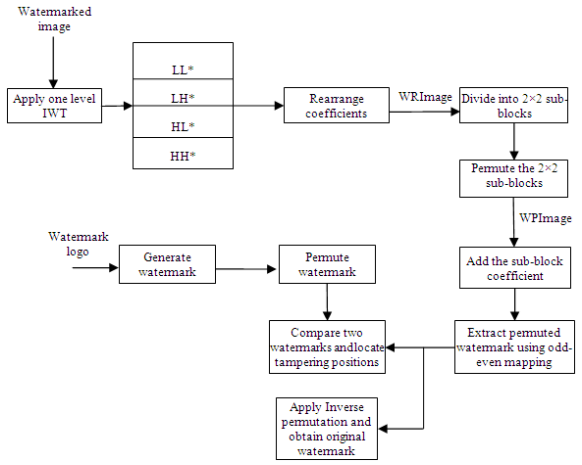

Fig. 5: Watermark extraction

Table 1: Experimental Results

Image	Size	MSE	PSNR
Lena	256×256	0.2296	60.9120
Mandrill	116×116	0.2826	59.1066
Peppers	512×512	0.2673	59.5915
Barbara	130×130	0.2744	59.3638
Camera	256×256	0.2481	60.2396
Zelda	512×512	0.2621	59.7627
Angel	98×130	0.2443	60.3706

RESULTS

The effectiveness of the proposed scheme is explained using the following experimental results. Figure 6a and b are the watermarked and tampered watermarked image. Figure 6c is the generated watermark for the Barbara image (130×130). At the receiving side, once the watermark is retrieved, it is compared with the original watermark. Since the retrieved watermark is in permuted form, the receiver must generate the watermark as per the size of the received image and permute it using the same key. Now the two watermarks are compared for equality. If they differ at some position, then the respective 2×2 sub-block is marked as black as shown in Fig. 6e. Figure 6d shows the retrieved watermark after applying the inverse permutation. It reveals that some tamperings have been occurred in the watermarked image. After applying inverse permutation to Fig. 6e, the tampering positions are clearly located as shown in Fig. 6f. The tampering positions are marked in white blocks in the watermarked image as shown in Fig. 6g. The proposed scheme is able to identify even a single pixel modification. Table 1 shows the PSNR and MSE of the watermarked images.

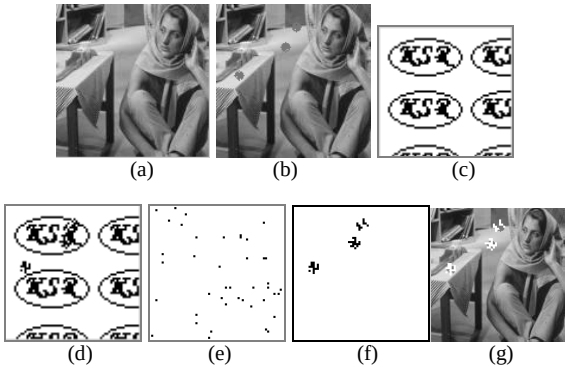

Fig. 6: Tampering Localization in Barbara image (a) watermarked image (b) tampered watermarked image (c) generated watermark (d) retrieved Watermark (e) Difference (generated Vs retrieved watermark) (f) difference (after inverse permutation) (g) watermarked image with tampering positions in white color.

DISCUSSION

The proposed method is tested on several gray-scale images of various sizes and can be extended to color images also. The main objectives are to provide image authentication and to localize tamper positions.

The embedded watermark is distributed in the wavelet coefficients in such a way that it does not causes perceptual artifacts. The quality of the watermarked image is not affected even though it provides localization at pixel level. The PSNR of different images shows that the system is successful in hiding the authentication signature without making noticeable changes in the original image.

Protection against VQ attack is a major issue for authentication and localization schemes. In the proposed system, the security of the whole system against VQ attack is achieved by permutation of wavelet coefficients. But, still it provides pixel-level tamper localization.

CONCLUSION

A wavelet-based fragile watermarking scheme for secure image authentication has been presented. In the proposed scheme, the embedded watermark is generated and scrambled based on the size of the image to be watermarked. This provides more protection to the watermarking system. Integer wavelet transform is applied and the proposed watermarking system localizes the tamperings at pixel level. Simulation results have been given to demonstrate the efficiency of the proposed scheme.

REFERENCES

1. Albanesi, M.G., M. Ferretti and F. Guerrini, 2001. A taxonomy for image authentication techniques and its application to the current state of the art. Proceeding of the 11th International Conference on Image Analysis and Processing, Sept. 26-28, IEEE Xplore Press, Palermo, Italy, pp: 535-540. DOI: 10.1109/ICIAP.2001.957065
2. Wu, M. and B. Liu, 2004. Data hiding in binary image for authentication and annotation. IEEE Trans. Multimedia, 6: 528-538. DOI: 10.1109/TMM.2004.830814
3. Kim, H.Y. and R.L. de Queiroz, 2004. Alteration-locating authentication watermarking for binary images. Lecture Notes Comput. Sci., 3304: 125-136. http://www.springerlink.com/content/n8du7x7c1lx2dhr7/
4. Kim, H.Y. and A. Afif, 2003. Secure authentication watermarking for binary images. Proceedings of the XVI Brazilian Symposium on Computer Graphics and Image Processing, Oct. 12-15, IEEE Xplore Press, USA., pp: 199-206. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1241009
5. Kim, H.Y. and A. Afif, 2004. A secure authentication watermarking for halftone and binary images. Int. J. Imag. Syst. Technol., 14: 147-152. DOI: 10.1002/ima.20018
6. Paulo, S.L.M., H.Y. Kim and V. Rijmen, 2001. Toward a secure public-key blockwise fragile authentication watermarking. Proceedings of the IEEE International Conference on Image Processing, Oct. 7-10, IEEE Xplore Press, Thessaloniki, Greece, pp: 494-497. DOI: 10.1109/ICIP.2001.958536
7. Yang, H. and A.C. Kot, 2006. Binary image authentication with tampering localization by embedding cryptographic signature and block identifier. IEEE Sign. Proc. Lett., 13: 741-744. DOI: 10.1109/LSP.2006.879829
8. Puhan, N.B., A.T.S. Ho and F. Sattar, 2007. Erasable authentication watermarking in binary document images. Proceedings of the IEEE International Conference on Innovative Computing, Information and Control, Sept. 5-7, IEEE Xplore Press, Kumamoto, pp: 288-291. DOI: 10.1109/ICICIC.2007.289
9. Wong, P.W., 1998. A watermark for image integrity and ownership verification. Proceedings of the Image Processing, Image Quality, Image Capture, Systems Conference, May 17-20, ACM, Portland, Oregon, USA., pp: 374-379. http://www.pubzone.org/dblp/conf/pics/Wong98
10. Wong, P.W. and N. Memon, 2000. Secret and public key authentication watermarking schemes that resist vector quantization attack. Proceedings of the Security and Watermarking of Multimedia Contents, Jan. 24-26, ETATS-UNIS, San Jose, California, pp: 417-427. http://cat.inist.fr/?aModele=afficheN&cpsidt=1379098
11. Celik, M.U., G. Sharma, E. Saber and A.M. Tekalp, 2001. A hierarchical image authentication watermark with improved localization and security. Proceedings of the International Conference on Image Processing, Oct. 7-10, IEEE Xplore Press, Thessaloniki, Greece, pp: 502-505. DOI: 10.1109/ICIP.2001.958538
12. Lin, P.L., P.W. Huang and A.W. Peng, 2004. A fragile watermarking scheme for image authentication with localization and recovery. Proceeding of the IEEE 6th International Symposium on Multimedia Software Engineering, Dec. 13-15, IEEE Xplore Press, USA., pp: 146-153. DOI: 10.1109/MMSE.2004.9
13. Yeung, M.M. and F.C. Mintzer, 1998. Invisible watermarking for image verification. J. Elect. Imag., 7: 578-591. http://adsabs.harvard.edu/abs/1998JEI.....7..578Y
14. Fridrich, J., M. Goljan and A.C. Baldoza, 2000. New fragile authentication watermark for images. Proceeding of the IEEE International Conference on Image Processing, Sept. 10-13, IEEE Xplore Press, Vancouver, BC., Canada, pp: 446-449. DOI: 10.1109/ICIP.2000.900991
15. Li, C.T., F.M. Yang and C.S. Lee, 2002. Oblivious fragile watermarking scheme for image authentication. Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP '02), IEEE Xplore Press, USA., pp: 3445-3448. DOI: 10.1109/ICASSP.2002.1004653
16. Zhong, H., F. Liu and L.C. Jiao, 2002. A new fragile watermarking technique for image authentication. Proceeding of the 6th International Conference on Signal Processing, pp: 792-795.
17. Lu, H., R. Shen and F.L. Chung, 2003. Fragile watermarking scheme for image authentication. Elect. Lett., 39: 898-900. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1209481&isnumber=27211
18. Wu, J., B.B. Zhu, S. Li and F. Lin, 2004. A secure image authentication algorithm with pixel-level tamper localization. Proceeding of the International Conference on Signal Processing, Oct. 24-27, IEEE Xplore Press, USA., pp: 1573-1576. DOI: 10.1109/ICIP.2004.1421367

19. Memon, N., S. Shende and P.W. Wong, 1999. On the security of the Yeung-Mintzer authentication watermark. Proceeding of the Image Processing, Image Quality, Image Capture, Systems Conference, Apr. 1999, Savannah, Georgia, pp: 301-306. http://www.imaging.org/store/epub.cfm?abstrid=1048
20. Fridrich, J., M. Goljan and N. Memon, 2000. Further attacks on yeung-mintzer fragile watermarking scheme. Proceedings of the Security and Watermarking of Multimedia Contents II, Jan. 24-26, ETATS-UNIS, San Jose, California, pp: 428-437. http://cat.inist.fr/?aModele=afficheN&cpsidt=1379060
21. Holliman, M. and N. Memon, 2000. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. EEE Trans. Image Proc., 9: 432-441. DOI: 10.1109/83.826780
22. Fridrich, J., M. Goljan and N.D. Memon, 2002. Cryptanalysis of the Yeung-Mintzer fragile watermarking technique. J. Elect. Imag., 11: 262-274. http://adsabs.harvard.edu/abs/2002JEI....11..262F
23. Wu, J., B. Zhu, S. Li and F. Lin, 2004. Efficient oracle attacks on Yeung-Mintzer and variant authentication schemes. Proceedings of the IEEE International Conference on Multimedia and Expo, June 30-30, IEEE Xplore Press, Taipei, pp: 931-934. DOI: 10.1109/ICME.2004.1394354
24. Fridrich, J., 2002. Security of fragile authentication watermarks with localization. Proceedings of the Security Watermarking Multimedia Contents IV, Jan. 21-24, ETATS-UNIS, San Jose, California, pp: 691-700. http://cat.inist.fr/?aModele=afficheN&cpsidt=14182163
25. Peter, M., 2001. Digital image watermarking in the wavelet transform domain. Master's Thesis, Department of Scientific Computing, University of Salzburg, Austria. http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/MasterThesis/
26. He, H., J. Zhang and H.M. Tai, 2006. A wavelet-based fragile watermarking scheme for secure image authentication. Lecture Notes Comput. Sci., 4283: 422-432. DOI: 10.1007/11922841
27. Li, C.T. and H. Si, 2007. Wavelet-based fragile watermarking scheme for image authentication. J. Elect. Imag., 16: 1-9. http://adsabs.harvard.edu/abs/2007JEI....16a3009L
28. Wu, X., J. Hu, Z. Gu and J. Huang, 2005. A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters. Proceedings of the Australasian Workshop on Grid Computing and e-Research, (GCR'05), ACM Press, Newcastle, New South Wales, Australia, pp: 75-80. http://portal.acm.org/citation.cfm?id=1082302
29. Tsai, M.J. and H.Y. Hung, 2005. Wavelet transform based digital watermarking for image authentication. Proceedings of the 4th International Conference on Computer and Information Science, (ICIS'05), IEEE Xplore Press, USA., pp: 408-411. DOI: 10.1109/ICIS.2005.128
30. Paquet, A.H., R.K. Ward and I. Pitas, 2003. Wavelet packets-based digital watermarking for image verification and authentication. Sign. Process., 83: 2117-2132. http://portal.acm.org/citation.cfm?id=950453
31. Rafiullah, C., A. Khan, A. Idris and Z. Munir, 2006. A secure semi-fragile watermarking scheme for authentication and recovery of images based on wavelet transform. Int. J. Applied Sci. Eng. Technol., 2: 30-33. http://www.waset.org/journals/ijaset/v2/v2-1-6.pdf
32. Liu, H. and M. Steinebach, 2006. Digital watermarking for image authentication with localization. Proceedings of the IEEE International Conference on Image Processing, Oct. 8-11, IEEE Xplore Press, Atlanta, GA., pp: 1973-1976. DOI: 10.1109/ICIP.2006.313112
33. Kundur, D. and D. Hatzinakos, 1998. Towards a telltale watermarking technique for tamper proofing. Proceedings of the International Conference on Image Processing, Oct. 4-7, IEEE Xplore Press, Chicago, Illinois, pp: 409-413. DOI: 10.1109/ICIP.1998.723403
34. Winne, D.A., H.D. Knowles, D.R. Bull and C.N. Canagarajah, 2002. Digital watermarking in wavelet domain with predistortion for authenticity verification and localization. Proceedings of the Security Watermarking Multimedia Contents IV, Jan. 21-24, ETATS-UNIS, San Jose, California, pp: 349-356. http://cat.inist.fr/?aModele=afficheN&cpsidt=14182221