I. J. Computer Network and Information Security, 2012, 2, 43-49
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.02.07

Semifragile Watermarking Schemes for Image Authentication- A Survey

Archana Tiwari[1], Manisha Sharma[2]

[1] Chhatrapati Shivaji Institute of Technology, Durg
archanatiwari@csitdurg.in

[2] Bhilai Institute of Technology, Durg
manishasharma1@rediffmail.com

Abstract—**Digital images are very easy to manipulate, store, publish and secondary creation this juggle will lead to serious consequence in some applications such as military image, medical image. So, integrity of digital image must be authenticated. Tools that help us establish the authenticity and integrity of digital media are thus essential and can prove vital whenever questions are raised about the origin of an image and its content. To project authenticity of images semi fragile watermarking is very concerned by researchers because of its important function in content authentication. Semifragile watermarking aim to monitor contents of images not its representations. In present paper various semi fragile water marking algorithm are studied using some image quality matrices, insertion methods used, verification method . Finally some observations are given based on literature survey of algorithms and techniques of semifragile watermarking techniques**

Index terms—**Image authentication, Content recovery, Robustness, Semifragile watermarking, Tamper detection.**

I. Introduction

The wide availability of powerful digital image processing tools allows extensive access, manipulations and reuse of visual materials. In fact, lot of people could now easily make unauthorized copies and manipulate images in such a way that may lead to big financial or human lives losses. These problems can be better understood with a simple example. A patient with a serious illness, discovered from medical diagnostic images, may eventually get better due to medical treatments. The medical follow-up of that patient involves the interpretation of historic images to evaluate the progression of the illness in time. A possible false diagnosis can jeopardize the patient life, if the stored image underwent malevolent manipulations, storage errors or compression, such that the resulted distortions cannot be detected by the doctor. This is an example where modifications are not tolerated. However, in many other applications we need to tolerate some image processing operations for transmission, enhancement or restoration while we still need to detect at the same time any significant changes in the image content [1].

Image authentication is meant for verifying integrity and authenticity of digital images. An image authentication should be able to 1) detect the tampering in image, 2) locate the positions of alternations, and 3) recover altered regions automatically. In general, an image authentication scheme consists of an embedding stage and a verification stage. The embedding stage embeds the authentication code to serves as the stamp for the integrity of the image; the verification stage evaluates the consistence between the authentication code evaluated from a received image and the one calculated in the embedding stage to decide whether the image is altered or not.

According to the processing of the generated authentication code, image authentication techniques can be divided into two categories: 1) digital-signature-based approach, and 2) watermarking-based approach [1]. Many problems are encountered with digital signatures. The first problem is related to the concept of a signed document. In fact, a conventional signature is physically attached to the signed document, which is not the case for digital signatures. A digital signature algorithm is needed to attach, in some way, the signature to the electronic document. The second problem is related to the verification of the signature authenticity. A conventional signature is authenticated by comparing it with a certified one. For example, when one signs an act of purchase by credit card, the salesman compares the signature with the one on the back of the card. This authentication method is obviously not very reliable, since it is easy to imitate the signature of someone else. An electronic signature however, can be verified by any person that knows the verification algorithm. Lastly, a fundamental difference resides between conventional and digital signature: Any copy of an electronic document is identical to its original while a signed paper document copy can usually be distinguished from its

original. This difference introduces a fundamental problem related to the conceptual definition of an original electronically signed document and methods that forbid its reuse. The digital-signature-based image authentication scheme computes the digest for an image and stores it in a separate file. The main advantage of this method is that the original image is exhibited without any modification, which ensures the value and originality to the original image [1].In watermarking-based image authentication approaches, the authentication data is embedded directly into the original image. The method by embedding authentication codes in an image itself has the advantage that no extra storage is needed, that benefits the transmission of the image [2].

The authentication watermark can he classified to fragile watermark and semi-fragile watermark according to its fragility and sensitivity. The fragile watermark is very sensitive and designed to detect every possible change in marked image; so it fits to verify the integrity of data, and is viewed as an alternative verification solution to a standard digital signature 'scheme. But in most multimedia applications, minor data modifications are acceptable as long as the content is authentic, so the semi-fragile watermark is developed and widely used in content verifying. Semi-fragile watennark is robust to acceptable content-preserving manipulations, while fragile to malicious distortions such as feature adding or removal, so it is suitable to verify the trustworthiness of data. The primary advantage of employing semi-fragile watermarking over digital signature and fragile watermarking technology is that there is greater potential in characterizing the tamper distortion, and in designing a method which is robust to certain kinds of processing. [3].Lossless and lossy compression, smoothing, format conversion and light additive noise, are typically acceptable modifications since image content interpretation is not affected but the exact representation during exchange and storage need not be guaranteed. The alterations on the documents can occur unintentionally or can be implanted intentionally. The so-called unintentional or innocent alterations typically arise from such diverse facts as bit errors during transmission and storage, or signal processing operations such as filtering, contrast enhancement, sharpening, and compression. Intentional or malicious alterations, on the other hand, are assumed to be due to an explicit forgery attempt by a pirate with the explicit purpose of changing the contents of a document [4]. The main distinction then, is whether the content is altered as in malicious and intentional attacks or whether only the representation, but not the content, of the document is altered, as occurs in unintentional, nonmalicious cases. The line of demarcation between these two attacks categories is, however, not always clear-cut, as it depends very much on the application domain.

In present paper existing semi-fragile watermarking schemes are discussed for image authentication application. In section 2 challenges in front of semifragile watermarking are discussed, section 3 discusses what requirements of semifragile watermarking schemes to combat these challenges are discussed, section 4 discusses methods and domain used by different watermarking schemes, section 5 presents summary of different semifragile algorithms, Section 6 gives analysis, finally section 7 presents brief conclusion of paper.

II. Semifragile Watermarking Challenges

Strict image authentication considers an image as non-authentic when just an image pixel or even one bit of data has been changed. There are applications that need such service. However, this is not the desired authentication method for most practical cases [2]. Ideally, we wish to compress an image in order to save memory space or bandwidth; we may want to enhance an image and restore it for better perceptual quality or even to convert its format.

In this context, we need an authentication service that tolerates specific image processing operations. These image processing operations change pixel values without modifying the image content. Therefore, the real problem of selective image authentication is related to the problem of image semantic content definition. Some of the challenges as found from literature survey are discussed here-

1. It is desirable in many applications to authenticate the image content, rather than the representation of the content. One would like the authenticator to remain valid across different representation as long as the perceptual content has not been changed. Conventional authentication techniques based on cryptographic hash functions, message digests and digital signatures only authenticate the representation.

2. Security is another crucial goal of semi-fragile authentication systems. A successful image authentication system must be designed to be secure against intentional tampering attacks. Compared to traditional “hard” authentication in which any modification to the signal is concluded as illegal tampering.

3. In applications, such as in law enforcement, medical image systems, it is desired to be able to reverse the stego-media back to the original cover media for legal consideration. semi-fragility which allows lossy compression or noise disturbing to some extent is required for an integrated and powerful authentication

system. It is a real tough task to design an effective reversible semi-fragile authentication watermark (RSAW) scheme with features as tamper localization, good perceptual invisibility, detection without requiring explicit knowledge of the original image

4. Good balance between robustness against mild incidental image distortions and fragility to tampering attacks is desirable in semifragile watermarking scheme. A semi-fragile authentication watermark should protect the integrity of the image content rather than its exact representation.

5. Distinguishing content-preserving operations from malicious attacks is also a big challenge for semifragile watermarking.

III. Requirements for Semi-Fragile Watermark-Based Image Authentication Systems.

1. Robustness and fragility objectives should be simultaneously addressed. When both cannot be completely achieved, one must have a quantitative mechanism to tradeoff between these objectives.

2. The semi-fragile authentication system must be secure to intentional tampering. For security, it must be computationally infeasible for the opponent to devise a fraudulent message.

3. Given the watermark is an authenticator, embedding must be imperceptible.

4. The authentication embedding and verification algorithms must be computationally efficient, especially for real time applications.

5. The Peak Signal to Noise Ratio (PSNR) metric is widely used to measure the amount of difference between two images based on pixel differences. High value of PSNR shows the watermarked image has a better quality, the difference between the original image and the watermarked image is imperceptible.

6. Reconstruction of altered regions: The system may need the ability to restore, even partially, altered or destroyed regions in order to allow the user to know what the original content of the manipulated areas was.

7. Asymmetrical algorithm: contrary to classical security services, an authentication service requires an asymmetrical algorithm.

8. Tolerance: The system must tolerate some loss of information and more generally nonmalicious manipulations.

IV. Semifragile Authentication Algorithm

Digital watermarking technology processing contains two cores: watermark embedding algorithm and detection algorithm. Robustness, imperceptibility, invisibility and security of digital watermarking is generally the focus of the requirements.

A. Integer wavelet transform (IWT) domain

Digital watermarking in wavelet transform is one of study-intensive activities. IWT can be computed starting from any real valued wavelet filter by means of a straightforward modification of the lifting scheme.

It can reconstruct the original image without distortion, has strong robustness and good invisibility [11, 12, 15, 19].

B. Discrete cosine transform (DCT) coefficient in high frequency domain

The characteristics of this algorithm are robust, well hidden and resistant to a variety of signal deformation resistance. The digital watermark of DCT transform domain has inherent ability of lossy compression resistance. The disadvantage is its large amount of calculation [7, 13, 18, 20].

C. Tchebichef Moments

Discreet orthogonal moments like Tchebichef moments are orthogonal in the domain of the image coordinate space, a feature that completely eliminates the need for any discrete approximation in their numerical implementation [17].

D. Contourlet transform

The contourlet transform is a directional multiscale decomposition scheme. It is constructed by combining: a multiscale decomposition followed by a directional decomposition, thus capturing geometric and directional information. Finally, the image is represented as a set of directional subbands at multiple scales [9].

E. Quantization technique

The DC coefficients are quantized into odd or even interval in terms of watermarking label generated by the key. It is very robust to JPEG compression and can precisely localize modified region [10, 20].

F. Pinned Sine Transform

In PST *(*Pinned Sine Transform), the image is divided into overlapped blocks which introduce an inter-block relationship to the pinned sine transformed images. Therefore the watermarking of any particular block also depends on its location in the image instead of depending only on its own content [7].

G. Discrete wavelet transform

Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation. It converts an input series x_0, x_1,.x_m, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series [3,5,6].

H. Arnold Transform

Arnold transform has much to do with the size of image. The amount of calculation will be too much if we recover the original image [14].

Summary representing algorithms used by different authors, PSNR values, applications suggested by authors and verification methods is given in table 1.

V. Summary of different semifragile watermarking methods

One design challenge for content authentication watermarks is to achieve a good balance between robustness against mild incidental image distortions and fragility to tampering attacks. According to summary table as given in table no 1, algorithm performances are application specific as some attacks are acceptable for some applications while same may be unsuitable in other application.

Telltale watermarks are semi-fragile watermarks that can survive small distortions and minor transformations such as lossy compression, but are destroyed when an image is heavily modified [3].

As suggested by Bassem Abdel-Aziz high sensitivity to de-synchronization is inherent in the wavelet transform. Rotation-invariant transforms such as Fourier-Mellin can be used to overcome that weakness.

Frequency-domain watermarking techniques usually insert the watermark into the mid-frequency subband because they are relative robust and have little impact on the image quality. Watermark embedding by quantizing the distance between coefficients is more robust than that by quantizing the coefficient itself watermark is protected by a private key but also building relations between coefficients significantly discourages an adversary from performing the collage attack [3].

DCT has many important properties that help significantly in image processing, especially in image compression. But does not perform efficiently for binary images characterized by large periods of constant amplitude (low spatial frequencies), followed by brief periods of sharp transitions [7, 13, 16].Discrete wavelet transform is having higher flexibility in comparison to DCT. Wavelet domain is used with semi-fragile watermarks for achieving better robustness [6] .The wavelet transform has a number of advantages over other transforms as it provides a multiresolution description, it allows superior modeling of the human visual system (HVS), the high-resolution sub bands allow easy detection of features such as edges or textured areas in transform domain [19].

In PST the watermark is embedded into the pinned field, which contains the texture information of the original image. This important property of the pinned field provides the scheme with special sensitivity to any texture alteration to the watermarked image. [5] It is thus suitable in applications where texture information is needed. Arnold transform has much to do with the size of image [18].The amount of calculation will be too much if we recover the original image depending on this periodicity, so the application of Arnold transform is limited. When compared to the discrete wavelet transform, the contourlet with their extra feature of directionality yield some improvements and new potentials in image analysis applications [19].

TABLE 1: SEMIFRAGILE WATERMARKING ALGORITHM

S. N.	Author	Insertion domain	Verification Method	PSNR	Applications
1	Bassen Abdul Aziz (2003)	DWT using Tellate watermarking	Benchmarking	44 dB	Real work applications
2	A Piva (2004)	DWT using scrambling	Inverse scrambling	36 dB	Video surveillance and remote sensing images
3	Yuan liang Tang (2004)	DWT domain	Coefficient quantization	33 dB	No specific application suggested
4	Guo rui Feng (2005)	DCT quantization technique	Chaotic permutation	37.04 dB	Still images for multimedia
5	Anthony T. S. (2005)	Pinned sine transform	Normalized cross relation using threshold	40 dB	Satellite remote sensing images.
6	Nadia Baziz (2006)	Contourlet transform	Error Control Coding	36.6 dB	No specific application suggested
7	Kurato maeno (2006)	Wavelet domain	Threshold criteria used	65 dB	All natural, printed and real time images
8	Xiaoping liang (2007)	I W T using reversible semifragile watermark	3rd level I I W T	43.4 dB	Law, commerce, defense journalism
9	Xiaoyun Wu (2007)	IWT domain	Inverse I W T, histogram shifting	43.4 dB	No specific application suggested
10	Li Bo (2008)	D C T domain	Normalized correlation	39 .1 dB	No specific application suggested
11	Zhu Xian (2008)	Arnold Transform	Human visual system	33.61 dB	No specific application suggested
12	Ching Yu Yang (2009)	IWT coefficient bias algorithm	Semifragile reversible data hiding	33.91 dB	No specific application suggested
13	Clara Cruz (2009)	2D- DCT	2 D DCT using R O I & R O E blocks	42.9 dB	No specific application suggested
14	Wen Hsin Chang ((2010)	Tchebichef moment	Human visual system	36.98 dB	No specific application suggested
15	Rafiazullan Chamlawi (2010)	DCT and wavelet transform	Correlation method	42 dB	Video surveillance and remote sensing
16	Yen Shun Chen (2010)	M - R C M encoding algorithm	Reversible contrast mapping watermarking	26. 9 dB	Medical or military images
17	Liu Hui (2010)	Haar wavelet transform	Normalized correlation function	-	No specific application
18	Jordi Serrwa Ruiz (2010)	DWT and vector quantization	IDWT	-	Remote sensing images

Tchebichef moments are suitable for square images and the accuracy of image reconstruction is much better than other continuous moment functions and discrete moment functions [17].

V I Analysis

In the current state of research, it is difficult to affirm which semifragile watermarking approach seems most suitable to ensure an integrity service adapted to images and more general way to multimedia documents. In this paper, we have only identified some algorithms used for image authentication in previous eight years. Many authors have worked on it but how to protect valuable images

and multimedia documents is also in the area of future research.

In literature survey it is obvious that in addition to content preserving and malicious manipulation detection semi fragile watermarking algorithms also have restoration capabilities which are desirable in many applications such as military, medical and satellite images. Some observation are made based on these algorithms are

1. A flexible algorithm that allows user to specify list of desirable and malevolent manipulation algorithm be implemented. As existing algorithms offer tolerance against some specific content preserving manipulations.

2. A combination of D C T and DWT can be

   used to improve performance tradeoff between alterations and can improve P S N R in comparison to DCT.

3. An image with many edges and texture could decrease algorithm’s performance since it is based on differences between adjacent fixed in special domain. So for images having more texture and edges should have lager value of watermark strength.

4. Frequency domain watermarking is preferred over spatial domain as it is more robust against image processing such as image compression.

5. Some methods use threshold to decide about image authenticity. The threshold is supposed to be adapted to a specific image within a specific region so fixed value of threshold may create problem.
6. Discrete moment functions are preferred over continuous moment function because they do not need numerical approximation capability.

7. If there are multiple watermarks used in the application hiding order must be taken into consideration as different watermarks will influence each other.

8. In applications such as space explorations, military investigation and medical diagnosis, where data authentication and original content recovery required at same time reversible technique can be used

VII Conclusion

This paper studies a comprehensive overview of semi fragile based image authentication techniques. In addition to comparison based on image quality matrix, some observation is also suggested to efficiently develop an effective watermarking technique. According to paper, it can be suggested that semi fragile watermarking is a potential approach for authentication in most of practical application. However decision on robustness and fragility can be based on application.

References

[1] Tong, Zheng-ding, “The Survey of Digital Watermarking Based Image Authentication Techniques”, Proc .IEEE International Conference on e-Technology , e-Commerce and e-Service, pp. 1556-1559, 2002.

[2] Archana Tiwari , Manisha Sharma,” Evaluation and Comparison of Semifragile Watermarking Methods for Image Authentication”, In International Journal of computational Intelligence and Information Security, Vol. 2, No. 8,pp 36-42,2011

[3]Bassem Abdel Aziz,” Performance Analysis of a Content Authentication Semifragile Watermark”, In IEEE International Conference, pp. 2055 – 2058, 2003.

[4] Ozgur Ekici “Comparative Evaluation of Semi fragile Watermarking Algorithms”, In Journal of Electronic. Imaging, pp. 209 – 216, 2004.

[5]A Piva, R Caldelli, “Semifragile Watermarking for Still Images Authentication and Content Recovery”, In International Workshop on Image Analysis for Multimedia Interactive Services, pp. 511 – 515, 2004.

[6] Yuan Liang Tang, Ching Ting Chen, “Image Authentication Using Relation Measures of Wavelet Coefficients”, In IEEE International Conference on Signal Processing, pp. 156-159, 2004.

[7] Guo-rui Feng, Ling-ge Jiang, Chen He, “Permutation Based Semi-Fragile Watermark Scheme”, IEICE Transaction Fundamentals lett., vol. E88–A, pp.375-378, 2005.

[8] Authony T. S., “A. Semifragile Pined Sine Transform Watermarking System for Content Authentication of Satellite Image”, In IEEE international conference, pp. 737 – 740, 2005.

[9] Nadia Baziz,” A Novel Image Authentication Scheme Based on Contoured and Error Control Coding”, In IEEE International Symposium on Signal Processing and Information System, pp. 34 – 39, 2006.

[10] Kuarto Maeno, “New Semifragile Image Authentication Techniques Using Random Bias and Nonuniform Quantization”, In IEEE Transactions on Multimedia ,pp. 32 – 45, Vol. 8, No. 1, 2006.

[11] Xiaoping Liang, Weizhao Liang, Wen Zhang, “.Reversible SemiFragile Authentication Watermark”, In. IEEE International Conference on Multimedia and Expo, pp 2122 - 2125, 2007.

[12] Xiaoyun Wu, “Reversible Semi fragile Watermarking Based on Histogram Shifting of Integer Wavelet Coefficients”, In. IEEE International Conference on Signal Processing, pp. 501 – 505, 2007.

[13] Li Bo, “A New Semifragile Watermarking Algorithm for Image Authentication”, In International Conference of World Congress on Intelligent Control and Automation”, pp. 5928 – 5932, 2008.

[14] Zhu Xi'an, “A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform”, In IEEE International Conference on Signal Processing, pp.2217-2220, 2008.

[15] Chang Min Hwang, Ching Yu Yang, P Yen Chang, Wu-Chih Hu, “A Semifragile Reversible Data Hiding by Coefficient Bias Algorithm”, In IEEE International

Conference on Intelligent Information Hiding and Multimedia Signal Processing , vol.1, pp. 132 –139, 2009.

[16] Clara Cruz, Jose Antonio Mendoza, Mariko Nakano ,Miyatake, Hector Perez Meana, "Semi-Fragile Watermarking Based Image Authentication with Recovery Capability", In IEEE International Conference Information Engineering and Computer Science, vol.1, pp. 749 –754, 2009.

[17] Wen Hsin Chang, Long-Wen Chang, "Semi-Fragile Watermarking for Image Authentication, Localization, and Recovery Using Tchebichef Moments", In IEEE International Conference on Security , vol.1, pp. 749 –754, 2010.

[18] Rafiullah Chamlawi,Chang Tsun Li, "Authentication and Recovery of Digital Images Potential Application in Video Surveillance and Remote Sensing", In IEEE International Conference, pp. 26 – 27, 2009.

[19] Liu Hui, HunYuping, "A Wavelet Based Watermarking Scheme with Authentication and Recovery Mechanism", In IEEE International Conference on Electrical and Control Engineering, pp. 323 – 326, 2010.

[20] Jordi Serra Ruiz,David Magias, "D W T and T S V Q Based Semi Fragile Watermarking Scheme for Tampering Detection in Remote Sensing Images", In IEEE International Symposium on Image and Video Technology, pp. 331 – 336. 2010.

[21] Z. Ni, Y.Q Shi, N. Ansari, W. Su, "Reversible Data Hiding" , In IEEE Transaction of Circuits and Systems for Video Technology , vol. 16, pp. 354-361, 2006.

Prof. Archana Tiwari received her B.E degree in Electronics and Telecommunication from Amravati in 1994 and completed her post graduation from GEC Jabalpur in 2005. She is pursuing her PhD from Swami Vivekananda Technical University, Bhilai. She has to her credit, more than 20 papers in various International and National Journals and Conferences. With more than 16 years of teaching and research experience .She is currently serving as Associate professor & head in the department of Electronics and Instrumentation, Chhatrapati Shivaji Institute of Technology, Durg. Her areas of interest include image processing, information security and digital watermarking. She is a life member of Indian Society for Technical Education and Institution of Electronics and Telecommunications engineers. She is member of IEEE also.

Prof. Dr. Manisha Sharma received her B.E degree in Electronics and Telecommunication from GEC Bhopal in 1993 and completed her post graduation from GEC Jabalpur in 1995. She received her PhD degree from Swami Vivekananda Technical University, Bhilai in 2010. She has to her credit, more than 50 papers in various International and National Journals and Conferences. With more than 20 years of teaching and research experience she is currently serving as a professor & head in the department of Electronics and Telecommunication, Bhilai Institute of Technology, Durg. Her areas of interest include, image and video processing, information security and digital watermarking. She is a life fellow of Indian Society for Technical Education and Institution of Electronics and Telecommunications engineers.