Journal of Information Security, **2012, 3, 189-195**
http://dx.doi.org/10.4236/jis.2012.33023 Published Online July 2012 (http://www.SciRP.org/journal/jis)

Comparative Evaluation of Semifragile Watermarking Algorithms for Image Authentication

Archana Tiwari[1], Manisha Sharma[2]
[1]Chhatrapati Shivaji Institute of Technology, Durg, India
[2]Bhilai Institute of Technology, Durg, India
Email: archanatiwari@csitdurg.in, manishasharma1@rediffmail.com

Received January 27, 2012; revised March 15, 2012; accepted April 26, 2012

ABSTRACT

Technology has no limits today; we have lots of software available in the market by which we can alter any image. People usually copies image from the internet and after some changes they claim that these are their own properties. Insuring digital image integrity has therefore become a major issue. Over the past few years, watermarking has emerged as the leading candidate to solve problems of ownership and content authentications for digital multimedia documents. To protect authenticity of images semifragile watermarking is very concerned by researchers because of its important function in multimedia content authentication. The aim of this paper is to present a survey and a comparison of emerging techniques for image authentication using semifragile watermarking. In present paper comprehensive overview of insertion and extraction methods used in different semifragile water marking algorithm are studied using image parameters, potential application, different algorithms are described and focus is on their comparison according to the properties cited above and future directions for developing a better image authentication algorithm are suggested.

Keywords: Image Authentication; Selective Authentication; Content Recovery; Robustness; Semifragile Watermarking; Tamper Detection; PSNR

1. Introduction

Many multimedia authentication systems have been proposed in the last few years for ensuring the integrity and origin of multimedia data such as images. Image authentication is used for verifying the integrity and authenticity of digital images [1]. An image authentication can 1) detect the tampering activities, 2) locate the positions of alternations, and 3) repair the corrupted regions automatically. In general, an image authentication scheme consists of a stamping stage and a verification stage. The stamping stage derives and embeds the authentication code to serve as the attestations for the integrity of the image; the verification stage evaluates the consistence between the authentication code evaluated from a query image and the one calculated in the stamping 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) label based systems, 2) watermarking-based approach. In label based systems, an authenticator is appended to the original signal for integrity verification of the protected signal. The authenticator can be a sensitive function of the signal (e.g. hash) or a set of coarser content features such as block histogram or edge maps. In watermark-based systems, the authenticator is imperceptibly embedded in the signal rather than appended to it, reducing the extra storage requirements of label based methods. Another advantage of watermark based systems is that lossless format conversion of the secured multimedia does not necessarily change its authenticity results.

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 be classified to fragile watermark and semifragile 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 semifragile watermark is developed and widely used in content verifying. Semifragile watermark fragile to malicious modifications while robust to incidental manipulations is drawing many attentions in image authentication. However, watermark security has not received enough attention yet. 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 semifragile watermarking schemes are discussed for image authentication application. In Section 2 challenges in front of image authentication 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 discussion of semifragile algorithms, Section 6 gives analysis and future directions, finally Section 7 presents brief conclusion of paper.

2. Challenges for Selective Image Authentication Techniques

Image authentication can be divided in two groups: strict and selective authentication. Strict authentication is used for applications where no modifications in the image are allowed, whereas selective authentication is used especially when some image processing operations must be tolerated which are image protecting operations uses Selective authentication based on semifragile watermarking to provide some kind of robustness against specific and desired manipulations.

- It is desirable in many applications to design a multipurpose watermarking scheme. There are three extra technical challenges in designing such a system. First, the embedding order of multiple watermarks should be analyzed in detail. Second, how to reduce the effect of the latter embedded watermarks on the former watermarks is a hard problem to solve. Third, the detection of such watermarks should be independent.
- 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 semifragile authentication watermark (RSAW) scheme with features as tamper localization, good perceptual invisibility, detection without requiring explicit knowledge of the original image.
- One design challenge for authentication watermarks is to achieve a good balance between robustness against mild incidental image distortions and fragility to tampering attacks. A authentication watermark should protect the integrity of the image content rather than its exact representation.
- One difficulty these algorithm face is the original host is not available at the receiver side for authentication verification. In practical applications, the original host generally has a much larger magnitude than the allowed legitimate channel distortions. The unavailability of the original host makes it hard to differentiate legitimate distortions from illegitimate ones. This challenge motivates to investigate the semifragile nature of multimedia authentication [5].

3. Prerequisites for Semifragile Watermark-Based Image Authentication Systems

There are certain requirements which are essential for any authentication system; these requirements are discussed here for semifragile watermarking techniques.

- Overemphasis on robustness, questions security issues for authentication applications. A well-designed semifragile system should, therefore, simultaneously address the robustness and fragility objective [5].
- The semifragile authentication system must be secure to intentional tampering. For security, it must be computationally infeasible for the opponent to devise a fraudulent message.
- Given the watermark is an authenticator, embedding must be imperceptible.
- The authentication embedding and verification algorithms must be computationally efficient, especially for real time applications.
- 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.
- 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.
- Asymmetrical algorithm: Contrary to classical security services, an authentication service requires an asymmetrical algorithm.
- Tolerance: The system must tolerate some loss of information and more generally nonmalicious manipulations.

4. Semifragile Authentication Techniques and Domains

In semifragile watermarking to provide image authentication it should tolerate image manipulations while detecting content changes. The authentication watermark used can be fragile to against content changing manipulations while robust to content preserving operations. In this section various techniques available are discussed in brief.

4.1. 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 [6-8].

4.2. Principal Component Analysis (PCA)

Principal component analysis (Principal Component Analysis (PCA)), is a commonly used method based on the variable covariance matrix of information processing, compression and extraction [9].

4.3. 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 [10-13].

4.4. Slant Transform

Slant Transform that has the performance of gradually changing the image signal intensity has been successfully used for image coding in recent years. The basic idea according to the relevance of image signal, the brightness of a line has performance of unchanged or linear gradient [14].

4.5. 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 [15].

4.6. Quantization Technique

In quantization-based schemes, a watermark is embedded by quantizing the host. The structure of the quantizer should provide a compromise among semi fragility, embedding distortion, and security. The basic idea of multistage VQ is to divide the encoding task into successive stages, where the first stage performs a relatively crude quantization of the input vector using a small codebook. Then, a second-stage quantizer operates on the error vector between the original and quantized first-stage output. The quantized error vector then provides a second approximation to the original input vector thereby leading to a refined or more accurate representation of the input. A third-stage quantizer may then be used to quantize the second-stage error to provide a further refinement and so on [16,17].

4.7. 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 [18].

4.8. 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 [3,19,20].

4.9. 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 [21].

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

of PSNR is average PSNR of different images used in paper.

5. Discussion of Different Semifragile Watermarking Methods

According to this summary **Table 1**, algorithms performances are similar. The properties of each group of methods are provided with references to algorithms. In fact, most of algorithms offer acceptable detection and localization of image manipulations while restoration performances still need to be improved. Semifragile algorithms show good results for detecting and locating malevolent manipulations while providing acceptable reconstruction performances. Unfortunately, their tolerance against desired manipulations includes mainly compression, noise addition and rotation by small angles, whereas, many of the desired manipulations need to be tolerated in practice.

Tellate watermarks are semifragile watermarks that can survive small distortions and minor transformations

Table 1. Semifragile watermarking algorithms.

S. N.	Author	Insertion Domain	Control Area	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	128 × 128 bits	Inverse scrambling	36 dB	Video surveillance and remote sensing images
3	Yuan liang Tang (2004)	DWT domain	8 × 8 block	Coefficient quantization	33 dB	No specific application suggested
4	Guo rui Feng (2005)	DCT quantization technique	64 × 64 bits	Chaotic permutation	37.04 dB	Still images for multimedia
5	Anthony T. S. (2005)	Pinned sine transform	8 × 8 block	Normalized cross relation using threshold	40 dB	Satellite remote sensing images.
7	Zhe-Ming Lu(2005)	DWT and DCT	128 × 128 bits	Vector quantization(VQ)	30:553 dB	No specific application suggested
6	Nadia Baziz (2006)	Contourlet transform	5128 × 128 bits	Error Control Coding	36.6 dB	No specific application suggested
8	Kurato maeno (2006)	Wavelet domain	5 × 31 integer	Threshold criteria used	65 dB	All natural, printed and real time images
9	Xiaoping liang (2007)	I W T using reversible semifragile watermark	-	3rd level I I W T	43.4 dB	Law, commerce, defense journalism
10	Xiaoyun Wu (2007)	IWT domain	128 × 128 bits	Inverse I W T, histogram shifting	43.4 dB	No specific application suggested
11	Li Bo (2008)	D C T domain	8 × 8 block	Normalized correlation	39 .1 dB	No specific application suggested
12	Zhu Xian (2008)	Arnold Transform	-	Human visual system	33.61 dB	No specific application suggested
13	Jean-Philippe Boyer (2008)	DCT transform	8 × 8 block	Scalar DC-QIM scheme	43 dB	
14	Ching Yu Yang (2009)	IWT coefficient bias algorithm	4× 4 block	Semifragile reversible data hiding	33.91 dB	No specific application suggested
15	Chuhong Fei (2009)	DCT	8 × 8 block	IDCT	42.9 dB	No specific application suggested
16	Wen Hsin Chang (2010)	Tchebichef moment		Human visual system	36.98 dB	No specific application suggested
17	Rafiazullan Chamlawi (2010)	DCT and wavelet transform	-	Correlation method	42 dB	Video surveillance and remote sensing
18	Li Yaquin (2010)	Principal Component analysis using Wavelet transform	-	Correlation coefficient	26. 9 dB	Copyright and authentication
19	Jordi Serrwa Ruiz (2010)	DWT and vector quantization	8 × 8 block	IDWT	61.37 dB	Remote sensing images
20	Hongwen Lin (2011)	LSB using quantization	2 × 2 block	Correlation	38.58 dB	Color image authentication
21	Rui Bao (2011)	Slant transform and channel coding	30 × 30 integer	Inverse slant transform	37.31 dB	No specific application suggested

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 [10,11,22]. Discrete wavelet transform is having higher flexibility in comparison to DCT. Wavelet domain is used with semifragile watermarks for achieving better robustness [20]. 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 [9].

The VQ-based watermarking algorithm can reduce the amount of the data transmitted [17].

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 [12].

PCA is a widely used in many areas like pattern recognition, quantitative analysis of chemical composition, multi-component determines the number of components, the dynamics of the reaction mechanism, etc. [9].

Slant Transformation has the property that intermediate frequency coefficients unchanged when host image suffered non-malicious tempered. So it is often used in image processing [14].

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 [9].

The quantization based embedding method outperforms spread spectrum in the tradeoff between algorithm robustness and fragility [23].

6. Analysis and Future Directions

It can be inferred from **Table 1**, almost all algorithm do well on detecting and substitution and have low rate of prone to attacks and they offer acceptable detection and localization of image manipulation while restoration performances still need to be improved, All algorithms can detect manipulation to certain content preserving operation is application specific. To study their relative performance one should consider following points.

1) The tamper indication must be statistically sound.

2) It should be possible to integrate the tamper over arbitrary region on images It should be robust to significant subset of signal processing attacks [4].

Some observation are made based on these algorithms are

- 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.
- A combination of DCT and DWT can be used to improve performance tradeoff between alterations and can improve PSNR in comparison to DCT.
- 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 strength should have lager value of watermark.
- Frequency domain watermarking is preferred over spatial domain as it is more robust against image processing such as image compression.
- 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.
- Discrete moment functions are preferred over continuous moment function because they do not numerical approximation capability.
- If there are multiple watermarks used in the application hiding order must be taken into consideration as different watermarks will influence each other. How to analyze the embedding order in general sense is a problem to solve.
- 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 [24].
- For each authentication algorithm legitimate and illegitimate transition region is application dependent

and that the semifragile methodology should employ this information during the design phase.

- To enhance the watermark invisibility, one can also introduce some additional local distortion constraint provided by a human visual system (HVS).
- In a number of sensitive medical and military applications where perceptual integrity of even fine spatial detail has utmost importance, aggressive lossy compression can be considered as a malicious attack that causes loss of vital information. In such a scenario, it is desirable that watermarks: 1) are robust against mild compression; 2) distinguish manipulated regions from other areas; and 3) vanish under aggressive compression to indicate the loss of significant visual content [25].

7. Conclusion

In present paper various semifragile watermarking algorithm are studied to verify image authenticity. In addition to comparison based on image quality matrix, some observation is also suggested to efficiently develop an efficient semifragile watermarking algorithm for image authentication. As content preserving operations are specific to application, a practical algorithm that allows users to specify list of desirable and malicious manipulation can be developed. Moreover, restoration capabilities need additional improvements.

REFERENCES

[1] I. J. Cox and M. I. Miller, "The First 50 Years of Electronic Watermarking," *Journal of Applied Signal Processing*, Vol. 2, 2002, pp. 126-132. doi:10.1155/S1110865702000525

[2] A. Tiwari and M. Sharma, "Evaluation and Comparison of Semifragile Watermarking Methods for Image Authentication," *International Journal of Computational Intelligence and Information Security*, Vol. 2, No. 8, 2011, pp. 36-42.

[3] B. A. Aziz, "Performance Analysis of a Content Authentication Semifragile Watermark," *Proceedings of IEEE International Conference*, Vol. 3, 2003, pp. 2055-2058.

[4] O. Ekici, "Comparative Evaluation of Semi Fragile Watermarking Algorithms," *Journal of Electronic Imaging*, Vol. 13, No. 1, 2004, pp. 209-216. doi:10.1117/1.1633285

[5] C. H. Fei and H. Kwong, "A Hypothesis Testing Approach to Semifragile Watermark-Based Authentication," *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 2, 2009, pp. 479-492.

[6] X. P. Liang, W. Z. Liang and W. Zhang, "Reversible SemiFragile Authentication Watermark," *Proceedings of IEEE International Conference on Multimedia and Expo*, 2-5 July 2007, pp. 2122-2125.

[7] X. Y. Wu, "Reversible Semi fragile Watermarking Based on Histogram Shifting of Integer Wavelet Coefficients," *Proceedings of IEEE International Conference on Signal Processing*, 21-23 February 2007, pp. 501-505.

[8] C. M. Hwang, C. Y. Yang, P. Y. Chang and W.-C. Hu, "A Semifragile Reversible Data Hiding by Coefficient Bias Algorithm," *Proceedings of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Vol. 1, 2009, pp. 132-139.

[9] Y. Q. Li, "Semifragile Watermarking Algorithm Based on Bi Watermarking Technology," *Proceeding of IEEE International Conference on Computer Applications and System Modelling*, Vol. 15, 2010, pp. 138-142.

[10] G. R. Feng, L. G. Jiang and C. He, "Permutation Based Semi-Fragile Watermark Scheme," *IEICE Transaction Fundamentals*, Vol. E88-A, 2005, pp. 375-378.

[11] B. Li, "A New Semifragile Watermarking Algorithm for Image Authentication," *Proceedings of International Conference of World Congress on Intelligent Control and Automation*, 25-27 June 2008, pp. 5928-5932.

[12] R. Chamlawi and C. T. Li, "Authentication and Recovery of Digital Images Potential Application in Video Surveillance and Remote Sensing," *Proceeding of IEEE International Conference*, 10-14 January 2009, pp. 26-27.

[13] J. S. Ruiz and D. Magias, "DWT and TSVQ Based Semi Fragile Watermarking Scheme for Tampering Detection in Remote Sensing Images," *Proceeding of IEEE International Symposium on Image and Video Technology*, 14-17 November 2010, pp. 331-336.

[14] R. Bao, T. Q. Zhang, *et al*., "Semi-Fragile Watermarking Algorithm of Color Image Based on Slant Transform and Channel Coding," *Proceeding of IEEE International Conference on Image and Signal Processing*, Vol. 2, 2011, pp. 1039-1043.

[15] N. Baziz, "A Novel Image Authentication Scheme Based on Contoured and Error Control Coding," *Proceedings of IEEE International Symposium on Signal Processing and Information System*, 2006, pp. 34-39.

[16] K. Maeno, "New Semifragile Image Authentication Techniques Using Random Bias and Nonuniform Quantization," *IEEE Transactions on Multimedia*, Vol. 8, No. 1, 2006, pp. 32-45. doi:10.1109/TMM.2005.861293

[17] Z.-M. Lu and D.-G. Xu, "Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization," *IEEE Transactions on Image Processing*, Vol. 14, No. 6, 2005, pp. 822-832. doi:10.1109/TIP.2005.847324

[18] T. S. Authony, "A Semifragile Pined Sine Transform Watermarking System for Content Authentication of Satellite Image," *Proceedings of IEEE International Conference*, 2005, pp. 737-740.

[19] A. Piva and R. Caldelli, "Semifragile Watermarking for Still Images Authentication and Content Recovery," *International Workshop on Image Analysis for Multimedia Interactive Services*, 21-23 April 2004, pp. 511-515.

[20] Y. L. Tang and C. T. Chen, "Image Authentication Using Relation Measures of Wavelet Coefficients," *Proceedings of IEEE International Conference on Signal Processing*, 2004, pp. 156-159.

[21] X. A. Zhu, "A Semi-Fragile Digital Watermarking Algo-

rithm in Wavelet Transform Domain Based on Arnold Transform," *Proceedings of IEEE International Conference on Signal Processing*, 26-29 October 2008, pp. 2217-2220.

[22] H. W. Lin and S. Q. Yang, "Watermark Algorithm for Color Image Authentication and Restoration," *Proceedings of IEEE International Conference on Electronic and Mechanical Engineering and Information Technology*, 2011, pp. 2773-2776.

[23] J.-P. Boyer, P. Duhamel and J. Blanc-Talon, "Scalar DC-QIM for Semifragile Authentication," *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 4, 2008, pp. 776-782. doi:10.1109/TIFS.2008.2004285

[24] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible Data Hiding," *IEEE Transaction of Circuits and Systems for Video Technology*, Vol. 16, 2006, pp. 354-361. doi:10.1109/TCSVT.2006.869964

[25] O. Altun, G. Sharma and M. Bocko, "A Set Theoretic Framework for Watermarking and Its Applications to Semifragile Tamper Detection," *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 4, 2006, pp. 479-492. doi:10.1109/TIFS.2006.885018

