Performance Comparison of Semifragile Watermarking Methods for Image Authentication

Archana Tiwari , Dr. Manisha Sharma

Abstract- Data authentication is one of the primary requisites in present day communication systems. In image processing, data authentication is implemented by using watermarking techniques. The specific interest in semifragile watermarking algorithms arises from the multitude of practical and commercial applications, where content needs to be strictly protected, 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. Semifragile watermarks are more robust and less sensitive to classical user modifications such as JPEG compression, content-preserving operations and content altering manipulations while sensitive to content integrity verification. In present paper the performance of seven semifragile watermarking methods are compared in terms of their PSNR, robustness and temper sensitivity properties.

Key words: semi-fragile watermarking, PSNR, Robustness, Tamper detection.

1 INTRODUCTION

To facilitate the authentication and content-integrity verification for multimedia applications where content-preserving operations are a common practice, semi-fragile watermarking scheme have been proposed in the last few years [1]. This class of watermarks is intended to be fragile only when the manipulations on the watermarked media are deemed malicious by the schemes [2]. Semifragile watermarking is a potential solution to the image content authentication problem which seeks to verify that the content of the multimedia has not been modified by any of a predefined set of illegitimate distortions, while allowing modification by legitimate distortions.

To be an effective image authentication system, it must satisfy the following criteria [8]:

a. Sensitivity: The system must be sensitive to malicious manipulations.

b. Tolerance: The system must tolerate some loss of information and more generally non-malicious manipulations.

c. Localization of altered regions: The system should be able to locate precisely any malicious alteration made to the image and verify other areas as authentic.

d. 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.

In this work focus is on different authentication based semifragile watermarking techniques, thus paper is organized as follows: Section 2 discusses methods of comparison used for comparing different algorithms, Section 3 gives details on attacks and their countermeasures, Section 4 outlines different semifragile watermarking algorithms and Sections 5 & 6 presents analysis and conclusion.

2 Methods for Comparison

The semifragile watermarking method should be moderately robust to discriminate between malicious manipulations, such as the addition or removal of a significant element of the image, and global operations preserving the semantic content of the image. The semifragile watermarking methods should be moderately robust to differentiate between malicious and non malicious attacks. However, the line of demarcation between the benign and malicious attacks is application and document dependent [3]. In this comparison for given algorithms values of PSNR(Peak Signal to Noise Ratio), robustness and tamper sensitivity properties are given, no specific application context is considered so depending on application particular

methods can be used .Analysis of available watermarking scheme is done on basis of-

I. PSNR: High value of PSNR shows the watermarked image has a better quality, the difference between the original image and the watermarked image is imperceptible.
II. Robustness: Robustness depends on the information capacity of the watermark, the watermark strength / visibility, and the detection statistics (threshold). Robustness is also influenced by the choice of images (size, content, color depth). The minimal required robustness is highly application dependent. It may not make sense to compare techniques intended for different applications.
III. Tamper detection- Tamper detection aims to monitor modifications on digital documents where a distinction needs to be made between innocent and malicious alterations. When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the data.

IV. Recovery of content-Lossless recovery of content especially reversible recovery is taken into consideration.
The main content-altering manipulations that must generate tamper alarm, hence, the non permissible alterations, are the following: Image forgeries intended to remove, substitute, or insert objects in the image. Image manipulations that modify the geometry of objects such as their rotation, flipping, translation, and scaling or image manipulations that change the appearance of objects such as color, shade, shadow manipulation, etc.

3 Attacks and Countermeasures

The aim of malicious attacks to authentication system is not to eliminate the watermarks, but to invalidate them-

[I]The attacker may bring a known valid watermark from a watermarked image as the mark for another. Then the detector regards it as authentic. This type of attack can also be performed on the same image: the watermark is first removed, then the image is modified, and finally the watermarkis embedded again. One can use the content-based or reversible watermarking algorithm to resist the attack.

[II] The attacker can modify the marked image without affecting the embedded mark. For example, if the watermark is embedded in the LSB bit plane of an image, the attacker may attempt to modify the image without disturbing any LSBs. One can choose the transform domain authentication scheme, which has higher security than spatial one. In many quantization-based authentication algorithms, the value of extracted watermark *is* determined by the quantization interval of marked image's coefficient. If the attacker knows the quantization interval, he can modify the image coefficients without changing the value of extracted watermark. To solve the problem better, the HVS model can be used to' determine the quantization interval.

[III] The attacker may attempt to completely destroy the mark by adding random noise, which maybe the most common type of attack. Improving the robustness of semi-fragile watermark is the only measure so far, but fortunately, if the attacker adds excessive noise, the image's quality will decrease too much and lost the commercial value consequently [4].

Table 1 discusses different characteristics of semi-fragile watermarking methods and their attack counteracting capacity.

Table 1: Performance analysis of semifragile watermarking methods

Author	Robust-ness	Tamper Detection	Content Recovery	Attacks
Guo Rui Feng	21%	Yes 10×10 block	…….	JPEG compression
Anthony T S	90%	Yes 10×10 block	Possible	Cutting, pasting, noise attacks, JPEG compression
Hyunho keng	60%	Yes 8×8 block	……	JPEG compression, Sharpening, Low pass filtering Median filtering, Salt Pepper noise, Gaussian noise Histogram equalization,
Xiaoping Liang	50%	Yes 3×3 window	Reversible	JPEG compression, Gaussian noise, filtering Content altering , content preserving operations,
Xiaoyun Wu	40%	Yes 4×4 block	Reversible	JPEG compression, Cutting, Displacement
Zhu Xian	40%	Yes	Possible	JPEG compression, Cutting, pepper noise, Gaussian noise, displacement.
Ching Yu Yang	……..	Yes 4×4 water-mark	Reversible	JPEG 2000, JPEG inverting, brightness

4 Semifragile Watermarking Algorithms

1. Guo rui Feng [2005]:- The keys of the scheme are how to devise the algorithm of permutation and maintenance of the security. In order to achieve these goals, chaotic sequences to permute the host image are suggested [5].

2. Anthony T. S. [2005]:- Watermark is embedded into pinned field which contains texture information of original image. This important properly provides the scheme with special sensitivity to any texture alteration to biomedical image [6].

3. Hyunho King [2006]: - Watermark is inserted in discrete wavelet transform domain and linear correlation is used to detect the presence or absence of the watermark on a block by block basis. Each block of attacked image is divided into low and high frequency coefficient [7].

4. Xiaoping Liang [2007]: - New RSAW (Reversible semi-fragile authentication watermark) scheme is proposed by explaining some characteristics of IWT and multi level embedding. This scheme provides tamper discerning in spatial region from frequency region and tamper localization [8].

5. Xiasyan Wu [2007]: Original image is preprocessed by histogram modification; four level IWT is performed on preprocessed image. A binary, watermark is embedded in LLG sub band for tamper localization and recovery information are embedded in high frequency of IWT domain[9].

6. Zhu Xian [2008]:- Copyright information is firstly made chaos by Arnold transform and then self adaptive embedded into host image in different intensity in wavelet transform domain based on calculating the adjacent wavelet coefficient by exploiting characteristics of Human visual system [10].

7. Ching Yu Yang [2009]: Effective lossless data hiding algorithm based on integer wavelet transform, a secret message is embedded in the three high subbands of IWT domain by the proposed coefficient-bias algorithm [11].

Table 2 shows the values of PSNR of the images recovered after the authenticated image have been JPEG compressed with respect to the image extracted when the authenticated images have undergone no compression as given in various algorithms.

Table 2 shows the values of PSNR of the images recovered after the authenticated image have been JPEG compressed with respect to the image extracted when the authenticated images have undergone no compression as given in various algorithms.

Table 2: PSNR of different images

Author	PSNR OF IMAGES									
	Baboon	Lena	Boat	Gold hill	Barbara	Pentagon	Pills	Pepper	Camera-man	Pyra-ra-mid
Guo Rui Feng	37.39 dB	37.40 dB			38.12dB	37.78 dB		36.9dB		38 dB
Anthony T S		38.41 dB	39 dB		37.9 dB		37.8 9 dB		36.9 dB	38 dB
Hyunho keng	41.7 dB	42 dB		40.9 dB		43 dB			41.9 dB	42.2 dB
Xiaoping Liang	37.38 dB	37.98 dB		38.15 dB	38.35 dB	38.14dB	38.2 1 dB	38.01 dB	33.61 dB	
Xiaoyun Wu	44.48 dB	43.42 dB			43.45 dB	43.46dB		43.45 dB		
Zhu Xian	33.83 dB	33.9 dB	34.23 dB		34 dB		34.3 dB		33.61 dB	
Ching Yu Yang	30.64 dB			29.13 dB		29.13 dB		30.12 dB		30.1 dB

5 Analysis And Discussion

This paper presents an investigation of existing semifragile watermarking techniques. Present work is an extension of work done by Ozgur Ekici [3] which covers the research done in the area of semifragile watermarking till year 2004. On comparing authentication based watermarking methods it is observed that, the information carried by the watermark can be accessed using a detection algorithm provided the secret key is known. The various attacks are applied to the images in various methods of semifragile watermarking, their experimental results show that the algorithm has robustness resisting conventional compression such as JPEG common image processing operations, such as filtering, lossy compression, noise adding, histogram manipulation, and various geometrical transformations, as a result of achieving a good semi-fragile watermarking algorithm. In some cases it is possible to trade robustness for security; techniques robust to a wider spectrum of image deformations may not have the best robustness for specific image deformations. Another important attribute of watermarking is PSNR; high value of it is desirable

for higher quality of image. The tamper detection block size should be flexible, as the attack size can vary from a line consisting of a few tens of pixels long to the entire image plane itself. Tamper proofing and hence tampers detection is crucial problem, to know clear demarcation between malicious manipulations and original content of image. For lossless recovery of images especially reversible digital watermarking techniques have been individuated so far to be adopted in application scenarios where data authentication and original content recovery were required at the same time[12]. In some applications, it is important that the embedding process be as fast and simple as possible (watermarking images in digital cameras for tamper detection) while the extraction can be more time consuming. In other applications, the speed of extraction is absolutely crucial (e.g., extracting captions from digital video [13].
To develop a fair method for comparing robustness of watermarking techniques, one will have to address the some difficult issues, as listed in table 3.

Table 3 Robustness vs. parameter

Operation	Parameter
JPEG compression	Quality factor
Blurring	Number of operations/kernel
Noise adding	Noise amplitude (SNR)
Median filtering	Kernel size
Histogram equalization	N/A

The following comments can be made on performance of semifragile method
1. Guo rui Feng- This algorithm preserves effective permuting performance and high security simultaneously.
2. Anthony T. S. - This algorithm is used for authentication of satellite images. Pinned field provide special sensitivity to any texture alteration to the biomedical images.
3. Hyunho King-The objective of this algorithm is to get a low number of non-detected blocks in non-malicious attacks and a high numbers of non-detected blocks in malicious attacks.

4. Xiaoping Liang- The proposed RSAW scheme is effective in a sense, and is desired in an integrated and powerful image authentication system, and can be applied in law, commence, defense and journalism.

5. Xiasyan Wu-This scheme is robust to JPEG lossy compression at a lower quality factor. The embedding distortion is small and it guarantees better visual quality of the marked image.

6. Zhu Xian-The algorithm has robustness resisting conventional compression such as JPEG and fragile resisting hostility attacks and falsification, as a result of achieving a good semi-fragile watermarking algorithm.

7. Ching Yu Yang- A semi-fragile reversible data hiding method is, developed which is capable of providing a larger hidden space and a better PSNR while the resulting perceptual quality.

6 Conclusions

In this work seven algorithms are compared on the basis of PSNR, robustness and temper-sensitivity properties. Then, given an application scenario with specific PSNR, robustness and tamper-sensitivity properties, in principle it could be possible to select the adequate algorithm. The comparative analysis of semifragile watermarking methods shows that semifragile watermarking is a potential approach for authentication. Semi-fragile watermarking method that can resist content-preserving operations while being sensitive to content-altering manipulations is more practicable for content integrity verification.

7 References

[1] R. G. Van Schyndel, A. Z. Tirkel and C. F. Osborne, "A Digital Watermark", In Proceedings of IEEE International Conference on Image Processing, Vol. 2, pp 86-90, 1994.
[2] I. J. Cox, Matt Miller, "Electronic Watermarking The First 50 years", In Proceeding of IEEE Workshop on Multimedia Signal Processing, pp. 225 – 230, 2001.
[3] Ozgur Ekici., Bulent Sankur., "Comparative Evaluation of Semi-Fragile Watermarking Algorithm", In Journal of Electronic Imaging, Vol. 13, pp. 209-216, 2004.

[4] Tong , Zheng-ding, "The Survey of Digital Watermarking Based Image Authentication Techniques", In Proceedings of IEEE International Conference on Signal Processing , pp. 1556-1559, 2002.
[5] Guo-rui Feng, Ling-ge Jiang, Chen He, "Permutation Based Semi-Fragile Watermark Scheme", In Journal of IEICE Transaction Fundamentals, Vol. E88–A, pp. 375-378, 2005.
[6] Anthony T. S. Ho, Xunzhan Zhu "A Semi-Fragile Pinned Sine Transform Watermarking System for Content Authentication of Satellite Images", In Proceeding of IEEE International Conference, pp 737-740, 2005.
[7] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "Detecting Malicious Attacks Using Semi-Fragile Watermark Based on Visual Model", In Proceeding of IEEE International Conference and Computer Society, pp 10-14, 2006.
[8] Xiaoping Liang, Weizhao Liang, Wen Zhang, ".Reversible Semi-Fragile Authentication Watermark", In Proceeding of IEEE International Conference on Multimedia and Expo, pp 2122 - 2125, 2007.
[9] Xiaoyun Wu, "Reversible Semifragile Watermarking Based on Histogram Shifting of Integer Wavelet Coefficients", In Proceedings of IEEE International Conference on Signal Processing, pp. 501 – 505, 2007.

[10] Zhu Xi'an, " A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform", In Proceedings of IEEE International Conference on Signal Processing,
pp.2217, 2008.
[11] Chang Min Hwang, Ching Yu Yang, P Yen Chang, Wu-Chih Hu, "A Semifragile Reversible Data Hiding by Coefficient Bias Algorithm", In Proceedingsf IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Vol.1, pp. 132 –139, 2009.

[12] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform,", In Journal of IEEE on Circuits and Systems for Video Technology, Vol. 16, pp. 1294-1300, 2006.
[13] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding" In Journal of IEEE on Circuits and Systems for Video Technology, Vol. 16, pp. 354-361, 2006.

Authors

1.Mrs Archana Tiwari-Associate Professor and HOD Electronics and Instrumentation,Chhatrapati Shivaji Institute of Technology, Durg

Email:archanatiwari@csitdurg.in

2.Dr Manisha Sharma- Professor and HOD Electronics and telecommunication, Bhilai Institute of Technology, Durg

Email: manishasharma1@rediffmail.com