International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 12 • Issue 1 pp. 82-87 June 2018 - Dec 2018 www.csjournals.com

Performance Analysis of Fragile and Semi-Fragile Watermarking Systems for Image Authentication and Tampering

Hiral Patel
Sutex Bank College of Computer Applications & Science, Veer Narmad South Gujarat University, Surat, India

Abstract

Digital images are highly modified by unauthorised users due to the availability of advanced editing tools. To address this challenge, watermarking techniques can be used. Fragile and Semi-fragile watermarking techniques are frequently used by researchers for authentication, tamper detection, localization, and in certain cases, self-recovery. This paper provides a comparative analysis of fragile and semi-fragile watermarking methods based on their embedding domains, image types, robustness, imperceptibility, and capability to differentiate between malicious and non-malicious attacks. The study concludes that fragile watermarking systems offer higher sensitivity to tampering, whereas semi-fragile watermarking provides practical robustness in real-world scenarios.

Keywords: *Fragile Watermarking, Semi-fragile Watermarking, Authentication, Tamper Detection, Tamper Localization, Tamper Recovery*

Introduction

The use of multimedia applications and online platforms has increased the need for reliable techniques to protect the authenticity and integrity of digital images. Traditional cryptographic approaches ensure data integrity but fail to localize tampered regions or recover the original image content. Digital watermarking has effective solution for image authentication, tamper detection and recovery. Watermarking methods are classified into robust, fragile and semi-fragile watermarking systems. Robust watermarking system focuses on Copyright protection where as Fragile and Semi-fragile watermarking systems are used for integrity. Fragile watermarking is highly sensitive to modifications and is suitable for strict authentication whereas Semi-fragile watermarking tolerates minor, non-malicious distortions like compression, salt & pepper noise while detecting malicious tampering.

This paper focuses on in-depth reviews and comparative analysis of fragile and semi-fragile watermarking systems.

Fragile Watermarking:

Fragile watermarking is a digital watermarking technique mainly designed for authentication and integrity verification of images. Fragile watermarking is intentionally sensitive—any slight modification to the image alters or destroys the watermark. This property makes it highly effective for applications such as tamper detection, localization of modifications, and limited content recovery. Its main advantage lies in its simplicity and high sensitivity, though it cannot distinguish between malicious and non-malicious attacks.

International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 12 • Issue 1 pp. 82-87 June 2018 - Dec 2018 www.csjournals.com

Many Researchers have been worked with Fragile Watermarking System for solving tampering issue. The detailed reviews are discussed in Table1.

Table 1 Reviews for Fragile Watermarking System

Ref No	Type	Image	Blind	Tamper Detection, Localization	Tamper Recovery	Watermark generation	Security	Embedding	Malicious Attacks
1	Fragile	Gray Scale	Blind	✓		Cover	Scramble	Spatial	Copy move attack, Text addition, Object removal, image splicing
2	Fragile	Color	Blind	✓	✓	Feature Extraction		Spatial	Cropping
3	Fragile	Color	Blind	✓	✓	Feature Extraction		Spatial	Collage
4	Fragile	Gray Scale	Blind	✓	✓	Feature Extraction	Scramble	Spatial	Copy move attack, Image splicing
5	Fragile	Gray Scale	Blind	✓	✓	Feature Extraction	Scramble	Spatial	Cropping, Image splicing
6	Fragile	Color	Blind	✓	✓	Feature Extraction		Spatial	Image Splicing
7	Fragile	Gray Scale	Blind	✓		Cover	Scramble	Spatial	Copy move attack, Text addition, Object removal, image splicing
8	Fragile	Gray Scale	Blind	✓		Cover		Spatial	Copy move attack, Text addition, Object removal, Collage, I mage splicing
9	Fragile	Color	Blind	✓		Cover		Spatial	
10	Fragile	Gray Scale	Blind	✓	✓	Feature Extraction	Scramble	Spatial	Object removal, Cropping, Image splicing

As per the Table1, majority of researchers who worked with fragile watermarking have worked with Blind watermarking system. The research for gray scale as well as color images are done for solving tampering issue. Watermark generation is done either by cover-based embedding or through feature extraction. Features are extracted using SVD, LWT, Halftoning, by applying non-overlapping blocking and then performing operations like minimum, maximum, mean etc. on each block. For providing more security, scrambling is applied using Arnold Transform, Permutation and shifting top to bottom rows and columns. Embedding is consistently performed in the spatial domain where mainly LSB method is applied. While fragile watermarks are highly sensitive, making them effective in detecting even small modifications, they are tested against a range of malicious attacks such as copy-move, cropping, collage, splicing, object removal, and text addition, showing their effectiveness for strict authentication and tamper localization but with

limited recovery capability. Non-malicious attacks like Compression, Salt & Pepper, Blur, sharpen image, these systems treat same as malicious attacks which is the limitation for Fragile system.

Semi-Fragile Watermarking:

Semi-fragile watermarking is a digital watermarking technique designed to balance sensitivity and robustness, making it suitable for content authentication in multimedia applications. Unlike fragile watermarking, which breaks under any modification, semi-fragile watermarking can tolerate non-malicious operations such as compression, salt & pepper, scaling while still detecting and localizing malicious tampering like object removal, splicing, or text addition. Semi-fragile watermarking offers a practical solution for authentication and tamper detection where content integrity must be ensured without rejecting acceptable image manipulations.

Many Researchers have been worked with Fragile Watermarking System for solving tampering issue. The detailed reviews are discussed in Table2.

Table 2 Reviews for Semi-Fragile Watermarking System

Ref No	Type	Image	Blind	Tamper Detection, Localization	Tamper Recovery	Watermark generation	Security	Embedding	Malicious Attacks
11	Semi-Fragile	Gray Scale	Blind	✓		Feature Extraction	Scramble	Frequency	
12	Semi-Fragile	Gray Scale	Blind	✓		Feature Extraction		Frequency	Text addition, Object removal, Image Splicing
13	Semi-Fragile	Gray Scale	Non-Blind	✓		Cover		Frequency	
14	Semi-Fragile	Gray Scale	Blind	✓		Feature Extraction	Scramble	Frequency	Copy move attack, Text addition, Image splicing
15	Semi-Fragile	Gray Scale	Blind	✓	✓	Feature Extraction	Scramble	Frequency	Object removal, Image splicing
16	Semi-Fragile	Gray Scale	Non-Blind	✓		Cover	Scramble	Frequency	
17	Semi-Fragile	Gray Scale	Blind	✓	✓	Feature Extraction		Frequency	Copy move attack
18	Semi-Fragile	Gray Scale	Blind	✓	✓	Feature Extraction		Frequency	Object removal, Image splicing
19	Semi-Fragile	Gray Scale	Non-Blind	✓		Feature Extraction		Frequency	
20	Semi-Fragile	Color	Blind	✓		Feature Extraction		Frequency	
21	Semi-Fragile	Gray Scale	Blind	✓		Cover		Frequency	Text addition, Cropping

As per the Table2, majority of researchers who worked with semi-fragile watermarking have worked with Blind as well as Non-blind watermarking system. Majority of researchers have focused on Gray-scale image tampering issue. Watermark generation is done either by cover-based embedding or through feature extraction. Features are extracted using different methods like DCT, DWT, Canny and Sobel edge detection techniques, SVD, PCA, Halftoning etc. For providing more security, scrambling is applied using Arnold Transform, Permutation and shifting top to bottom rows and columns. Embedding is consistently performed in the frequency domain where DCT, DWT, IWT as well as Hybrid methos are applied. Semi-fragile methods are designed not only for tamper detection and localization but in some cases also support tamper recovery. They are particularly effective in distinguishing non-malicious changes from malicious ones and have been tested against a variety of attacks such as copy-move, text addition, cropping, object removal, and image splicing. These techniques are robust for non-malicious attacks like compression, salt & pepper, sharpen, blur, scaling. Compared to fragile watermarking, these schemes offer greater robustness and reliability.

Comparative Analysis:

As per the literature reviews, the comparative analysis between fragile and semi-fragile watermarking systems are discussed in Table3.

Table 3Comparison between Fragile & Semi-fragile Watermarking

Criteria	**Fragile Watermarking**	**Semi-Fragile Watermarking**
Purpose	Authentication, tamper detection, localization, limited recovery	Authentication, tamper detection, localization, benign vs malicious differentiation, partial recovery
Image Support	Gray scale, Color	Gray scale, Color
Watermark Generation	Separate watermark image, feature-based (SVD, LWT, halftoning)	Feature-based (DCT, DWT, SVD, PCA, edge detection)
Embedding Domain	Spatial (LSB)	Frequency (DCT, DWT, Hybrid)
Security Mechanism	Scrambling (Arnold, permutation, row/col shifting)	Scrambling (Arnold, Logistic map)
Blindness	Mostly blind	Both blind and non-blind
Robustness	Fails to differentiate malicious & non-malicious attacks	Differentiates malicious & non-malicious attacks
Attacks Tested	Copy-move, object removal, collage, splicing, cropping	Copy-move, text addition, cropping, object removal, splicing
Complexity	Simpler to implement	Higher complexity
Tamper Recovery	Provides limited or no tamper recovery	Some methods support partial recovery of tampered regions.

Fragile watermarking is mainly used for strict authentication and tamper detection, offering high sensitivity where even minor changes break the watermark, making it simple but unable to differentiate between malicious and benign modifications. It typically works on grayscale and color images using spatial domain embedding (LSB) with scrambling for security, providing high imperceptibility (PSNR) but limited recovery. In contrast, semi-fragile watermarking is more advanced, designed to not only detect and localize tampering but also distinguish between non-malicious operations and malicious attacks. It usually operates in the frequency domain (DCT, DWT, hybrid) with stronger security mechanisms (Arnold transform, chaotic maps), feature-based watermark generation, and both blind/non-blind approaches. While it offers moderate imperceptibility with partial recovery and robustness against benign changes, its implementation is more complex compared to fragile watermarking.

Conclusion:

Fragile and semi-fragile watermarking systems complement each other in the domain of image authentication and tampering Issues. Fragile watermarking provides high sensitivity to any modification, making it useful for applications requiring strict authentication but limited robustness. Semi-fragile watermarking, although more complex, offers a balance between robustness to non-malicious operations and sensitivity to malicious tampering, making it more suitable for real-world applications such as medical imaging, forensics, and multimedia communications. Future work should focus on semi-fragile watermarking technique which is more suitable for real-world applications with optimized imperceptibility and recovery performance.

References:

1. Vaishnavi D., and T. S. Subashini. "Image Tamper Detection based on Edge Image and Chaotic Arnold Map." Indian Journal of Science and Technology vol. 8, No. 6: pp. 548-555, 2015.

2. Pongsomboon, Paween, Toshiaki Kondo, and Yoshiyuki Kamakura. "An image tamper detection and recovery method using multiple watermarks." Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 13th International Conference on. IEEE, 2016.

3. Dadkhah, Sajjad, et al. "An effective SVD-based image tampering detection and self-recovery using active watermarking." Signal Processing: Image Communication Vol. 29, No.10 : pp. 1197-1210, 2014.

4. Haghighi, Behrouz Bolourian, Amir Hossein Taherinia, and Ahad Harati. "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique." Journal of Visual Communication and Image Representation, 2017.

5. Kim, Cheonshik, Dongkyoo Shin, and Ching-Nung Yang. "Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC." Personal and Ubiquitous Computing Vol. 22 No. 1: pp.11-22, 2018.

6. Kiatpapan, Sawiya, and Toshiaki Kondo. "An image tamper detection and recovery method based on self-embedding dual watermarking." Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on. IEEE, 2015.

7. Vaishnavi, D., and T. S. Subashini. "Fragile watermarking scheme based on wavelet edge features." Journal of Electrical Engineering & Technology Vol. 10 No.5 : pp. 2149-2154, 2015.

8. Rawat, Sanjay, and Balasubramanian Raman. "A chaotic system based fragile watermarking scheme for image tamper detection." AEU-International Journal of Electronics and Communications Vol. 65 No.10 : pp. 840-847, 2011.

9. Botta, Marco, Davide Cavagnino, and Victor Pomponiu. "A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection." AEU-International Journal of Electronics and Communications Vol. 69 No. 1 : pp. 242-245, 2015.

10.Bravo-Solorio, Sergio, et al. "Fast fragile watermark embedding and iterative mechanism with high self-restoration performance." Digital Signal Processing Vol. 73 : pp. 83-92, 2018.

11.Sathik M. M., and S. S. Sujatha. "Authentication of digital images by using a semi-fragile watermarking technique." International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2 No. 11 : pp. 39-44, 2012.

12.Madduma Buddhika, and Sheela Ramanna. "Content-based image authentication framework with semi-fragile hybrid watermark scheme." Man-Machine Interactions 2. Springer Berlin Heidelberg, pp. 239-247, 2011.

13.Arathi Chitla. "A semi fragile image watermarking technique using block based SVD." International Journal of Computer Science and Information Technologies Vol. 3 No. 2 : pp. 3644-3647, 2012.

14.Kommini Chaitanya, Kamalesh Ellanti, and E. Harshavardhan Chowdary. "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain."International Journal of Computer Applications Vol. 28 No. 3 : pp. 42-46, 2011.

15.LV LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." Journal of Theoretical and Applied Information Technology Vol. 42 No. 2 : pp. 287-291, 2012.

16.Gokhale U. M., and Y. V. Joshi. "A semi fragile watermarking algorithm based on SVD-IWT for image authentication." International Journal of Advanced Research in Computer and Communication Engineering Vol. 1 No. 4, 2012.

17.Li Chunlei, et al. "Semi-fragile self-recoverable watermarking scheme for face image protection." Computers & Electrical Engineering on Elsevier ,2016.

18.Molina-García, Javier, et al. "Watermarking algorithm for authentication and self-recovery of tampered images using DWT." Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 2016 9th International Kharkiv Symposium on. IEEE, 2016.

19.Gadhiya, Tushar D., et al. "Use of discrete wavelet transform method for detection and localization of tampering in a digital medical image." IEEE Region 10 Symposium (TENSYMP), 2017. IEEE, 2017.

20.Ramos, Clara Cruz, et al. "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain." Discrete Wavelet Transforms-Algorithms and Applications. InTech, 2011.

21.Tiwari, Archana, and Manisha Sharma. "An Efficient Vector Quantization Based Watermarking Method for Image Integrity Authentication." Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Springer, Singapore, pp. 215-225, 2018.