International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 1 pp. 297-301 Sept 2017 - March 2018 www.csjournals.com

Comparative study of Semi-Fragile Watermarking on Grayscale and RGB Images for Authentication and tampering issue

Hiral A. Patel

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

Abstract: With the rapid growth of digital image usage in medical diagnostics, legal documentation, insurance processing and online media transmission, ensuring image authenticity has become a critical challenge. To address this issue, semi-fragile watermarking provides an effective solution by allowing tolerance to non-malicious operations while remaining sensitive to malicious modifications. The comparison of Semi-fragile watermarking using Grayscale and Color image is discussed here. By applying same algorithm for both type of image, the performance is evaluated based on parameters like imperceptibility, robustness, watermark capacity, embedment capacity, computational complexity.

Keywords: Grayscale image, RGB color image, Semi-fragile watermarking, Authentication, Tampering.

INTRODUCTION

Digital images are widely used in medical sector, Legal evidence, Insurance companies, Online media transmission etc. As these images are valuable there are chances of Content modification, Forgery, Copy-paste tampering etc. can be easily done using Image editing software like Adobe Photoshop. So, there is a need to check the authenticity of image. For providing online security to the image, lots of research work is going on. Using watermarking technique, the image authentication as well as tampering issue can be solved.

Fragile and Semi-fragile watermarking are two separate techniques for solving this purpose. But with Semi-Fragile watermarking technique, image authentication, tamper detection, localization as well as image recovery will be more preferable. Semi fragile technique's behaviour is different for malicious as well as non-malicious attacks. It becomes robust against non-malicious attacks where as sensitive for malicious attacks.

LITERATURE REVIEW

Researchers have worked for Digital image authentication and tampering issue and have tried to solve the issue using different approach. Kommini Chaitanya [1] have worked for tamper localization issue for grayscale image and tried to solve the issue using Semi-fragile system. Gokhale U.M. et.al. [2] have worked for authentication issue for grayscale image and solved it using Semi-fragile watermarking system. Monila-Garcia et. al. [3] have worked for authentication and recovery issue for grayscale image and tried to solve using Semi-fragile system. Gadhiya Tushar et.al. [4] have worked for tamper localization issue for grayscale image and solved issue using Semi-fragile system. Ramos et.al. [5] have worked for authentication issue for color image and using semi-fragile approach. Tiwari Archana et.al. [6] have worked for tamper localization issue for grayscale image and solved using semi-fragile watermarking technique. Chetan et.al. [7] have worked for authentication and tamper recovery for grayscale images by using semi-fragile approach. Pongsomboon, Paween et.al.[8] have worked for authentication and recovery issue for color image and tried to solve the issue using fragile system. Dadkhah, Sajjad et.al. [9] have worked for authentication and tamper recovery for color image using fragile watermarking approach. Haghighi et.al. [10] have worked for tamper recovery issue for color image using fragile watermarking system.

As per the literature review, it is found that [1-7] researchers have solved the issue using Semi fragile watermarking approach where as others [8-10] have solved issue using Fragile watermarking approach. Among these [5,8-10] tried to solve issue for color image where as others solved issue for grayscale image. Very few work has been carried out for color image using semi-fragile watermarking. This gap motivates author for working on comparison based on parameters for grayscale and color image.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 1 pp. 297-301 Sept 2017 - March 2018 www.csjournals.com

TYPES OF DIGITAL IMAGES

Digital images can be of different format and of different quantity of colors. As per the quantity of colors, digital images are divided into three types named Binary image, Grayscale image and RGB Color image.

Binary images use 1 bit to represent single pixel. The intensity value can be either 0 or 1 which represents only Black and White two colors. The limited content can be demonstrated using Binary images.

Grayscale images use 8 bits to represent single pixel. The intensity value is in the range of 0 to 255 which allows 256 shading options. In medical sectors, biometric system, scanned document image etc. , today also these grayscale images are used. As compare to binary image, higher content can be demonstrated with grayscale image. The computational complexity is low because of limited complexity in image.

RGB color images, use 3 color channels named Red, Green and Blue. For each pixel, 8 bits are used for each color channels means 8*3=24 bits are used to represent color image. For red, green and blue color channels, separate 256 color shades can be represented. The combination of these 3 true color combinations will represent one color to the pixel. Now a days, in majority of sectors, these images are used. Large amount of content can be demonstrated using RGB Color image. As higher data capacity is there with this image, the computational complexity is high.

The digital image combination is demonstrated in Fig.1.

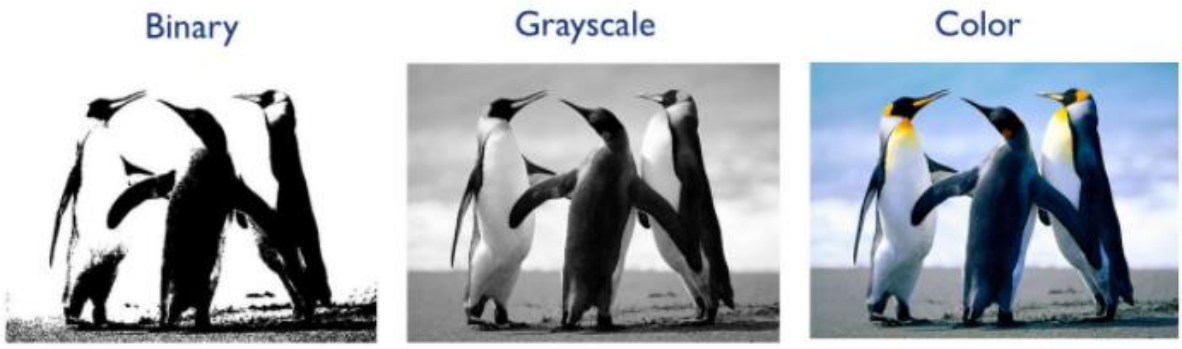

Fig.1 Types of Digital Images

SEMI-FRAGILE WATERMARKING MECHANISM

The watermarking system for authentication and tampering issue is internally divided into multiple subprocesses. First of all, watermark is generated from the original image and it is embedded within the same image. This image is known as Watermarked image. At the time of authentication process, first of all, the embedded watermark will be extracted from watermarked image and it is compared with the generated watermark. If both the watermarks are matched then the image is considered as authentic otherwise it is considered as tampered.

For comparing Grayscale image and Color image performance, following algorithm is used.

A. *Generating watermark:*

Input: Original Image
Output: Watermark
The feature of original image is extracted using following steps:

1. Let IM is the original image of size 512 X 512.
2. Apply 2nd level Haar Wavelet transform and select LL2 subband which is of size 128 x 128.
3. Apply canny edge detection to generate watermark (WM) of size 128 x 128.

B. Embedding Watermark:

Input: Original Image, Watermark
Output: Watermarked Image

1. Apply 2nd level Haar Wavelet transform on original image and select LL2 subband.
2. Apply SVD on LL2 to get U, S and V and on WM (Watermark) to get U_W, S_W and V_W.
3. Modify the singular values S with S_W using scaling factor (α). Following the formula: S_NEW = S + α * S_W
4. Apply inverse SVD using iLL2 = U * S_NEW * V'.
5. Apply 2nd level inverse DWT to get watermarked image (WMD).

C. Extracting Watermark:

Input: Watermarked Image
Output: Extracted watermark

The watermark extracting process from watermarked image is as follow:

1. Apply 2nd level DWT to WMD and get LL2, LH2, HL2 and HH2.
2. Apply SVD on LL2 to get WU, WS and WV.
3. Obtain the singular values using formula SR = (WS – S)/ α.
4. Apply inverse SVD using formula WM_E= U_W * SR * V_W' to extract the embedded watermark.

D. Authenticating Image:

Input: Extracted Watermark, Generated Watermark
Output: Image authentic/tampered

The authenticating image process is as follow:

1. Compare two watermarks using XOR technique.
2. Using threshold value, the image is considered as Authentic or tampered.

EXPERIMENTAL OUTCOME

The mentioned algorithm is applied in MATLAB. For comparison, grayscale images as well as color images of 512 x512 size are selected. For color image, Red color channel is used for above implementation. The performance is observed as per following parameters:

A. Imperceptibility:

Imperceptibility is tested using PSNR. Higher the PSNR means the watermarked image is closer to Original Image. With the system the PSNR is 50.2347dB with Color image and 52.5378dB with Grayscale image.

B. Watermark Generation

When the watermark is generated then for grayscale image, due to single plane one watermark can be generated where as for color image three watermarks can also be generated.

C. Embedding Capacity

As the gray scale image is having only one plane where as RGB color image is having three color planes so for Watermark Embedment, large capacity is available with Color images as compare to Grayscale image.

D. Robustness

For robustness testing, different non-malicious attacks like JPEG Compression, Blur, Sharpening, Salt & Pepper and malicious attacks like copy move, slicing are applied to the watermarked image. And the outcomes are observed. Grayscale as well as Color image, both images become robust against non-malicious attacks and become fragile for malicious attacks. For performance evaluation, NCC is calculated after each attacks then it is observed that with Color image, NCC outcomes are better than Grayscale image.

E. Computational Complexity
Processing time is observed for both images and it is found that Grayscale image's processing time is less as compare to Color image.

F. Authenticity
Image authentication and tamper detection point of view the accuracy is observed and for both the images, similar results are found. Almost, both type of images classify the image as authentic or tampered properly.

The overall comparative outcomes are shown in Table-1.

Table-1 Comparative Outcomes

Parameters	Grayscale Image	RGB Color Image
Channels	1	3
PSNR	High	Slight Low
Imperceptibility	Achieve	Achieve
Watermark Generation	Less amount of data	More amount of data
Watermark Embedment	Low	High
Robustness	High	Higher
Computational Complexity	Less	More
Processing Time	Fast	Slow
Authenticity / Tamper Detection	High	High

The comparative analysis indicates that grayscale images offer lower computational complexity and faster processing with high authentication accuracy, making them suitable for lightweight watermarking applications. In contrast, RGB color images provide higher embedding capacity and enhanced robustness due to multi-channel processing, making them more effective for advanced tamper detection and secure image authentication systems.

CONCLUSION

The semi-fragile watermarking system is compared for Grayscale and color image. Experimental analysis shows that grayscale images provide higher PSNR, reduced computational complexity and resulting in faster processing time. RGB color images offer significantly higher embedding capacity and improved robustness due to multi-channel availability. Both image types are enough capable for high authentication accuracy and reliable tamper detection. Now a days, Grayscale images are used in medical field where fast processing is the major concern. Whereas color images are normally used where high reliability is at demand and no bother for time complexity. So, Semi-fragile watermarking system with Grayscale as well as Color image for authentication and tampering point of view can be used.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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
5. Ramos, Clara Cruz, et al. "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain." Discrete Wavelet Transforms-Algorithms and Applications. InTech, 2011.

6. 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.
7. Chetan, K. R., and S. Nirmala. "Intelligent Multiple Watermarking Schemes for the Authentication and Tamper Recovery of Information in Document Image." Advanced Computing and Communication Technologies. Springer, Singapore, pp. 183-193, 2018.
8. 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.
9. 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.
10. 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.