International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-9 March-2013

Attack Detection in Watermarked Images with PSNR and RGB Intensity

Neha Chauhan[1], Akhilesh A. Waoo[2], P. S. Patheja[3]

Abstract

For more security to the information and to enhance the hiding capacity of an image. A new strategy in image steganography here we propose the region-adaptive watermarking algorithm which will be used for the novel application to detect watermark attacks. The major advantages of the proposed watermarking detection technique are PSNR and RGB Intensity value. For tamper detection using linear classifier by providing these discriminating features. The watermark is embedded on different regions of the host image using a combination of discrete wavelet transform and singular value decomposition technique. Certain types of attack have occurred and there is a novel use the region-adaptive watermarking technique as a means to detect. At the same time, translation, scaling and rotation belongs to geometric attacks are also applied. The severity of these attacks can be adjusted by modifying their corresponding parameter values. Our experimental results will detect the hiding data on the original image and also little relation to secret message file. For more security to the information. It providing more helps.

Keywords

RGB Color Intensity, PSNR, Image steganography, Image encryption, Linear Classifier, Message Encryption.

1. Introduction

However, one of the most significant problems, which affect the commerce of digital media, is how to protect copyright and ownership. The watermarking, 1 of the popular approaches consider ding as a tool for providing the copyright protection, is a technique based on embedding a specific mark or signature into the digital products. While several watermarking algorithms have been proposed [1].

Neha Chauhan,Student, M. Tech, Organization: BIST, Bhopal, India.

Akhilesh A. Waoo, Assistant Professor, Organization: BIST, Bhopal, India.

P. S. Patheja, HOD, BIST, Bhopal, India.

Transform domain schemes, such as discrete wavelet transform (DWT) based watermarking have shown more advantages and provide higher performance than others. As one of the most popular and viable techniques in protecting copyrights in digital media, watermarking technology has received enormous level of attention of researchers and practitioners alike. Unfortunately, due to the same reason, watermarking technology has also attracted the attentions of hackers and criminals alike who are interested in breaking the watermarks in order to crack the copyright protection system. As a result, there is a constant challenge on the researchers to keep improving the robustness of the watermarking technique while at the same time maintaining its transparency as to not intruding any legitimate use of the media. Progress in this area has been steady as can be seen from a healthy number of publications in the field and the sheer number of institutes around the world that deal with the issue [2]. In the more specific field of digital image watermarking, one of the most notable techniques is region-based image watermarking [3]. The paper described a method for embedding and detecting chaotic watermarks in large images. An adaptive clustering technique is employed in order to derive a robust region representation of the original image. The robust regions are approximated by ellipsoids, whose bounding rectangles are chosen as the embedded area for the watermark. The drawback of this technique is due to limited number of suitable regions for storing the watermark the watermark storing capacity can be low.

Most first generation digital watermarking algorithm embedded the watermarking into the time domain samples or transform domain to transform coefficients, but this leads to a poor robustness of time domain algorithms to the signal processing like compression, noise and filtering, transform domain watermarking uses the idea of audio masking effect and spreads spectrum technology to improve the robustness, simultaneous reduces the performance of anti-synchronization attack. In the field of digital audio watermarking, the idea is to use the stable feature points of the audio to mark the embedded position of the watermarking, and use the stable performance of these feature points anti-synchronized

attacks to improve the ability of the watermark anti-synchronization attack. Feature points should have the feature such as stability, more uniform distribution and the ability to accommodate the watermarking [4].

2. Introduction

In this Research paper [5] here they advancement of digital image watermarking technology have reviewed an analysis of on a number of attack types on image watermarking. The analysis was carried out using two image analysis tools namely Image Histogram and Fourier Spectrum for frequency domain analysis. Using the results of the experiments, they argue that existing techniques have different sensitivity and robustness levels to different attacks. The results also uncover a number of common similarities between different types of watermark attack. They have presented a novel digital image watermarking technique that takes into account the results of previous analysis and testing of the hypothesis. There technique utilizes a number of technologies namely dual watermarking, image segmentation and partitioning, and DWT-SVD to fulfill the design criteria set to prove the hypothesis. The experiment results show that the technique is more robust to attacks than the original DWT-SVD technique. The watermark detection process uses coefficients derived from the Region-Adaptive Watermarking algorithm in a linear classifier. The experiment conducted to validate this feature shows that in average 94.5% of all watermark attacks can be correctly detected and identified.

A watermarking technique based on the frequency domain is presented in this research work [6]. The JPEG is a usually file format for transmitting the digital content on the network. Thus, the proposed algorithm can used to resist the JPEG attack and avoid the some weaknesses of JPEG quantification. And, the information of the original host image and watermark are not Needed in the extracting process.

In this research work [6], a modified algorithm is presented to improve the defect of the JPEG quantification in order to reduce the bit error rate (BER) of the retrieved watermark. Addition, two parameters are regarded as the controlling factors. They are used to adjust the value of the DCT coefficient in order to trade-off the qualities between the Watermarked images and retrieve watermark. Moreover, the proposed algorithm is design as a blind mechanism. Thus, the original image and watermark are not needed for extracting watermark. To demonstrate the robustness of the proposed scheme The peak signal to noise rate (PSNR) is used to estimate the quality between the original image and the watermarked image.

This research work [7] presents a novel and robust color watermarking scheme of embedding color watermark into color host image. The technique shows efficient extraction of Watermark with high PSNR of embedded image. The proposed algorithm is experimented in frequency domain in which combination of DWT and DCT is applied on the host image. The High energy content of color watermark i.e. low frequency DCT coefficients are embedded into mid frequency DCT coefficients of high frequency components of multi resolved host color image. The proposed algorithm is more secure, robust and efficient because of use of DWT and DCT. Performance evaluation and testing of the proposed algorithm using standard benchmarks Reveals that it is fairly robust against a wide range of signal and image processing operations.

Digital images are easy to manipulate and modify for ordinary people [8]. This makes it more and more difficult for a viewer to check the authenticity of a given digital image. Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. This research work present an improved algorithm based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to detect such cloning forgery. The proposed scheme accurately detects such specific image manipulations as long as the copied region is not rotated or scaled and copied area pasted as far as possible in specific position from original portion.

For efficiently verifying the integrity of images cannot, therefore, is overemphasized in this digital era. The primary task of a copy-move image forgery detection algorithm is to determine if a given image contains cloned regions without prior knowledge of their shape and location. An obvious approach is to exhaustively compare every possible pair of regions. However, such an approach is exponentially complex. The drawback with schemes based on watermarking is that the water mark must be embedded right during the image formation to avoid

the possibility of watermarking an already forged image. This is practically difficult as most digital cameras and other image acquisition devices do not have instantaneous watermarking facilities.

3. Proposed Algorithm

The proposed watermark attack detection scheme. The scheme requires the certain threshold in addition image equations. The scheme start with calculate PSNR values between original watermarked image and tested watermarked image.

Get Image

- Original Watermarked Image
- Tested Watermarked Image
- Find PSNR Value
- If PSNR is higher then
- No Attack
- Else
- PSNR is lower then
- Find RGB intensity levels
- If RGB Intensity Match
- Then
- No Attack
- Else
- RGB Intensity No Match
- Coefficients Calculate
- Linear Classification
- Result Plotting

If PSNR value is higher than certain threshold, it represents original watermarked image and tested watermarked image are almost identified.

However, if PSNR is lower than certain threshold, it means that tested watermarked image suffer from attack. Then calculate RGB Intensity values. If RGB Intensity values are Match with tested watermarked image, it represents original watermarked image and tested watermarked image are almost identified. If RGB Intensity values are No Match with tested watermarked image, it means that tested watermarked image suffer from attack after that, we will signify what type of attack has been applied to the tested watermarked image. This process will use linear classifier. In addition, a number of discriminating features will apply which is described below.

4. Test Results and Analysis

We applied the watermarking technique to hiding data inside the image and after hiding data we try to detect attack in given water mark image. The host image has dimension are more than 512×512 pixels and data file is more than 1 kb. As a quantitative measure of the degradation effect caused by the attacks we use Peak-Signal-to-Noise Ratio (PSNR). The formulation between the original and the attacked watermarked signals can be found described in [2]. High PSNR values indicate lower degradation hence indicating that the watermarking technique is more robust to that type of attack. Two experiments were conducted to test the algorithm. The first experiment is aimed to verify that inserted watermarks images can be extracted with minimal distortion.

Fig 1: Original Image of Boat

To detect the watermarked attacked we test the robustness of the proposed watermarking scheme, seven watermark removal attacks are applied to the watermarked image. The PSNR of each watermarked image will be given of each picture however these pictures are only to be taken lightly. PSNR does not take aspects of the HVS into effect so images with higher PSNR's may not necessarily look better than those with a low PSNR.

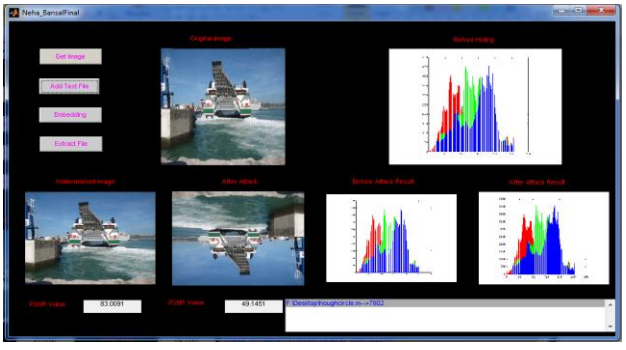

Fig 2: Screen snapshot

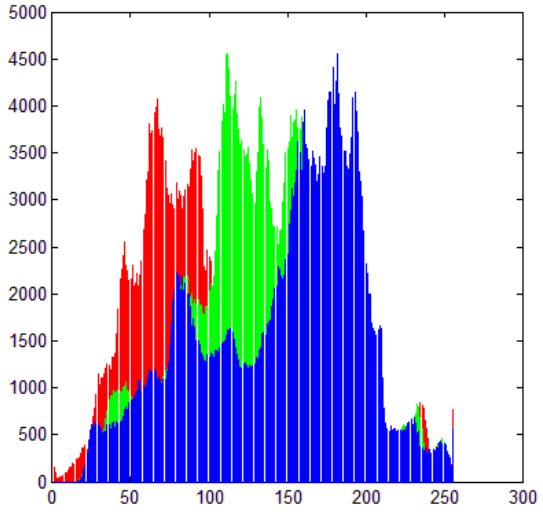

Fig 3: RGB intensity of Boat Image Before watermarking

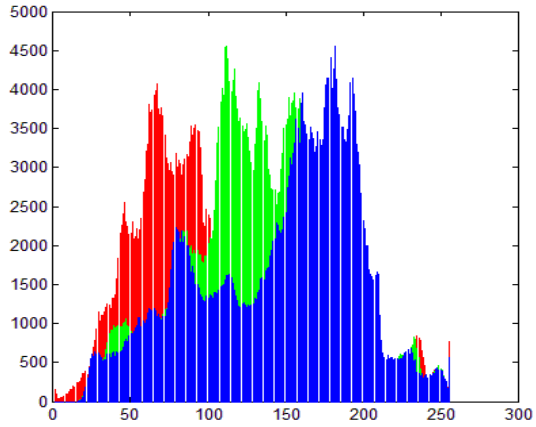

Fig 4: RGB intensity of Boat Image After watermarking

Performance requirements are similarly only to be used as a rough guideline. In general, algorithms were implemented in the most straightforward way, not the most computationally optimal. Furthermore, MATLAB may handle certain programming constructs differently from other languages, thus the best performing algorithm may vary for each language and implementation.
Different watermark attacks have different coefficient to detect. Some of the attacks only require one coefficient which include Gaussian noise and salt and pepper noise, moreover, the rest of them need 2 factors. And also we propose to check The PSNR values between the unmodified watermark image and the attacked watermarked image are then averaged. After PSNR we compare RGB intensity of both image original and attacked watermarked image.

Here theoretical it is clear that after check RGB intensity and PSNR technique In addition to the improving the robustness of the watermark to attacks, they can also show a novel use the watermarking technique as a means to detect if certain type of attacks have occurred. This is a unique feature of watermarking algorithm which separates it from other state-of-the-art watermarking techniques. The watermark detection process uses coefficients derived from the Watermarking algorithm in a linear classifier. The experiment conducted to validate this feature will shows that in average 96% of all watermark attacks can be correctly detected and identified.

Table 1: Show Different Attacker

S. No	Attackers
1	Gaussian noise
2	Salt and pepper noise
3	Sharpen
4	Smoothing
5	Median filter
6	Histogram equalization
7	JPEG compression

They show a novel use the region-adaptive watermarking technique as a means to detect if certain type of attacks has occurred. This is a unique feature of our watermarking algorithm which separates it from other state-of-the-art watermarking techniques. The watermark detection process uses coefficients derived from the Region-Adaptive Watermarking algorithm in a linear classifier. The experiment conducted to validate this feature shows that in average 94.5% of all watermark attacks can be correctly detected and identified.

Our Proposed Algorithm is able to detect any type of attack if applied in watermarks image. And improves the speed of detection, and also test the robustness of the watermarked images.

5. Conclusion

We have proposed in this Research paper a novel digital image watermarking detection technique using

RGB intensity and PSNR Value approach. To improve the reliability of the DWT based watermark detection, this paper introduces the new solution based image watermark detection method that is used to recover the geometrically distorted image before detecting the watermark. it can be implemented by the blind based DWT based watermarking scheme.
The technique is derived from our previous work [5].

Our hypotheses are:
1. By Calculating RGB color intensity value of the host data and the inserted watermark data.
2. In order to counter both high frequency and low frequency type attacks by calculating PSNR value. If we found PSNR value of watermarked image is lower its mean in host was attacked by attackers.

Our RGB intensity and PSNR Value watermarking technique is realized by using two watermark images, each with a strong High Frequency or Low Frequency components. Non overlapping regions of these watermark images are inserted into the host image using a combination of image segmentation. The experimental results will performed and analyze of different images file is implemented in matlab tool.

References

[1] G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital watermarking: An overview", *EUSIPCO, vol. 1, pp. 9-12*, 1998.
[2] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., Information Hiding—A survey, *Proceeding of the IEEE, Special Issue on Protection of Multimedia Content*, 1062-1078, July 1999.
[3] A. Nikolaidis and I. Pitas, "Region-based image watermarking," *Image Processing, IEEE Transactions on*, vol. 10, no. 11, pp. 1726-1740, 2001.
[4] H. X. Wang Overview of content based adaptive audio watermarking. *Journal of Southwest Jiao tong University. 44(3), 2009, 430-437 (in Chinese).*
[5] s.sudirman, m.merabti, d.aljumeily, "Region-Adaptive Watermarking System and Its Application", *Developments in E-systems Engineering, PP-215-220, IEEE 2011.*
[6] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang, "A watermarking technique based on the frequency domain", *journal of multimedia, vol. 7, no. 1*, February 2012.
[7] Satishkumar Chavan, Rohan Shah, Roshan Poojary, Jaisel Jose and Gloria George,"A Novel Robust Color Watermarking Scheme for Color watermark images in Frequency Domain", *International Conference on Advances in Recent Technologies in Communication and Computing IEEE* 2010.
[8] Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection", *IEEE* 2011.
[9] Cl.Song, S.Sudirman and M.Merabti, ―A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks‖, Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.
[10] C.Song, S. Sudirman, M.Merabti and D.L.Jones, "Analysis of Digital Image Watermark Attacks", 6th IEEE International Workshop on Digital Rights Management, 2010.

I am **neha Chauhan** pursuing M Tech in Computer science final year from Bansal Institute of Science And Technology, Bhopal. As our country increasingly relies on electronic information storage and communication it is imperative that we as a software engineer should use our technical skills to implement a program for the better online communication. So this is my small effort toward this target. Hope this effort of mine will result in better electronic communication.