ISSN (Online): 2230-7893
www.IJCEM.org

Information Hiding Watermarking Detection Technique by PSNR and RGB Intensity

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

[1]Research Scholar, BIST, Bhopal, India.

[2,3]Assistant Professor, BIST, Bhopal, India.

Abstract

There has been many techniques for hiding messages in images. We propose a new region-adaptive watermarking algorithm which will be used for the novel application to detect watermark attacks. One of the major advantages of the proposed watermarking detection technique is PSNR and RGB Intensity value that it allows tamper detection using linear classifier by providing these discriminating features. The watermark data is embedded on different regions of the host image using a combination of discrete wavelet transform and singular value decomposition technique. In addition, there is a novel use the region-adaptive watermarking technique as a means to detect if certain types of attack have occurred. As will be elaborated, the technique to improves the speed of detection, and also test the robustness of the proposed watermarking scheme. They are Gaussian noise, salt and pepper noise, sharpen, smoothing, histogram equalization and JPEG compression attack. At the same time, rotation, translation and scaling belongs to geometric attacks are also applied. The severity of these attacks can be adjusted by modifying their corresponding parameter values. Experimental results will detected the hiding data on the original image and has little relation to secret message file. It helps, for providing more security to the information

Keywords- *RGB Color Intensity, PSNR, Image steganography, Image encrypton, L*inear Classifier, *Message Encryption.*.

1. INTRODUCTION

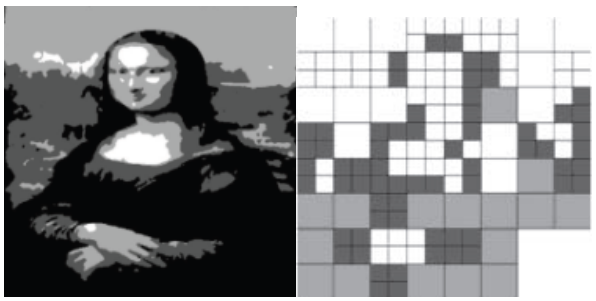
Digital audio watermarking has been widespread concerned in the academic cycles, which is an effective way to protect audio product property rights, meanwhile, digital audio watermarking technology faces greater challenges than the digital image and video watermarking technology now. As one of the most 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 [1]. In the more specific field of digital image watermarking, one of the most notable techniques is region-based image watermarking [2]. 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.

In this paper, we present a novel watermarking technique which works by adaptively embedding the watermark data into different region of the host image. The rationale of our approach is based on the research finding we came into in our previous work [3][4]. This finding will be described in detailed in this paper for convenience. 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. The core idea of the second generation watermarking is to embed in the media to identify the important part of the media itself, which is proposed by Cox *et al.* [5], and extended by Kutter *et al.* [6]. It indicates that some important data feature of the media should be taken full advantage. of the process of embedding the watermark. 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 [7].

2. RELATED WORK

In this Research paper [8] 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.



(a) (b)

(c)

Figure 1. (a) MRF segment tied host image, (b) watermark insertion region and (c) watermarked image

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. In addition to the improving the robustness of the watermark to attacks, they can also show a novel use the region-adaptive 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 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 [9]. 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 [9], 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 algorithm has been simulated using C++ program. The host images of size 256× 256 are 8-bit gray level images and the watermarks of size 128×128 are binary images. And, one watermark and five host images (i.e. Lena, F16, Pepper, Baboo, and Girl) are used to test. The peak signal to noise rate (PSNR) is used to estimate the quality between the original image and the watermarked image.

This research work [10] 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.

In the presented research work, combined DWT-DCT method is used where first level or second level DWT decomposition of host image is carried out followed by

DCT of the high frequency coefficients of these DWT coefficients. The color watermark is converted into appropriate luminance plane on which block wise DCT is applied and low frequency DCT coefficients are embedded into high frequency coefficients of the host image. The method can be made blind as well as non-blind watermarking.

Digital images are easy to manipulate and modify for ordinary people [11]. 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.

Maliciously manipulate, and tamper digital images without leaving any obvious clues became very easy with the widely available, easy to use and extremely powerful digital image processing tools such as Photoshop and Freehand. As a result, there is a rapid increase of the digitally manipulated forgeries in mainstream media and on the internet. The necessity of algorithms

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. PREDEFINE TECHNIQUE

a. RGB intensity

Consider an image (Io) with dimension M×N×P, Where, P represents color combination (3 for a color image); M, N represents rows and column of intensity level. Separate R, G, B matrix of Image and convert each R, G, B matrix into single array (1×mn). For example, Lena image which is one of the common image used for image processing algorithms has a dimension of 225 × 225 × 3 and after separation of R, G, B and converting it in to single array vectors, we get 3 vectors of dimension 1× 50625.

For encryption we first generate elements from chaos map equal to the dimension of 3×M×N matrix.

b. PSNR

In order to better compare this new technique with the existing algorithm based on 8 bits binary information, the hiding capacity of an image along with the PSNR value (Peak Signal to Noise Ratio). The PSNR value gives the measurement of the distortion of carrier image after hiding information. The signal in this case is the original data, and the noise is the error introduced by compression.

The PSNR is defined as:

$$PSNR = 10\log_{10}\frac{(MAX^2 I)}{(MSE)}$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using B bits per sample, MAXI is 2B−1.And MSE stands for Mean Square Error. For two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other. The higher the PSNR, the better the quality of the compressed or reconstructed image. When the two images are identical, the MSE will be zero. For this value the PSNR is undefined i.e. ∞.

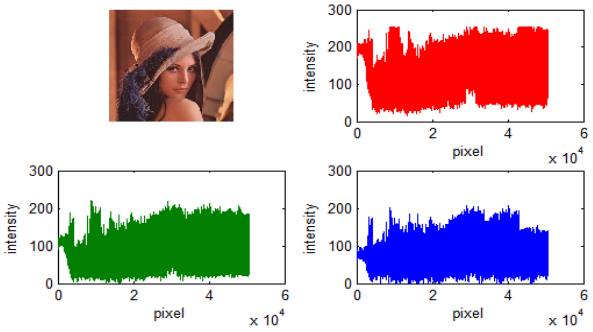


Figure 2 Lena image and RGB intensity plots

c. Linear Classifier

Linear classification belongs to the field of statistical classification; the goal of statistical classification is to use an object's characteristics to identify which class or group it belongs to. A linear classifier achieves this by making a classification decision based on the value of a linear combination of the characteristics. Suppose some given data points each belong to one of two classes, and the goal is to

decide which class a new data point will be in. for example, a data point is viewed as a p-dimensional vector, and we want to know whether we can separate such points with a (p-1) dimensional hyper-plane. There are many hyper-planes that might classify the data. One reasonable choice as the best hyper-plane is the one that represents the largest separation, or margin, between the two classes. So we choose the hyper-plane so that the distance from it to the nearest data point on each side is maximized. If such a hyper-plane exists, it is known as the maximum-margin hyper-plane and the linear classifier it defines is known as a maximum margin classifier.

d. Correlation coefficient

Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. The coefficient *r* can be calculated by the following formula.

$$r = \frac{\sum_i (Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i (Xi - Xm)^2}\sqrt{\sum_i (Yi - Ym)^2}}$$

Where

Xi - pixel intensity of original image

Xm- mean value of original image intensity

Yi- pixel intensity of encrypted image

Ym - mean value of encrypted image intensity

The correlation values are calculated for original and encrypted.

4. PROPOSED ALGORITHM

In Figure 2 shows 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.

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.

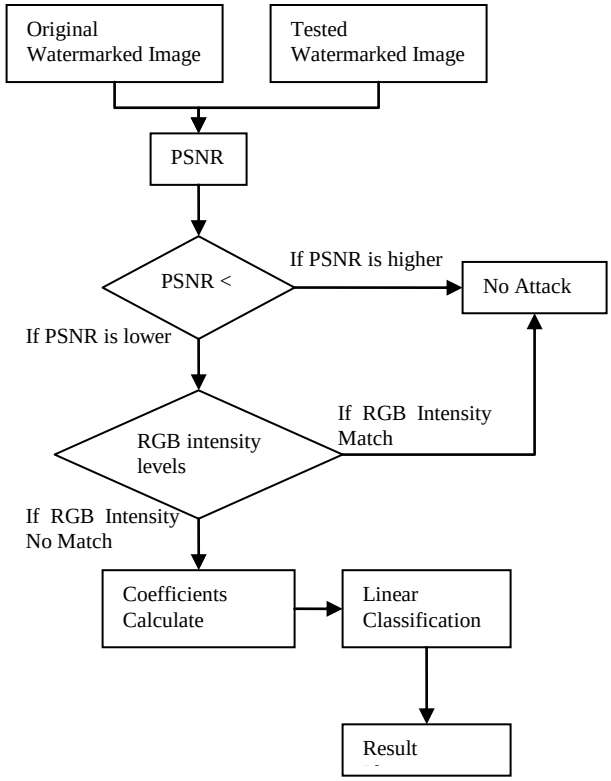


Fig 3 Block diagram of propose Algorithm

This process will use linear classifier. In addition, a number of discriminating features will apply which is described below. The embedding process of the proposed technique will be illustrated by the block diagram shown in Figure 2.

5. TEST RESULTS AND ANALYSIS

To detect the watermarked attacked we test the robustness of the proposed watermarking scheme, seven watermark removal attacks are applied to the watermarked image. They are Gaussian noise, salt and pepper noise, sharpen, smoothing, median filter, histogram equalization and JPEG compression attack. The severity of these attacks can be adjusted by modifying their corresponding parameter values. Definitions of these parameters can be found is given in [12]. 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.

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

Table 1 Show Different Attacker

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.

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.

6. CONCLUSION

We have proposed in this Research paper a novel digital image watermarking detection technique using RGB intensity and PSNR Value approach. The technique is derived from our previous work [8]. 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.

REFERENCE

[1]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.

[2] A. Nikolaidis and I. Pitas, "Region-based image watermarking," *Image Processing, IEEE Transactions on*, vol. 10, no. 11, pp. 1726-1740, 2001.

[3]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.

[4] 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.

[5] J. Ingemar Cox, J. Kilian, F. Thomson Leighton et al. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1997, 1673-1687.

[6] M. Kutter, S. K. Bhattacharjee, T. Ebrahimi. Towards second generation watermarking schemes, *In Proceedings of IEEE International Conference on Image Processing ICIP (*1999). 1999, 320-323.

[7]H. X. Wang Overview of content based adaptive audio watermarking. *Journal of Southwest Jiao tong University. 44(3), 2009, 430-437 (in Chinese).*

[8] s.sudirman, m.merabti, d.aljumeily, "Region-Adaptive Watermarking System and Its Application", *Developments in E-systems Engineering, PP-215-220, IEEE 2011*

[9] 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.

[10]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.

[11]Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection", *IEEE* 2011.

[12]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.*