Detection of Tampering in Image Using Watermarking

[1]Nidhi Patel,[2]Narendra Limbad

[1]PG Student, L.J.I.E.T, Ahmedabad, Gujarat, India
[2] Asst.Prof. L.J.I.E.T, Ahmedabad,Gujarat, India

Abstract

In the last few years there is a tremendous development in the area of high quality digital camera technology. So our life is full of the use of these digital images. However now a days there are lot of software (for example Photoshop, Photoscape, Photoplus and Picasa etc.) that can be used to modify these digital image. Therefore we cannot use these images as a proof or evidence. Therefore detection of tampering in image is important issue for forensic department. This paper presents digital watermarking for detection of tampering in image and improve the security of image. We worked on RGB components such as red, green and blue.3-DWT applied on RGB components for better results and chaos based encryption is used for security of watermark image. The proposed scheme provides high security and localizes tampered areas in tampered watermarked image.

Keywords: Tamper Detection, Watermarking, Spatial Domain, Transform Domain, Discrete Wavelet Transform (DWT)

1. INTRODUCTION

Detection of tampering means showing alteration which is not easily observable. Many researchers focus on how to detect tampering in digital images. In last few years, malicious attackers generally try to alter meaningful information of an image so that meaning of image is changed. Tamper detection is very important for some applications which involve highly sensitive data like medical imagery, satellite imagery and confidential documents etc. Tamper detection is also useful in court of law where digital images could be used as a forensic tool for criminal identification[2].

Watermarking methods are desirable because these methods provides integrity to image. Therefore, detection of tampering using watermarking method has much attention. In watermarking method additional data is added into the digital content of image in such a way that distortion caused by data embedding remains imperceptible. The additional data which is embedded is called "watermark"[2]. Many watermarking algorithms determines whether image has been altered or not and some of them can localize the altered areas and some of them have capability to recover altered or tampered areas[2].

There are several advantage of watermark. First, watermark does not need to store as a separate, associated metadata such as cryptographic signature. Second, watermark undergoes same transformation as the content of image in which watermark is embedded. There are many digital watermarking techniques for protecting digital content. The digital image watermarking techniques works into two domains: spatial domain and transform domain. The spatial domain techniques directly work with pixels. These techniques embed the watermark by altering the pixels value. Spatial domain techniques are least significant bit(LSB), correlation based technique, predictive coding technique[1] etc. But commonly least significant bit (LSB) spatial domain technique is used. The transform domain techniques embed the watermark by modifying the transform domain coefficients. DCT, DWT and DFT are commonly used transform domain techniques [9].

1.1 ATTACKS ON WATERMARKS

There are several kind of attacks are done on watermark, some of them given below[3] :

A. Active Attacks

In active attack the hackers try to eliminate the watermark or make it invisible. This is a large problem in fingerprinting, copy control or copyright protection.

B. Passive Attacks

In this attack, attacker is not trying to eliminate the watermark but simply trying to find out if a specified mark is present or not. As the reader must know, security against passive attacks is of the most importance in secret communications where the simple information of the existence of watermark.

C. Collusion Attacks

In this attack, the goal of the attacker is same as for the active attack but the technique is a little different. In order to eliminate the watermark, the attacker uses a number of copies of the same data, holding each different watermark, to create a new copy which is not having any watermark. This is a difficulty in fingerprinting applications but is not the usually spread because the hacker should have access to a number of copies of the same data.

The paper is organized as follows: Section 2 presents literature review, Section 3 presents proposed method, Section 4 shows experimental results and at the end concludes the paper.

2. LITERARURE REVIEW

Various researchers are working on watermarking method to detect tampering in image. Many methods are used for tamper detection in image.

Surya Bhagavan Chaluvadi and Munaga V. N. K. Prasad[15] proposed dual watermark scheme for image tamper detection and recovery.They divide image into 2x2 block and generate a 12-bit watermark by 5MSB of average intensity of two blocks after padding 3LSB zero remaining two bits of watermark are generated by parity check of 10 bit generated watermark. But low tamper detection rate in this method. Motoi Iwata et.al[16] presents digital watermarking method for tamper detection and recovery of JPEG images. They embedded an information into LSBs of the of the quantized DCT coefficients in a JPEG image directly. Difficulty is occurred while detection and recovery of large tampered areas.

Sawiya Kiatpapan and Toshiaki Kondo[17] used image tamper detection and recovery method based on self-embedding watermarking. The watermark taken which is down sampled version of original image. Two identical watermarks are decomposed into bit planes and embedded into least significant bit plane of cover image. This dual watermarking strategy is used for image tamper detection and recovery. They could not get perfect results while watermarks are damaged in both upper and lower sections.

Md. Moniruzzaman et. al[18] fragile watermarking scheme based on chaotic system has been proposed. Arnold's catmap is used to obtain the scrambled image by shuffling the pixel positions of host image. Therefore, the number of iteration and initial values which are used to obtain the scrambled image can be used as secret keys. The watermark can be extracted from watermarked image by using correct keys. The tampered areas are located by applying exclusive-OR operation between extracted watermark and original watermark. High error bit rate values for some images is drawback of this method.

Madhuri Rajawat and D S Tomar[19] proposed two level DWT for tampering detection in image. Wavelet domain is secure domain for watermark embedding. Wavelet domain is a frequency domain technique in which original image is transformed into frequency domain and then its frequency coefficients are modified in accordance with transformed coefficients of watermark and watermarked image is obtained. DWT decomposes image hierarchically and providing both frequency and spatial description of image. Experimental results shows that algorithm works only on big, little and blurring attacks.

Jun-Dong Chang et. al [20] presents fragile image watermarking scheme with recover ability based on local binary pattern (LBP). The LBP of each image block represents the spatial relation of localized image. LBP operator is used to generate authentication data which are embedded into 2LSBs of each image block with 3x3 pixels size for tamper detection and recovery. If the spatial relation of localized image is changed or altered then

LBP would be changed and different from the original LBP. LBP base watermarking and image tamper detection are lossy.

III. BACKGROUND

This section gives a detailed study of the technique used for the proposed work:

A. DWT Technique

Watermark can be embedded in the cover either in the spatial or frequency domain. DWT is one type frequency domain technique. Wavelet domain is secure domain for watermark embedding. Wavelet has reference to too tiny waves[6].

When the discrete time domain signal is passed through successive low pass and high pass filters, the resultant signal is available in DWT.

In the decomposition, the image is divided into four bands in horizontal direction, vertical direction, diagonal direction and low frequency part .

For higher level of decomposition any one sub-band is chosen and is further decomposed into four bands. We have chosen the low frequency domain as the embedding domain and perform 3-level DWT decomposition in proposed method. DWT does not divide image into blocks of processing[19].

B. Chaos Based Image Encryption

For watermark image chaos based image encryption is done. Chaos theory describes the behavior of certain nonlinear dynamic systems that under specific conditions exhibit dynamics that are highly sensitive to initial conditions.

The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. It provides a good combination of speed, high security, complexity, reasonable computational overheads and computational power.

Chaos-based encryption algorithms are usually composed of two processes generally:

(i) Chaotic confusion of pixel positions by permutation process and

(ii) Diffusion of pixel grey values by diffusion process.

$$x(i+1) = s*(y_i - x_i) \quad (1)$$

$$y(i+1) = r*x_i - y_i - x_i z_i \quad (2)$$

$$z(i+1) = x_i\, y_i - b*z_i \quad (3)$$

where, s,r and b are system control parameters and consider values of it as 10, 28 and 8/3 respectively. x0, y0 and z0 are initial conditions and set their values for encryption and decryption. The equation generates sequence in the range of 0 and 1 with chaotic behavior.

III. PROPOSED METHOD

My proposed algorithm consists of two stages. First stage consists watermark embedding process and second stage is authentication stage which consists of watermark extraction and authentication and localization using extracted watermark. 3-level DWT based watermarking is used.

.

3.1 Watermark Embedding stage:

Watermark embedding steps are given below:

1). Take original image and divide it into 3 components.

2). Perform 3DWT on 3 components to decompose it into four non-overlapping coefficient sets: L_L3, L_H3, H_L3, H_H3.

3). Take watermark image/ logo and resize it as L_L3 by using bilinear interpolation.

4). Encrypt watermark using chaos based encryption algorithm. And call the encrypted watermark as "W_E".

5).Embed shuffled watermark with L_L3 decomposed level of original image using scaling factor. Where, scaling factor value is consider as 0.01

6).Use inverse DWT(I3DWT) on 3DWT transformed image and produced final watermarked image.

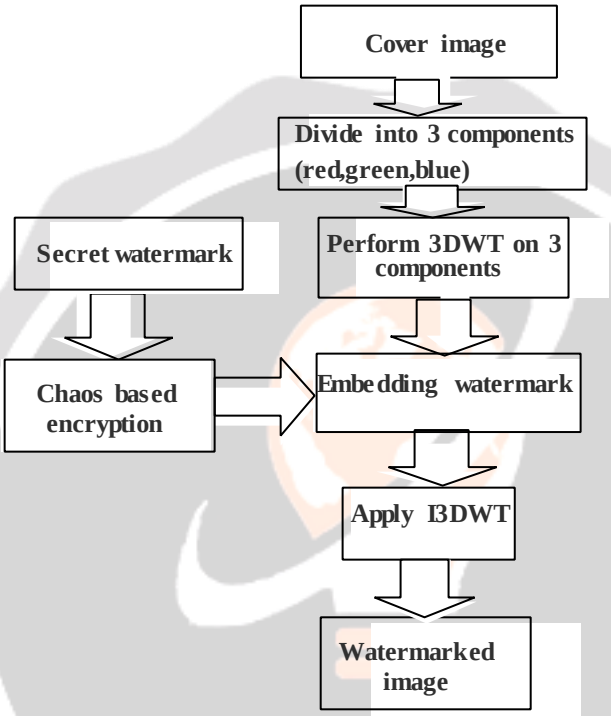

Fig 1: Flow graph of watermark embedding process

3.2 Watermark Extraction stage:

Watermark extraction steps are given below:

1). Take watermarked image and divide it into 3 components.

2). Apply 3DWT on watermarked image.

3). Extract watermark by using scaling factor which is embedded in watermarked image.

4). Combine watermarks of all 3 components.

5). Decrypt extracted encrypted watermark W_{EXE} using chaos based decryption algorithm by entering right key which is used in encryption. And call the decrypted watermark as "W_{EXD}".

6). Resize secret watermark "W" and get final extracted decrypted watermark "W_{EXD}" to the same size of cover image and round their values to be 8bit binary values.

7). Compare "W_{EXD}" with secret watermark "W" to identify tampered regions in image using XOR operation between them.

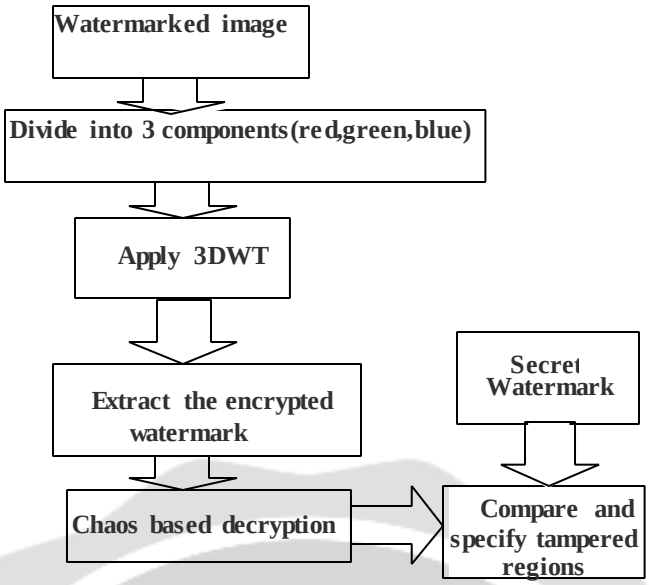

Fig 2: Flow graph of watermark extraction process

IV. EXPERIMENTAL RESULTS

The image quality of the watermarked image is one of the most important factors in evaluating information - hiding techniques. In the experiment we have applied algorithm to 100 images to check its efficiency. We have applied different types of attack on the images. Extracted watermark is decrypted after entering right keys means values of x0,y0 and z0 are considered as key. Here, we take values as x0=1.1840, y0=1.3627 and z0=1.2519.

In this paper, we have taken 24-bit color scale images as original image with size 512×512 is shown in Fig.3 (a) and (b). Red, Green and Blue components of original image are shown in Fig.4.The watermarked image quality is measured by the peak-signal-to-noise ratio (PSNR).

If the original image is I of size M × N and after embedding watermark into I the watermarked image is I*, then Mean Square Error(MSE) can be obtained by-

$$MSE = [\Sigma_x \Sigma_y \{I(x, y) - I^*(x, y)\}^2] / (M \times N) \quad (4)$$

Where, x is form M-1 and y is from 0 to N-1.

PSNR is used to measure the quality of the image and high value of PSNR means high quality of image affected by low quality of noise. PSNR is obtained from MSE and is given by-

$$PSNR = 10 \times \log_{10} (L^2 / MSE) \quad (5)$$

Where, L is the maximum intensity of the original image.
The watermarked image, which is given in Fig.5(d) and Fig.8(a) are having PSNR values 63.819dB, and 62.573dB respectively. Fig.7(c) and Fig.8(c) shows located tampered areas .

(a) (b) (c) (d)

Fig 3: Two Original images with 512x512 pixels (a) Image1 –"Pepper", (b) Image2 –"Airplane", (c) Image3 – "Lena", (d) Image4 –"Sailboat"

(a) (b) (c) (d)

Fig 4: (a) Original Image,(b) Red Component of Original Image,(c) Green Component of Original Image,(d) Blue Component of Original Image

(a) (b) (c) (d)

Fig 5: (a) Watermark Image,(b) Red component of Watermark Image,(c) Green Component of Watermark Image,(d) Blue Component of Watermark Image

The following figures display the effectiveness of our proposed approach against various attacks like insertion and deletion attacks. We apply deletion attack on watermarked image in Fig.7 and insertion attack in Fig.8.

(a) (b) (c) (d) (e)

Fig 7:Deletion Attack: (a) Watermarked final image, (b)Tampered watermarked Image, (c)Tampered extracted decrypted watermark using right keys, (d) Tampered area detection after XOR operation, (e)Tampered area located in original image

(a) (b) (c) (d) (e)

Fig 8: Insertion Attack: (a) Watermarked Final Image, (b) Tampered Watermarked Image, (c)Tampered extracted decrypted watermark using right keys, (d) Tampered area detection after XOR operation, (e)Tampered area located in original image

(a) (b) (c)

(d) (e) (f)

Fig-9: Watermarked images attacked by Salt & pepper noise with different intensities 0.01, 0.02 and 0.04 respectively; (d), (e) and (f) are corresponding extracted watermark.

The Bit Error Rate (BER) is the number of bit errors per unit time. It is used to compute the rate of error bit on the whole watermark accurate bits. For the original watermark image W of size m × n and the extracted watermark image W*, Bit Error Rate (BER) is given by-

$$BER = [\Sigma i \, \Sigma j \, \{W(i, j) \oplus W^*(i, j)\}] / (m \times n) \quad (6)$$

where, i is from 0 to m-1 and j is from 0 to n-1.

High PSNR values of watermarked images as shown in below table which defines low image quality degradation by using proposed method as compare to base paper.

TABLE 1
PSNR of watermarked images

Images	Rajawat and Tomar scheme	Proposed scheme
Image1	45.646	63.819
Image2	43.749	62.573
Image3	45.649	63.825
Image4	48.286	60.748

A low value of BER indicates extracted watermark is almost similar to the original watermark. In table 2 it can be seen that the proposed method gives low value of BER than the method in [18] which proves that proposed method is resist common image processing attack like salt and pepper.

TABLE 2
Comparison results of BER

Attack	Intensity	Method[18]	Proposed method
Salt & Pepper noise	0.01	3.64	1.19
	0.02	3.76	1.29
	0.04	5.84	3.94

CONCLUSION

In this paper we presented an efficient method for detection of tampering using watermarking. Digital Watermarking is very useful technique for detection of tampering, localization and recovery of image. We performed 3-level DWT on RGB components and chaos based encryption for security purpose. Experimental results shows that proposed method work efficiently and detect tampered areas effectively. High PSNR values shows less image quality degradation by using proposed method. The proposed method also gives low value of BER compared to existing method. The proposed method is also capable of locating the tampered areas when image is attacked by attacker.

REFFERENCES

[1] Chin-Feng Lee, Kuo-Nan Chen, Chin-Chen Chang, Meng-Cheng Tsai , " A Block Feature Correlation Based Image Watermarking for Tamper Detection Using Linear Equation" , 2009 Fifth International Conference on Information Assurance and Security, pp.615-618, IEEE 2009.

[2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN), ISBN: 0-7803-9094-6, pp. 709-716,IEEE 2005.

[3] Xiang-Gen Xia, Charles G. Boncelet, Gonzalo R. Arce, "A Multiresolution Watermark for Digital Images", Image Processing, 1997. Proceedings., International Conference, pp.548-551, IEEE 1997.
[4] Phen-Lan Lin, Po-Whei Huang, An-Wei Peng, "A Fragile Watermarking Scheme for Image Authentication with Localization and Recovery", Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering (ISMSE'04), IEEE 2004.
[5] Chin-Feng Lee, Kuo-Nan Chen, Chin-Chen Chang, Meng-Cheng Tsai, "A Block Feature Correlation Based Image Watermarking for Tamper Detection Using Linear Equation", 2009 Fifth International Conference on Information Assurance and Security,pp.615-618, ISBN: 978-0-7695-3744-3, pp.615-618, IEEE 2009.
[6] Luis Rosales-Roldan, Manuel Cedillo-Hernández, Mariko Nakano-Miyatake, Héctor Pérez-Meana, "Watermarking-based Tamper Detection and Recovery Algorithms for Official Documents" , IEEE 2011.
[7] Song Qiang, Zhang Hongbin, "Image Tamper Detection and Recovery Using Dual Watermark", IEEE 2010.
[8] Pradyumna Deshpande, Prashasti Kanikar, "Pixel Based Digital Image Forgery Detection Techniques". International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 539-543.
[9] Wu Penghui, Yang Bailong, Mao Jing, Zhang Zhongmin, "Block Compressive Sensing Based Watermarking Scheme for image tampering detection", IEEE 2012.
[10] Fang Ma, JianPing Zhang, Wen Zhang, "A Blind Watermarking Thchnology Based on DCT Domain", ISBN: 978-0-7695-4719-0, pp.398-401,IEEE 2012.
[11] Peng Zheng , Weihua Wang, Juan Wang, "A Hybrid Watermarking Technique to Resist Tampering and Copy Attacks", 2011 International Symposium on Intelligence Information Processing and Trusted Computing, ISBN: 978-0-7695-4498-4, pp.111-114, IEEE2011.
[12] Prasad Patil, Shefali Sonavane, "FragileWatermarking Scheme for Image Tamper Detection" , 2011 International Conference on Communication Systems and Network Technologies, ISBN: 978-0-7695-4437-3, pp.531-535, IEEE 2011.
[13] Mohmmad Ali M. Saiyyad,Nitin N. Patil, "Authentication and Tamper Detection in Images Using Dual Watermarking Approach", IEEE 2014.
[14] Vinayak S. Dhole,Nitin N Patil, "Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks", 2015 International Conference on Computing Communication Control and Automation, pp.752-757, IEEE 2015.
[15] Surya Bhagavan Chaluvadi, Munaga V. N. K. Prasad, "Efficient Image Tamper Detection and Recovery Technique using Dual Watermark" , 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009), ISBN: 978-1-4244-5053-4, pp.993-998,IEEE 2009.
[16] Motoi Iwata, Tomoki Hori, Akira Shiozaki, and Akio Ogihara, "Digital Watermarking Method for Tamper Detection and Recovery of JPEG Images", IEEE 2010.
[17] Sawiya Kiatpapan,Toshiaki Kondo, "An Image Tamper Detection and Recovery Method Based on Self-Embedding Dual Watermarking",DOI:10.1109/ECTICon.2015.7206973, pp.1-6 , IEEE 2015.
[18] Md. Moniruzzaman, Md. Abul Kayum Hawlader and Md. Foisal Hossain , "An Image Fragile Watermarking Scheme Based on Chaotic System for Image Tamper Detection" , 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014, ISBN: 978-1-4799-5179-6 ,pp.1-6, IEEE 2014.
[19] Madhuri Rajawat, D S Tomar ,"A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", 2015 Fifth International Conference on Communication Systems and Network Technologies, ISBN: 978-1-4799-1796-9,IEEE 2015.
[20] Jun-Dong Chang, Bo-Hung Chen, and Chwei-Shyong Tsai, "LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26, Kaohsiung , Taiwan, ISBN:978-1-4673-3036-7, pp.173-176, IEEE 2013.