Detection of Tampering in Image Using Watermarking - A review

[1] Nidhi Patel, [2] Narendra Limbad
[1]PG Student, [2]Assistant Professor
[1, 2]Department of Computer Engineering,
[1, 2] L. J. Institutes of Engineering and Technology, Gujarat Technological University
Ahmedabad, Gujarat, India

Abstract: As the rise of the digital era, analog data such as text, audio, photo and video are transformed to digital format for wide use and applications. In order to easy use and analysis on computers, analog images are transformed to digital file format by digital encoding techniques. Although digital images are widely used and analyzed on computers, the ease of alteration and duplication over the Internet also causes a serious issue on digital content protection. Digital images are easily altered by using photo editing soft wares. These types of softwares include Photoshop, Picasa, Photoscape and online alternatives are Pixlr.com, Paint.net, Photoshop.com. Therefore these tampered images can not be taken for the purpose of any proof. So,detection of these tampered areas in image is a serious challenge for forensic department. This paper shows that digital watermarking methods are of increasing interest and gaining popularity for image tamper detection. Digital watermark is one type of marker which is embedded in the signal such as audio or image data. Digital watermarking is a process of hiding information in the original data for protection of illegal duplication and unauthorized alteration.

Keywords: Watermarking, Tamper Detection, Spatial Domain, Transform Domain

I. INTRODUCTION

The authenticity and integrity of the digital images cannot be judged just by the human eyes. Many researchers focus on the problem how to detect tampering in digital images. The digital image authentication watermarking technology, which is used to detect and locate the tampered region.

In the recent few years, malicious attackers may try to modify meaningful information of an image such that its meaning is changing. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery, medical imagery and confidential documents etc. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not[7]. Watermarking methods used to detect these tampered areas are more desirable because these techniques protect the integrity of image and provide authentication. Therefore, this method for tamper detection has much attention.

The tremendous development of watermarking techniques by mean of embedding a reference pattern into image the problem of integrity and authentication of image have evoked the interest of research field. 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[7].

Digital watermarking has attracted lot of awareness of researcher mainly for two reason: one is, it is easily available and second is convey enough redundant information. Digital watermarking has many 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 pixel value. Spatial domain techniques are least significant bit(LSB), correlation based technique[13] and predictive coding technique etc. But commonly used spatial domain technique is least significant bit (LSB). The transform domain techniques embed the watermark by modifying the transform domain coefficients. Commonly used transform domain techniques are DCT, DWT and DFT[9].

1.1 TYPES OF WATERMARKS

Some of the important watermarking based on different watermarks which are given as follows:

A. Visible watermarks

A visible watermark is image or sub image or logo that is placed on top of another image. Such watermarks are applicable to images only. These logos or image are inlaid into the image in transparent form[1].

B. Invisible watermarks

Invisible watermark is embedded into image content. It can be identify by an authorized agency only. Such watermarks are used for content and author authentication, tamper detection and discovering unauthorized copier[1].

The paper is organized as follows: Section 2 deals with classification of tampering detection methods, Section 3 deals with literature review and at the end concludes the paper.

II. CLASSIFICATION OF TAMPERING DETECTION METHODS

According to the presence of extra information tampering detection methods can be divided into two parts[8].

(1) Active and
(2) Passive

Active methods are based on watermarking for tampering detection. They are based on the embedding of some additional data(generally extracted from the digital content of image) into the image itself. During the authentication process the detection of alteration in the additional data are used for determining tampering of the original image.

Passive methods do not need any additional information about the image and take advantage of specific detectable modification that tampering bring into the image. Since passive techniques do not need any addition information embedding into the digital content of images, they are considered as "blind tampering detection" methods. These types of techniques make decisions on the extraction of some features from the image based on some predefined rules or statistical thresholds or by some assumptions.

III.LITERATURE REVIEW

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

MadhuriRajawat and D S Tomar[1] 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.

They applied 2 level DWT on color images by extracting red, green and blue components. Experimental results shows that algorithm works only on big, little and blurring attacks.

Mohmmad Ali M. Saiyyad and Nitin N. Patil[2]proposed multimedia authentication and tamper detection scheme with the security of AES ciphered watermarking and hash function. They embed two watermarks in host image for authentication and tamper detection. They used unique identification code as first robust watermark which is then embedded in image using 2 level DWT. Hash code of host image is calculated and used as secondary watermark for tamper detection. It is not working for different types of attacks.

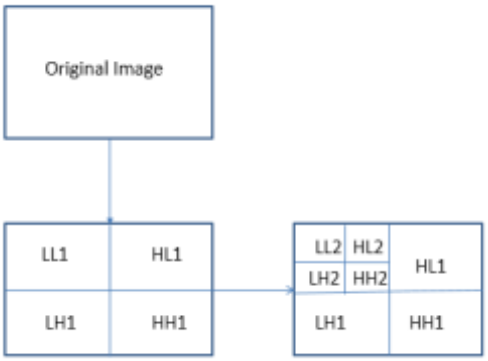

Fig: 2-level decomposition of an image [2]

Sawiya Kiatpapan and Toshiaki Kondo[3]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.

Vinayak S. Dhole and Nitin N Patil[4]mentioned fragile watermarking is mentioned for authentication and content integrity verification.They introduce modified watermarking technique which is based on non-sequential block chaining and randomized block chaining and this block chaining is created on the basis of secret key. Watermark information and information of block are put into image block. These blocks are linked with next randomly generated block of image. To obtain first watermark image the block chaining method is used. Self-embedded image is obtain by merging original image on original image so the final shuffled image is produced. At last firs watermark image is merge with shuffled image which produce final watermarked image. During recovery reverse process is follow to obtain original image from tampered image. By comparing block by block mean values of tampered blocks recovery of tampered block is done. The quality of watermarked image which is generated by using this method is low.

Jun-Dong Chang et. al[5]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.

Md. Moniruzzaman et. al[6] fragile watermarking scheme based on chaotic system has been proposed. Arnold's cat map is used to obtain the scrambled image by shuffling the pixel positions of host image. Therefore, the number of iterations and initial values which are used to obtain 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. The disadvantage of system explained in this is high error bit rate values for some images.

SajjadDadkhah et. al[9] presents efficient two level image tamper detection using three LSB watermarking. They divide image into 2x2 size block and pad 3LSBs of each pixel zero. Average intensity was calculated which is simply average of 4 pixels of block. Checking the parity of this value which gives one bit of 12-bits watermark.10 bits of watermark is generated as 5MSBs of first pixel inside the block and second 5MSBs is selected from second pixel of the block. After generating 11 bit watermark last bit of watermark is generated by checking parity of 10 bit which is making by MSBs. Tamper detection is done by extracting 12-bit watermark from watermarked image if there are any changes in watermark then image is tampered in first level of tamper detection. After first level detection, in second level bit by bit comparison is done of 5 MSBs of first two pixel of block and first 10 bit of extracted watermark. While embedding watermark into 3LSBs of each pixel which degrade the image quality and suitable for only grayscale images.Motoi Iwata et. al[10]presents digital watermarking method for tamper detection and recovery of JPEG images. Check symbols are embedded to an information which reduced original image into LSBs of the of the quantized DCT coefficients in a JPEG image directly. Therefore the method completely extracts the embedded data from watermarked JPEG images. Disadvantage is that difficulty in detection and recovery of large tampered areas.

Phen-Lan Lin et. al[11]discussed a fragile, block wise and content based watermarking for image authentication and recovery. The block watermark is generated by encrypting the combination of block location, the content features of randomly selected block and CRC checksum to break up the block independency and complicate the VQ attack . By using this proposed method the image quality distortion is high in some images.

Song Qiang and Zhang Hongbin in [12] embed watermark information into original image using least significant bit and DWT algorithm. First they embed bit stream into watermark image using DWT and secondly they scramble the bit stream using Arnold transformation with secret key K to obtain embedding watermarking information which is converted into binary image. For tamper detection in image make comparison between extracted watermark image and watermarked image.

Luis Rosales-Roldan et. al[13]presents two watermarking-based algorithms for tamper detection and recovery of the tampered regions, which can be applied to official documents, such as digitized passports and governmental registrations are proposed. A halftone version of the original grayscale image is used as an approximated version
of the host image in both algorithms(image digest), which is then embedded as a watermark sequence into the
frequency domains of the host image. In first algorithm watermark embedding is carried out in integer wavelet transform domain and second algorithm is discrete cosine transform. By using these two different algorithms they detect tampered areas in official document images.

Chin-Feng Lee et. al[14]proposed block feature correlation based watermarking with linear equation.By using a pair of watermark pixels as the coefficients of linear function the authentication number is created. The central pixel of host block is as the input data to the linear function. The authentication information of that block is then embedded into host image using revisited embedding procedure of LSB matching. In detection stage, LSB matching revisited applied to extract the authentication information and verify whether the image block have been tampered with. The authentication information establishes the block feature correlation and this kind of correlation helps to resist VQ attack.

Surya BhagavanChaluvadi and Munaga V. N. K. Prasad[15] proposed dual watermark scheme for image tamper detection and recovery. Each block in the image contains watermark of other two blocks means two copies of watermark of whole image is maintained and provide second chance for block recovery in case of one copy is destroyed. They divide entire image into non overlapping blocks of size 2x2 pixels. Pad 3 LSB of each pixels zero and take average intensity is calculated using new pixel values and this average is presented in 8 bits. Then take 5MSB of average intensity of two blocks and make 10 bit watermark from 12 bit watermark and remaining two bits of watermark are generated by parity check of 10 bit generated watermark and parity check of average intensity of block. Experimental results shows low tamper detection rate and they are work only for grayscale images.

Wu Penghui et. al[16]proposed watermarking based scheme using block compressive sensing for tampered image detection. First the image is divided into sub blocks whose size can be changed by data quantity of watermarking and tamper detection accuracy. By using compressive sensing of Fourier matrix the sub blocks are observed. The observing results were combined to form the watermarking which will be embedded to whole image. By using Fourier measurement matrix the possible forgeries are localized.

CONCLUSION

Digital Watermarking is very useful technique for detection of tampering, localization and recovery of image. In this paper, survey of different tampering detection techniques based on spatial domain and transform domain are presented. Each method has its own positives and negatives. According to literature review different algorithm/method techniques of watermark embedding cause distortion to original image. Distortions will very badly affect the image. In Proposed work use watermark method which reduce distortion of image and detect tampering. Also prove effectiveness of method with different parameters like PSNR, EBR.

REFERENCES

[1] MadhuriRajawat, 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 NetworkTechnologies,pp.638-642,IEEE 2015.

[2] Mohmmad Ali M. Saiyyad,Nitin N. Patil, "Authentication and Tamper Detection in Images Using Dual Watermarking Approach", IEEE 2014.

[3] SawiyaKiatpapan,Toshiaki Kondo, "An Image Tamper Detection and Recovery Method Based on Self-Embedding Dual Watermarking", IEEE 2015.

[4] 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.

[5] 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, 2013.

[6] Md. Moniruzzaman, Md. AbulKayumHawlader and Md. FoisalHossain , "An Image Fragile Watermarking Scheme Based on Chaotic System for Image Tamper Detection" , 3rd INTERNATIONAL CONFERENCE ON INFORMATICS, ELECTRONICS & VISION 2014, IEEE.

[7] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN),pp. 709-716.
[8] Pradyumna Deshpande, PrashastiKanikar, "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] SajjadDadkhah, AzizahAbdManaf,SomayehSadeghi, "Efficient Two Level Image Tamper Detection Using Three LSB Watermarking", Fourth International Conference on Computational Intelligence and Communication Networks, pp.719-723,IEEE.
[10] Motoi Iwata, Tomoki Hori, Akira Shiozaki, and Akio Ogihara, "Digital Watermarking Method for Tamper Detection and Recovery of JPEG Images", IEEE 2010.
[11] 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.
[12] Song Qiang, Zhang Hongbin, "Image Tamper Detection and Recovery Using Dual Watermark", IEEE 2010.
[13] Luis Rosales-Roldan, Manuel Cedillo-Hernández, Mariko Nakano-Miyatake, Héctor Pérez-Meana, "Watermarking-based Tamper Detection and Recovery Algorithms for Official Documents" , IEEE 2011.
[14] 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.
[15] Surya BhagavanChaluvadi, 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), pp.993-998,IEEE 2009.
[16] Wu Penghui, Yang Bailong, Mao Jing, Zhang Zhongmin, "Block Compressive Sensing Based Watermarking scheme for image tampering detection", IEEE 2012.