International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.512-519
DOI: http://dx.doi.org/10.21172/1.81.066
e-ISSN:2278-621X

REVIEW ON WATERMARKING SCHEME FOR IMAGE AUTHENTICATION AND TAMPER DETECTION

Nirali Jani[1] and Aashish Jani[2]

Abstract: The scopes of information interchange between the users of internet are increasing in exponential pattern .The challenges are equivalently increasing with regards to image authentication and tamper detection. In recent days, the use of image segmentations in watermarking has been found to increase the performance of image tamper search significantly to extract a manipulated region so that prove the authenticity of image. In the various studies, novel characteristic of the watermarking such as pixel based and segments based image watermarking has been studied to embed watermark and help to find tamper segment of cover image as well as tamper watermark. Spatial and frequency watermarking algorithms reviewed as pre-processing steps for find tamper region and authentication of images. Here we reviewed various watermarking schemes for tamper detection and image authentication and find a novel concept of superpixel segments watermarking.

Keywords: superpixel segmentation, fragile watermarking, tamper detection, image authentication

I.INTRODUCTION

Although traditional data authentication technology for message integrity verification was mature, image authentication and tamper detection is still in its development stage, and many significant questions remain open. Many spatial and frequency domain techniques for authentication and tamper finding can be reviewed and examine for fragile and semi-fragile watermarking. Operating on pixel-based algorithms and block based method generally ignore the image content and so it fail to detect tampered block exactly. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values and same with blocks pixels. Watermarking techniques are rule on on the basis of their performance on a small set of different properties.

II.REVIEW WORK

Following are some watermarking methods are reviewed.
Dr. N.Shivananda [1] proposed fragile watermarking scheme for tamper detection and recovery of digital image in which image is devided into blocks and PN sequence generated for each block. Watermark in form of LSB of each pixel value in each block.when watermark extracted from each block parity check method applied for block is tampered or not. Here author used grey scale images for tamper detection and

1 *BM College of computer Application, surat*

2 *SK Patel College of computer studies ,KSV, Gandhinagar*

recovery. Author took different size of blocks for images and analysis that small size blocks gave more tamper detection rates. He tampered watermarked image with insertion, deletion , modification of text and evaluated PSNR with existing system[2].Tamper detection and recovery percentage values in his system are more than achieved by existing system.Saiyyad M.A.M, Patil N.N[3] proposed dual watermark approach for tamper detection and authentication Of image. Here author generate first watermark UIC is the decimal number which is encrypted using the AES algorithm which provide efficient way to encrypt the BCD code. After that he divide image into block and each block converted into DWT domain up to two level decomposition with LL band. Hash code can be calculated on dual watermark embedded image. If it not matches then image can be tampered. Here author used fragile invisible grey scale image with the size512*512 .PSNR and SSIM obtain through this method are satisfactory.S.P.Mohanty, B.K.Bhargava [4], proposed watermarking scheme for authentication of image embedding and extraction of digital watermark. Author used block segmentation for generating synthetic image, compound watermark contain user watermark and image statistics data and embedded into original image. For watermark creation and insertion process. he use DCT domain for block segmentation and PR seed key sequence with the scaling factor for making watermarked image. During extraction and authentication process author compute IDCT from extracted watermark and PR number. He verified compound watermark image with scaling factor with correlation detector. If it match then authentication proved. Author's algorithms results for grey scale and color image observed that watermark present after most of the attacks so it proves authentication. The average PSNR using this algorithm for all the test images, watermarks, and attacks is 24dB. Yuhang Li, Ling Du [5], proposed watermarking scheme for image tamper localization and self-recovery. Here author used two watermarks for authentication and recovery respectively with the use of chaotic function which guarantees the safety of our two types of watermarks and it encrypt cover image then after wavelet based watermark embedded to make scheme tolerable against manipulation. For generation of recovery watermark author used IntWT for low computational complexity. Author test tamper recovery performance under malicious tamper and JPEG compression, noise addition, brightness/contrast adjustment and format conversion. Image tamper localization, he use two quantitative measures PDA (Pixel Detection Accuracy) rate and PFP (Pixel False Positive) rate to evaluate the performance of our localization performance. Experiment results shows that effectiveness of this method is sensitive against malicious tamper and robust to some incidental manipulations like JPEG compression, slight noise addition, brightness/contract adjustment and format conversion. Wei-Che Chen, Ming-Shi Wang [6], proposed block based fragile watermarking scheme with the use of Fuzzy c-mean (FCM) clustering for image authentication and tamper detection.FCM create relationship between blocks of image.it is also effective for attacks like cut and paste and VQ attacks. The scheme consists of two procedures: authentication data embedding and tamper detection. Authentication data is generated by combining the membership matrix with a secret-key-generated random sequence. Authentication data is embedded into two least significant bits (LSBs) of each image block. Generate feature sequence and random sequence by PRNG with secretes key Sk used for data embedding for authentication. Here author used 8bit grey scale image with different sizes256*256 and 320*240 pixels. The image quality of each watermarked image got through these schemes is greater than 40 dB, so it's better imperceptibility. TP rates

achieved by the proposed scheme under different attacks are close to 1.so this high values indicate this scheme can effectively survive various attacks.

Oussama Benrhouma,Houcemeddine Hermassi Safya Belghith [7], proposed algorithm use cat map and consider approximation coefficient of discreate wavelet decomposition as the watermark inserted in remaining coefficient. He proposes a semi fragile watermark for tamper detection and partial recovery for images. This scheme also used chaotic methods with private keys for embedding and extracting the watermark. At the time of detection this method is perform blind detection and gives good result to locate tampered areas. Author used cat map iteration on the 4×4 blocks of the 256×256 image, and DWT with coefficient cA cH, cV and cD with the low_D and high_D for decomposition of image and with IDWT recreates the original image from its coefficients by using an up sampling process and the two filters Low_R and High_R with grayscale image. After IDWT author applied inverse cat map permutation and reconstruct the watermark image.for tamper detection author use the steps like Image decomposition, Block permutation, DWT decomposition, Estimation of the approximation coefficient cAP, Construct the approximation coefficient error for each block, Construction of the error image block, Inverse cat map permutation, Witness image reconstruction, Recovery of the original watermarked image blocks, Reconstruction of the recovered image. Author used true-positive rate (TPR), false-positive rate (FPR) for tamper detection performance. The proposed algorithm should have neither high nor low level of TPR because it is semi-fragile algorithm. The proposed algorithm resists most common image processing operations which cannot be considered as a forgery attack. Eugene T. Lin ; Christine I. Podilchuk ; Edward J. Delp III [8], proposed a semi fragile watermark for image authentication and tamper detection with the lozzy compressed watermarked image. He proposes a technique based on spread spectrum watermarking with modified detector which makes correlation of pixels in spatial domain.insted of using whole image he detect each block of image for altered region identification.in this scheme watermark generated in DCT domain which resist from jpeg compression.8*8 block, PR-zero mean and unit variance Gaussian number used in each block for watermark. Any embedding at AC high frequencies is to be destroyed by lossy JPEG compression and DC unmarked because non zero value added which are not contribute to the detector. Detection can be done with the block by block and compared it with a threshold of the block authentic block or altered. Block correlation detector is based on the differences of adjacent pixel values in the spatial domain. Here noted that large regions of image are smooth and edges and textures of image increase the probability of erroneous detection. Author concludes that under reasonable compression watermark image contain 75% and 90% on light compression of semi fragile watermark image accuracy. Here one thing we noted that block size also plays role for performance result .To detect tampering, larger block size in practical application gives better performance. PL Lin, PW Huang, AW Peng[9],proposed a method for image authentication with localization and recovery using fragile block wise and content based watermarking. Here author used encrypted signature for watermark which contain CRC check sum for authentication of it , block location, content of other block. Here Diffie-Hellman key exchange method makes the scheme robust against collage attack.8*8 pixels and above size of tampering can be detect and localize with recover 40%damage image can be major by this scheme.it is also more robust against VQ attack and higher tamper detection rate using block signature generation method. CRC-r checksum, where r can be 8, 16, 24, or 32, based on the system's requirement for security and quality of recovered image. If r is larger than

more information loss and it cause the system to give the recovered quality image so maintain r as low to reconstruct a higher quality image. For signature authentication extraction author use block LSB with CBC-3DES for verification and error recovery. Author experiments tamper localization, recovery when CRC-8-coded watermark used, and cropping attack. If lower cropped image watermark recovered ratio is less in phase1 restoration.

Terzjia N, Repges M, Luck K, Geisselhardt [10] has proposed a method for improving efficiency and robustness of the image watermarks. Three different ECC code, BCH, Hamming code and Reed–Solomon code are applied to the ASCII representation of the text which is being used as watermark. In order to be able to use only 7 bit ASCII instead of 8-bit ASCII value, this changed thereby allowing the use of BCH and Reed–Solomon codes. For embedding, the original image is decomposed up to 2 levels using the DWT with the pyramidal structure and watermark is added to the largest coefficients in all bands of details which represent the high and middle frequencies of the image. The Reed–Solomon code shows the best results due to its excellent ability to correct errors. Sergio Bravo-Solorio, Asoke K.Nandi [11], proposed image watermarking method with improvement of tamper localization and self-recovery for image authentication. Author used secure block wise method and iterative pixel wise method which are robust to cropping attack s and localise distorted blocks of pixels. This scheme is effective for reconstruction of cover image when 5% of its total number of pixels cropped .here watermarked image contain pixel wise and block wise embedding with a security key and detect the tampering each single block wise with the LSB of every pixel of image for watermark availability if it there then pixel wise detection validate pixels to improve the localization and recovery done with the existed secrete key. Proposed system's performance depends on size of tampered region detection and proportion of altered pixels of images. Image tampered area extended up to 10% of total pixel then 50%of pixels could be received by using 3LSB method as a part of proposed system. Radu O. Preda [12] , proposed a semi fragile watermarking for tamper detection and image authentication using wavelet domain. DWT based 2 level decomposition on the greyscale image can be used for experiments. Here for watermarked image generation, wavelet sub band selection after decomposition of original cover image can be done like LH HH HL with the random permutation and passing the secretes key k with wavelet coefficient grouping after that watermark can be embedded. Here author used inverse permutation and IDWT for watermark image encoding. For decoding and authentication work erosion and dilation can be applied after filtering process. Here algorithm detects exact tampering region and tampering during JPEG compression and VQ attack. This scheme obtains high quality and high detection of tampering with a low watermark payload. Xinpeng Zhang, ShuozhongWang, ZhenxingQian, GuoruiFeng [13] , proposed a jpeg image authentication using fragile watermarking which can be obtain by folding hash bit to reduce amount of watermark data and hash value obtain from DCT image coefficient with original zero value create a spare space of each block for accommodate watermark data and using reversible watermarking scheme each block of image carry two watermark bit. Here cover image alterations is small and during extraction process . HongJie He, JiaShu Zhang, and Heng-Ming Tai [14], proposed scheme for image authentication based on wavelet based fragile watermarking in which it finds that whether modification done with the content or embedded watermark and if watermark modified then it cannot affect the authenticity of image. Here author used 1level DWT with LL coefficients band for watermark creation and chaotic systems are embedding using LSB method to set m*n

image to zero. It also provides security against VQ attack, transplantation attack and localizes tamper region of host image. Here author used secrete key with 4-bit non-uniform scalar quantization method with LL band of obtain the image with a block size 2*2 so embedded watermark image W is a same size with original grayscale image. During the authentication process, using predefined threshold T modification identify in content of image or watermark and also localize the areas of changes on image content. Here author also introduced new feature called tamper discrimination of watermarked image.

Raphael C. and W. Phan [15], analysed block based image authentication scheme. Here author shown how to tamper with both the watermarked and unwatermarked pixels of an image that has been processed with the existing image authentication scheme of Chang et al.Results disprove the security claims of the scheme and conclude that it is not suitable for its designed purpose of image authentication and rightful ownership. Author show how the existing Chang et al. watermarking scheme cannot strictly tampered pixels of the image blocks so authentication of ownership they cannot individually bind. Here author tampering the existing scheme of Chang et al and claim for tampering in it. Author show some proposition to break the tamper resistance through divide the whole image into M $\times$ N pixels into M/2 $\times$ N/2 overlapping blocks of size 3 $\times$3 pixels. Another proposition like with the secret key SK used to perform the watermark embedding and later image authentication process. Here SK is secret and known only to a single person, there is nothing that binds that secret SK to the identity of that person, and so there is no prove for image authentication. Here Author suggests redesigned the existing Chang et al scheme based on above proposition.

Shao-Hui Liu a, Hong-Xun Yao a, Wen Gao b and Yong-Liang Liu [16] proposed Fragile watermarks are used to determine if any watermarked digital content has been tampered, and differentiate tampered areas from non-tampered areas without referring to the original image. Scheme involves embedding process start from evaluate the difference between cover image and its chaotic pattern which can be used to improve the security of watermark algorithm. Here author also map the pixel value difference image into binary image which then insert into LSB of the main image. Here author use binary watermark with permutation transformation and inverse permutation for embedding watermarked image with using LSB biplane. This method is efficient, secure, blind image used and finds the exact tampered. Also reliable in still images. Author used feature extraction for old image and add key for authentication with old feature extraction so he finally obtain new feature extraction which are then form as a watermarked content. A cryptographic hash or message authentication code (MAC) function is used in this method. Here author analysed Walton scheme, Yeung–Mintzer scheme, Holliman and Memon block-wise or pixel-wise independent fragile watermarking schemes which are vulnerable to theirs attacks like Vector quantization attack and oracle attack. This scheme results high fidelity and excellent capability of localizing modified areas in watermarked image. Hong- Jie He, Jia-ShuZhang and FanChen [17] proposed self-embedding adjacent block based method for identify the tamper blocks. Here author used statistical detection method for analysis of tamper detection performance under collage attack and content tampering attack.Author address the above problem of Fridrich and Goljan.

Clara Cruz-Ramos, Rogelio Reyes-Reyes, Mariko Nakano-Miyatake,and Héctor Pérez-Meana[18] proposed block wise and content wise semi-fragile scheme for authentication tamper finding.here author segmented image as per ROI with watermark sequence 66 bits and embed it through DCT middle frequency band of

ROE. Watermark sequence and extracted sequence from ROE if match and its authenticated or its tampered. It works with only grayscale images and quality factor better than 70. Hongjie He · Jiashu Zhang · Heng-Ming Tai[19] proposed neighbourhood characteristics based tamper detection using statistical fragile watermarking .This method is capable for finding tamper pixel and resist against collage attack. Here author use steps like confirming low PFA decreasing PFR using NC matrix and enhance detection ratio for tamper pixel from image boundry.Author proposed NC based SDM method for block wise fragile watermarking scheme for image authentication. Here each blocks watermark data are scattered in whole image instead of the same or distinct block. It has high computation overhead.
Xiumei Qiao , Rongrong Ni and Yao Zhao [20] proposed fragile watermarking scheme for image authentication based on superpixel segmentation mechanism. Here author used superpixel region for watermark self-region embedding using chaotic system. Superpixel content is embedded into another neighbour superpixel region. Superpixel boundaries are marked for extraction process and detect tampered region. Author used Lsb method to embed the watermark into the image. This scheme resist against VQ attack. It also recovered tamper region. Yan Xing , Jieqing Tan [24] proposed method presents block svd for embedding colour watermark into colour host image and through Arnold transformation generate scramble image for security against some attacks like cropping etc. Here each blocks maximum singular value taken from block svd of host image using RGB channel. Because of into the maximum SVs of blocks of host image to resist the attacks of image processing .Singular Values of image matrix, watermark bits are embedded into host image. This scheme is robust to the Gaussian noise pollution, low pass filtering, lossy JPEG compression, rescaling, cropping and so on. But this scheme is not survive with large angle of rotation.

III.REVIEW FINDINGS

Existing all fragile watermarking methods usually divide an image into regular size square blocks which ignore the image content and so it fail to detect tampered block exactly. Fragile watermarking schemes partition the image into blocks of the same size to localize the tampered area but these schemes might be vulnerable to the collage and do not discriminate well whether the tampering is on the watermark or on the image content.[19][20]
Most of self-recovery watermarking schemes not vulnerable to the Vector quantization well. Some watermark embedding strategy inserted the watermark data of an image block into the other distant block instead of the same block makes the self-recovery watermarking algorithms difficult to detect and localize the possible tampering.[7][8][9] Sometimes tampered pattern will not be accurate so half of the tampered pixel cannot be identified by existing systems.
Blocks based watermarking methods often lead to ambiguous detection, miss matches of blocks, and decrease of detection performance of tampered region.[13][14][15]

IV.CHALLENGES

Existing fragile watermarking methods usually divide an image into regular size square blocks which ignore the image content and so it fail to detect tampered block exactly. Most of Block based fragile method cannot resists counterfeiting attack like VQ attack.

Dependency of blocks often leads to ambiguous detection, miss matches of blocks, and decrease of detection performance of tampered region.

V.CONCLUSION

In this paper, we have reviewed some of the watermarking techniques based on image authentication and tampered detection. A research challenges for the development of robust and computationally efficient watermarking schemes have been pointed out. There is no single technique that can provide satisfactory performance against all parameters and attacks. When many such pixel and blocks based approaches are used to improve multiple performance parameters, the combined effect need to be tested practically. Based on above reviewed work we find some novel approach of super pixel watermarking techniques which protect the integrity and authenticity of image and high tamper detection rate.

REFERENCES:

[1]. Chetan K.R, Dr. Nirmala Shivananda" A new fragile watermarking approaches for tamper detection and recovery of document images" 2014 IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI) Pages 1494 - 1498

[2]. Z. Qian, G. Feng, and Y. Ren, "Fragile watermarking for colour image recovery based on colour filter array interpolation", Lecture Notes in Computer Science, vol. 6184, Pages. 537-543, springer 2010

[3]. Mohmmad Ali M. Saiyyad, Nitin N. Patil" Authentication and Tamper Detection in Images Using Dual Watermarking Approach" Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), IEEE 2014 Pages 1-5

[4]. Saraju P. Mohanty, Bharat K. Bhargava," Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", ACM Journal Name, Vol. V, No. N, February 2008, Pages 1–24.

[5]. Yuhang Li, Ling Du,"Semi-Fragile Watermarking for Image Tamper Localization and Self-Recovery"IEEE SPAC2014 Pages 328 – 33

[6]. Wei-Che Chen, Ming-Shi Wang," A fuzzy c-means clustering-based fragile watermarking scheme for image authentication" Elsevier2007 Science Direct/Expert system Pages 1300-1307

[7]. Oussama Benrhouma · Houcemeddine Hermassi Safya Belghith," Tamper detection and self-recovery scheme by DWT watermarking", Springer Science+Business July 2014 February 2015, Volume 79, Issue 3, pp 1817-1833

[8]. ET Lin, CI Podilchuk, EJ Delp III," Detection of image alterations using semi fragile watermarks" Proc. SPIE 3971, Security and Watermarking of Multimedia Contents II, 152 (May 9, 2000)

[9]. PL Lin, PW Huang, AW 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) 2004 IEEE pages 146 – 153

[10]. Terzjia N, Repges M, Luck K, Geisselhardt W (2002)" Digitalimage watermarking using discrete wavelet transform: performance comparison of error correction codes" International Association of Science and Technology for Development, International Journal of Advanced Computer Research (ISSN (print):2249-7277-ISSN (online):2277-7970) Volume2 Number 4 Issue7 December 2012 pages 2277-7970

[11]. Sergio Bravo-Solorio,AsokeK.Nandi," Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities " Elsevier 2010 pp 728-739

[12]. Radu O. Preda " Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain" SciVerse ScienceDirect Elsevier 2012 pp. 367-373

[13]. Xinpeng Zhang , ShuozhongWang,ZhenxingQian,GuoruiFeng" Reversible fragile watermarking for locating tampered blocks in JPEG images" 2010 Elsevier pp 3026–3036

[14]. Y.Q. Shi and B. Jeon (Eds.):" A Wavelet-Based Fragile Watermarking Scheme For Secure Image Authentication" IWDW 2006, LNCS 4283, 2006. Springer-Verlag Berlin Heidelberg 2006 pp 422–432

[15]. Raphael C.-W. Phan. "Tampering with a watermarking-based image authentication scheme" Elsevier Pattern Recognition (2008) pages 3493 – 3496
[16]. Shao-Hui Liu a, Hong-Xun Yao a, Wen Gao b and Yong-Liang Liu." An image fragile watermark scheme based on chaotic image pattern and pixel-pairs"
Science Direct- Applied Mathematics and Computation (2007) pages 869–882
[17]. Hong- Jie He, Jia-ShuZhang and FanChen." Adjacent-block based statistical detection method for self-embedding watermarking techniques" Elsevier -Signal Processing 89 (2009) pp1557–1566
[18] Clara Cruz-Ramos, Rogelio Reyes-Reyes, Mariko Nakano-Miyatake, and Héctor Pérez-Meana"Image Authentication Scheme Based on Self-embedding Watermarking" Springer-Verlag Berlin Heidelberg 2009 pages 1005–1012
[19] Hongjie He · Jiashu Zhang · Heng-Ming Tai," A neighborhood-characteristic-based detection model for statistical fragile watermarking with localization" Springer Science+Business Media, LLC 2010 pages 307–324
[20] Xiumei Qiao, Rongrong Ni and Yao Zhao. "Superpixel-Based Watermarking Scheme for Image Authentication and Recovery" Digital-Forensics and Watermarking Volume 9023 of the series Lecture Notes in Computer Science pages 160-173
[21] Radhakrishna Achanta, Appu Shaji, Kevin Smith, Aurelien Lucchi ,Pascal Fua, and Sabine Susstrunk," SLIC Superpixels" EPFL Technical Report 149300, June 2010
[22] R. Achanta ,A. Shaji , K. Smith , A. Lucchi , P. Fua and S. Süsstrunk," SLIC Superpixels Compared to State-of-the-Art Superpixel Methods" IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume:34 , Issue: 11) Pages 2274 – 2282
[23] http://opencv-python tutroals.readthedocs.org/en/latest/py_tutorials/py_core/py_optimization/py_optimization.html
[24] Yan Xing , Jieqing Tan," A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation" IEEE Digital Media and its Application in Museum & Heritages, Second Workshop on Dec 2007 pages 3-8