Available online at www.elixirpublishers.com (Elixir International Journal)

Digital Processing

Elixir Digital Processing 115 (2018) 49954-49957

ISSN: 2229-712X

Image Segmentation Level Key Driven Image Tampering Detection and Localization Enhancement

Nirali N. Jani and Ashish N. Jani
P.P.Savani University, Kosamba BMCCA, SURAT.

ARTICLE INFO

Article history:
Received: 24 January 2018;
Received in revised form:
18 February 2018;
Accepted: 27 February 2018;

Keywords
Superpixel Segment,
Key Encryption,
Singular Value Decomposition,
Attacks.

ABSTRACT

To speed up the process of detection of tamper in an image it is withheld to segment the image, embed segment with watermark and key as to trace the tamper segment in which key is not found rather than tracing for entire image for tamper detection. Tamper detection algorithm based on superpixel segment level key encryption with svd based watermarking scheme is proposed. This method finds tamper location from watermarked superpixel segments of watermarked image. Secrete key embedded in each segment of watermarked image for finding tamper segment first. If keys not found from any of the segment that segment shows tamper segment of image then find area which is tampered from that segment. To improve the efficiency of the proposed tamper detection against various security attacks such as collage attacks, VQ attacks and content removal attacks. The experimental results shown that proposed tamper detection scheme is shows better performance in terms of efficiency of tamper detection rate higher than 99% in average complex attacks, 100% in common attack and tamper finding speed is 0.02 to 0.04 sec. in various attacks.

1. Introduction

Authentications of digital assets are increasing with the increasing data repository volume is the biggest challenge. This is creating image authentication and tamper detection as a challenge which is becoming more complex as volume size of data repository. Use of superpixel segments of an image can speed up existing pixel/block based algorithms and progress result cases. Block based method ignores the image content and so it fails to detect watermark exactly and tamper finding from tampered image. Utmost Block based watermarking method cannot resists some attacks like VQ attack, collage attacked. Image blocks interdependency sometimes leads to uncertain detection and so it decrease the detection performance of tampered segments.Requiring recognised ideal method as SLIC for image segmentation [1]. For the authenticity of digital image individual segment level watermark image embedment with key and extraction from each segment of watermarked image after decrypting key value of each segment and tamper detection with localization scheme that use watermarking techniques.

A SVD-based image tamper detection and self-recovery by active watermarking is proposed. A proposed aspect of singular values for each image block is utilized to improve the tamper detection rate. The author use combination of 4×4 and 2×2 block sizes for improvement of the image's quality. The proposed optimizations improved the scheme's security against several malicious attacks. The results of algorithm showed the strength of the algorithm in terms of accuracy, security and recovery in grayscale images and proposed a color image for the same. [4] Author proposed image watermarking scheme based on pixel level tamper detection using five most significant bits as a watermark bit and embed them into 3 most significant bits. He proposed logistic map and hashing technique for evaluating results of tampering pixels of image. Results from this proposed scheme of watermark and tampered data-PSNR near about 38db and tamper detection rate 99.38%. [5] He proposed a fragile watermarking scheme for tamper detection and recovery using singular value decomposition with 4*4 image blocks which further divided into 2*2 blocks for second level of tampering of image. Here author used self-embedding with block mapping and LSB scheme implemented for tamper detection of watermarked image. Results for grayscale image for 50% tamper rate will be 99.5% in average. Author scheme not applicable to colour image in detail. [6]

The existing algorithms are achieving on the entire space of image for localization and tamper finding. This sacrifices the processing speed. To optimize processing speed, one can segment the image and trace the desired segment for fast detection .This concept is implemented with the use of superpixel in which each segment in the process is embedded with key. This makes easier to trace the tampered segment where key is not found in the segment during process of detection.

Many other fragile watermarking algorithms applied against the various attacks like VQ attack, collage attack, content removal attack, cropping attack for tamper detection and localization. Present paper carried out experiments on color image with highest tamper detection rate and localization of tamper from image. The analysis and experiments results show better efficiency of the proposed scheme in terms of precise tamper localization and high tamper detection rate compare to previous methods.

Tele:
E-mail address: janinirali@gmail.com

2. Superpixel SVD-based segment level key encryption scheme for image tampering detection using watermarking scheme:

In this paper, Superpixel SVD-based segment level key encryption scheme for image tampering detection using watermarking technique is proposed. It divides an image into four segments and embed watermark image into it using singular value decomposition.The proposed key embedding into watermarked segment enable authentication of image. If the key from any of the segment is not mapped then tamper area of that segment is shown.

2.1 Segment based Watermark embedding scheme and Image Authentication

For image segmentation Super pixel based SLIC algorithm [2] used in the scheme.After getting all individual segments make svd on blue color channel of image. Proposed scheme embed watermark image's svd value of blue color channel into cover image. Because of authentication proposed scheme use SHA-3_256 for key embedding into each water marked segment of image.Reconstruct Superpixel and Join all the segments to get the Authenticated Image.

2.2 Watermark extraction and tamper detection:

The watermarked image tamper detection, localization and watermark extraction scheme is shown on figure1 and explain with following steps.

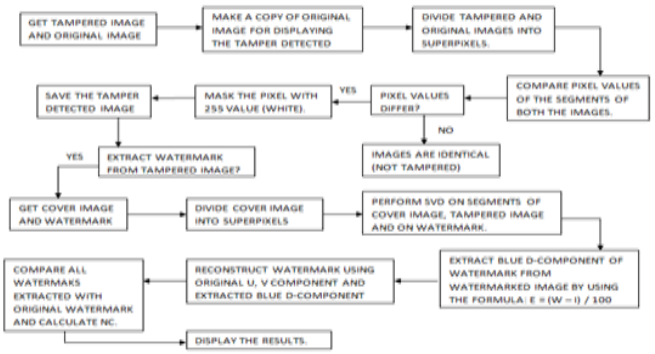


Fig.1. Block diagram of Tamper detection and watermark extraction.

The extraction process of watermark from watermarked image is opposites of embedding process.Tamper can be detected from each segment's pixel level comparison.The proposed scheme find key from each watermarked segment if it not found then those segments are tampered and then from only those segment consider for tamper finding and localization.From each tampered segment proposed scheme compare respective pixels of both the segments of tamper and original image. Read one segment at a time of both images and make a pixel-by-pixel comparison. Such that:

O (i, j) = T (i, j); where i and j are the row and column of both the images respectively.

If at any pixel index, the given equation turns out to be false, mask that specific pixel value to white.That is the value of that specific pixel will be changed to 255 (or 1).Repeat this process for every single pixel of the images.This will continue for each segment.Now join all the segments of tampered watermark image to construct final whole image for the tamper detection. Finally, proposed scheme will show that precisely only the region which was tampered has been masked out where rest of the image (including the pixels near to tampering) is unchanged and visible.

Proposed scheme has advantage like no need to find whole image for pixel wise tampering but only tampered segment in which keys not found are traced for tamper finding. So here proposed scheme takes less time and precisely localize tampered area of image compare to other pixel wise tamper finding methods. Also if watermark was manipulated then it shows tampering in watermarked image during tamper finding.

2.3 Attacks on watermarked Image

There are some attacks for tampering watermarked image in which tampering can be not detected easily.The proposed algorithm is tested on these various attack and shown tampering areas of them.The details of VQ attack, collage attack, content removal attack and cropping are as follows. [7][8]

(a) In collage attack, tampering occurs at specific location only. Therefore, we have fixed the locations at which object from another image can be added on the original image. There are three locations which are fixed for testing and out of these;any one will be selected randomly.The three locations are: Object will be added in the center of the image. This will give us tampering in each superpixel. Object will be added in the right half of the image. This will tamper only segments out of four of the image. Object will be added in the bottom left quarter of the image (3rd segment). This will tamper only one segment.

(b) In VQ attack, tampering occurs at random location. Therefore, we have set up two random functions each for extracting object from one image and pasting it on the original image.The task of each random function is as follows: First function randomly generates coordinates with the help of which a 100 x 100 pixel square is cut out of the image. The second random function generates the coordinates on the original image at which the extracted image is to be pasted.

(c) In content removal, we have to remove some information out of the image. Thus, we have set up a random function which generates coordinates for the image which is to be tampered. With the help of these coordinates the information of a 100 x 100 square area is removed from the image such that the location becomes black (0 pixels).

(d)In cropping attack, we have to crop the part of image like 10%, 20% etc. Detection of cropping part from the image can be localizing the area of image.

3. Performance Analysis and experimental Results:

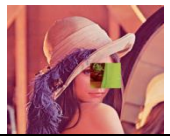
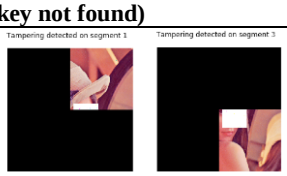
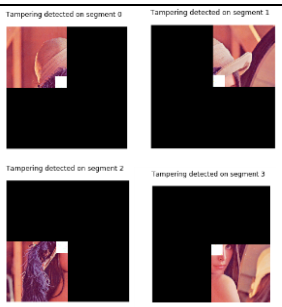
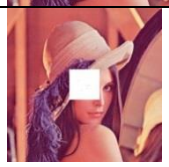
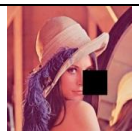
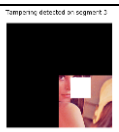
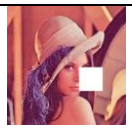
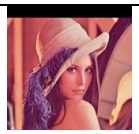
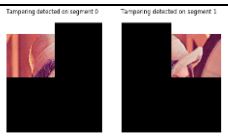
To check the performance of proposed scheme we are tested images of PNG BMP and TIFF format of different size and watermark with segment level key embedding and segment level tamper detection using tool PYTHON2.7. For this experiments and results more than 25 images analyst and tested. Here amongst them 2 PNG images analyst and tested with general attacks.In our experiments we use FPR, FNR and TDR majors for tampering of images are calculated VQ attack, Content removal attack,cropping attack,and collage attacks.

3.1 The embedment with key/ extraction of digital watermark is carried out on the segments as follows.

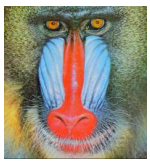
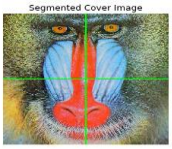
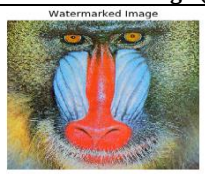
Cover image	Segmented Image	Watermark image	Watermarked Image (with key)	Extracted Watermark
				
Lena.png	4 segments	Peppers.png	PSNR: 48.3db	NC: 0.99

3.1.1 General tampering attacks:

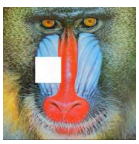
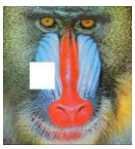
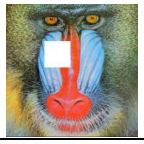
Following table shown tampering on watermarked image (Lena) and corresponding tamper detection and localization with TDR.

Attack Name	Attacked Image	Tamper Detected segment (key not found)	Tamper localization	TDR
VQ Attack				97.77%
Collage Attack				97.23%
Content Removal Attack				100%
Cropping Attack [10%]				100%

3.2 With the above same approach experiments other image for tamper detection and localization as follows.

Cover image	Segmented Image	Watermark image	Watermarked Image (with key)	Extracted Watermark
				
Baboon.png	4 segments	Peppers.png	PSNR: 47.88db	NC: 0.99

3.2.1 Following table shown tampering on watermarked image (baboon) and corresponding tamper detection and localization with TDR

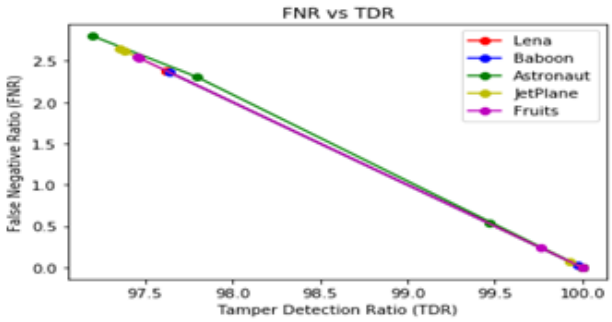
Attack Name	Attacked Image	Tamper Detected segment (key not found)	Tamper localization	TDR
VQ Attack				96.75%
Collage Attack				97.79%
Content Removal Attack				100%
Cropping Attack [10%]				100%

Results of above experiments show that Tamper detection Rate is about 97 % to 100 % in different attacks which is under acceptable range.

The proposed method was able to detect and localize common as well as complex

Attacks such as vector quantization, collage attack with tamper detection rate 96% to 97 %, and content removal attack; cropping attack with detection rate is 100%. Here FPR 0.0% average and FNR 0.02% average.

The proposed algorithm is robust against above attacks. In a pproposed method if any segment is tampered it cannot effect on whole image so still we can extract watermark like original one from any of untampered and tampered segments. Following chart analysis shows TDR and FNR Ratio for various tampered image.



FALSE NEGATIVE RATIO VS TAMPERING DETECTION RATIO

3.3 Evaluation Parameters:

Here PSNR is the ratio between the maximum possible power of the signal and power of corrupting noise and Normalized cross correlation (NC) is calculated to find similarity between original watermark and the extracted watermark from watermarked image. Results shown above both the parameter under acceptable range PSNR 48db and NC 0.99 to 1.0

For tamper detection rate for VQ attack, collage attack, content removal attack and cropping attack evaluated using FPR, FNR and TDR.

*FNR = (TamperUndetected_pixel) / (Tampered Pixels)) * 100*

*FPR = ((UntamperDetected_pixel) / (Untampered_pixel)) * 100*

*TDR = (Detected_pixel) / (Tampered Pixels)) * 100*

4. Conclusion

The proposed work watermarking Scheme for image tamper detection is implemented with the concept of segment level key encryption. The obtained result indicated that tamper detected from watermarked image comes under acceptable range its 97% and 100% in complex as well as common attacks respectively. Proposed scheme also speed up processing time for finding tamper from image and its 0.02 to 0.04 second in various attacks. This justifies the set target. The analysis of scheme in terms of the tamper detection rate, false positive rate and false negative rate validate the efficiency of tamper detection and precise localization of tampered watermarked image. The tamper detection algorithm to accurately detect the tampered segments even though the image is manipulated by attacks such as Collage attacks, VQ attacks, content removal attacks and cropping attack. The extension of this work is applied on external tampering with the use of deep learning concepts for color images.

References

1. R Achanta. “SLIC Superpixels” EPFL Technical Report 149300, 2010, Pg.no.1-15.
2. Radhakrishna Achanta, Appu Shaji, Kevin Smith, Aurelien Lucchi, Pascal Fua, and Sabine Susstrunk. “SLIC Superpixels Compared to State-of-the-art Superpixel Methods”JOURNAL OF LATEX CLASS FILES, VOL. 6, NO. 1, DECEMBER 2011
3. 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 pp 160-173
4. S Dadkhah, AA Manaf, Y Hori, AE Hassanie” An effective SVD-based image tampering detection and self-recovery using active watermarking” Elsevier Science Direct Signal Processing: Image Communication2014, pages 1-14
5. Shan Suthaharan,” Logistic Map-Based Fragile Watermarking for Pixel Level Tamper Detection and Resistance” EURASIP Journal on Information Security2010, Volume 2010, Article ID 829516,7 pages 1-7
6. IA Ansari, M Pant, CW Ahn “SVD based fragile watermarking scheme for tamper localization and self-recovery” Springer, International Journal of Machine Learning and Cybernetics December 2016, Volume 7, Issue 6, pp 1225–1239
7. 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
8. Raphael C.-W. Phan. “Tampering with a watermarking-based image authentication scheme” Elsevier Pattern Recognition (2008) pages 3493 – 3496
9. 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
10. 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