ISSN : 2231-0711

Deepali N. Pande et al | International Journal of Computer Science Engineering and Technology(IJCSET) | April 2014 | Vol 4, Issue 4,121-124

Generic Algorithm for Image Tampering Detection Based on Claimant Suspect Decision Rule

Deepali N. Pande[1], A.R. Bhagat Patil[2], Antara S. Bhattacharya[1]

[1]*Dept. of Computer Science & Engineering, GHRIETW 440016, MH., INDIA*
[2]*Dept. of Computer Science & Engineering, YCCE 441110, MH., INDIA*

Abstract—**This paper presents an innovative algorithm for image tampering detection based on forgery suspect generated by the claimant. The scheme has good scope for third party based authentication of raw images. The image at the sender side is shielded with security parameters generated from cumulative visual word from unique color features of the image. The recipient checks for the match with secret parameters shared commonly. A mismatch helps in generation of suspicion parameters which serves as a testament in generation of bag of features. The Euclidean distance is used as a metric in localization of tampered regions. The scheme successfully localizes copy-paste attack, image splicing and also transformation based attacks. The experimental results show accurate results in localization of tampering.**

Keywords-**image security, active tampering detection, passive tampering detection, image forgery detection**

I. INTRODUCTION

Advances in digital image processing technology have proved means for digital crimes. Ease of availability of advanced processing tools has hindered image security. Proving trustworthiness of image is a major challenge when transmitted raw. Some attacks are imperceptible and difficult to trace. Image forensic science is an emerging platform to resolve such problems. The general methodology used includes analyzing the contents of the image for detection of malevolent actions. Digital image forensics deals with development of such tools helpful for the problem domain. It is worth notifying that a certain algorithm cannot detect all possible attacks. Hence, the field of image forensics aims at developing tools for the corresponding purpose.

The field of image tampering detection is categorized into two streams namely active tampering detection and passive tampering detection. The stream of active tampering detection uses the in-built construct which was used to provide security to the image. A good example of this is watermarking. In such a method of active tampering detection, a security structure is embedded into the image. This structure is used for integrity evaluation in the sense that if any discrepancy is found with the structure then the image is tampered and an inverse analysis over the structure is done to locate tampered regions of the image. Various schemes for providing security to the image analogous to the concept of watermarking like, message authentication code, image hash, image checksum and image shielding were recently proposed as a counterpart to it. The stream of passive tampering detection deals with analyzing the raw image based on various statistics and semantics of image content to localize tampering of image. No construct is embedded in the image nor associated with it for security and hence this method is also known as raw image analysis. The localization of tampering is solely on the basis of image feature statistics. Hence algorithms and methods of detection and localization of image tampering vary depending upon the type of security construct used. But passive tampering detection typically aims for localization of tampering on raw image.

In this paper we propose an algorithm for localization of tampering based on claimant suspect decision rule. The sender transmits the image after shielding it for security. The receiver performs inverse operation for retrieving the security parameters to check its integrity. If parameters are violated, the image is declared as tampered image. The receiver claims for breaching of image security. So the image is judged as tampered. After this, to localize the tampered regions, the test image is analyzed with the tampering detection method proposed. The algorithm is described in detail under the section of proposed methodology.

The paper is organized into various sections. A discussion on past approaches used for tampering detection done under the section of theoretical background. The section system overview gives a detailed working of the proposed method. An evaluation of results obtained on varying tests is made under the section of results and evaluation. The conclusions are derived based on the results obtained under the section of conclusion and discussions.

II. THEORETICAL BACKGROUND

The platform of image forgery detection is vast and infinite. Due to advancements in image processing tools and their ease of flexibility, the task forgery creation is simplified. As discussed in the above paragraph, forgery detection needs a specific algorithm for a certain type of attack. In [1], the authors proposed an adjacent-block based statistical detection method for self-embedded watermarking. The method was based on active tampering detection. It used adjacent blocks of image in comparison with the test block to which a statistic-based rule was utilized to validate the block. The algorithm worked well for detection of content-tampering attack and collage-attack. Image splicing is also one of the types of image forgery. Authors in [2] proposed a Markov based method for detection of this specific attack. The method proceeded by first generating the Markov features from the probability matrices in the DCT domain. This was performed for inter-block and intra-block correlation between DCT coefficients of the block. DWT

domain was used to capture more features for describing wavelet coefficients across positions, scales and various orientations. The features obtained were then reduced using SVM-FRE. After then SVM was used to discriminate between feature vectors of spliced image and authenticate image. Another type of image forgery is copy-move forgery. One of the methods for detection of such type of forgery is proposed in [3]. The authors proposed J-Linkage algorithm. The algorithm uses feature extraction by clustering features with keypoint matching to discriminate the copied region. Image splicing is also a very common type of forgery wherein a composite image is obtained by copying certain portion of an image, transforming it and pasting into it. The image thus obtained is a composite of the original image. Authors in [4] proposed a method to detect such types of forgeries. They used the fact that a copied region shows a blurred boundary on the region and used edge detection for the same. The edges were divided into three types based on coefficients of non-subsampled contourlet transform. A six dimensional feature was acquired from each edge point. The feature consists of two non-subsampled contourlet coefficients, four statistics based on phase congruency. After that, support vector machines for each edge type were trained to detect blurred edge points. The local features were used to discriminate artificial blurred edge points. The analysis showed that the method proved robust in detection of splicing forgeries. Sometimes the portions inside the images are duplicated for breaching the semantic meaning of the contents of the image. The attacks based on this are categorized as region duplication attacks. Authors in [5], proposed the method for detecting such type of forgeries. The said attack is difficult to detect when the portion is applied geometrical transformations. The method proposed in [5], was based on acquiring Harris corner interest points from which descriptors of image sections based on step sector statistics were obtained. A matching on these sections of images was performed using best bin- first algorithm to find duplicate regions. The method worked well on images from two databases. One more type of image forgery attack is called image inpainting wherein the intruder modifies the image in an indiscernible form to remove certain regions from it thus changing semantic meaning of its contents. Authors in [6] proposed a technique for detection of inpainting forgeries specifically when such an image is stored in jpeg compressed format. The image under test is resaved and stored in jpeg format. Tampering is detected by computing averaged sum of absolute differences at different quality factors over tampered image and the resaved jpeg image. Authors in [7] proposed a region based tampering detection and restoring scheme. The scheme is based on the stream of active tampering detection. Recovery of tampered region was possible here by inverse analysis of the embedded information. The recovery feature is extracted by analyzing the image for homogeneity making use of quad-tree decomposition technique wherein the image is divided into variable sized blocks and the average value of every block is chosen as a feature. One more such scheme is proposed in [8] where the authors used semi-fragile data hiding. The method used the embedded binary signature and image digest for recovery of image blocks by modulating the integer wavelet coefficients using dither based quantization.

III. SYSTEM OVERVIEW

The proposed tampering detection and localization scheme is shown in the figure-1 and figure-2. The image to be transmitted by the sender is first shielded with an information security schema to help in tampering decision as described below. It is then transmitted to the receiver in the shielded form.

The recipient first unwraps to retrieve the hidden parameters from it. A matching is performed along with the secret information commonly known to the sender and the receiver. The visual word generation procedure is the secret information. A mismatch acts as the decision rule in tampering detection thus raising suspicion parameters for localization of tampering.

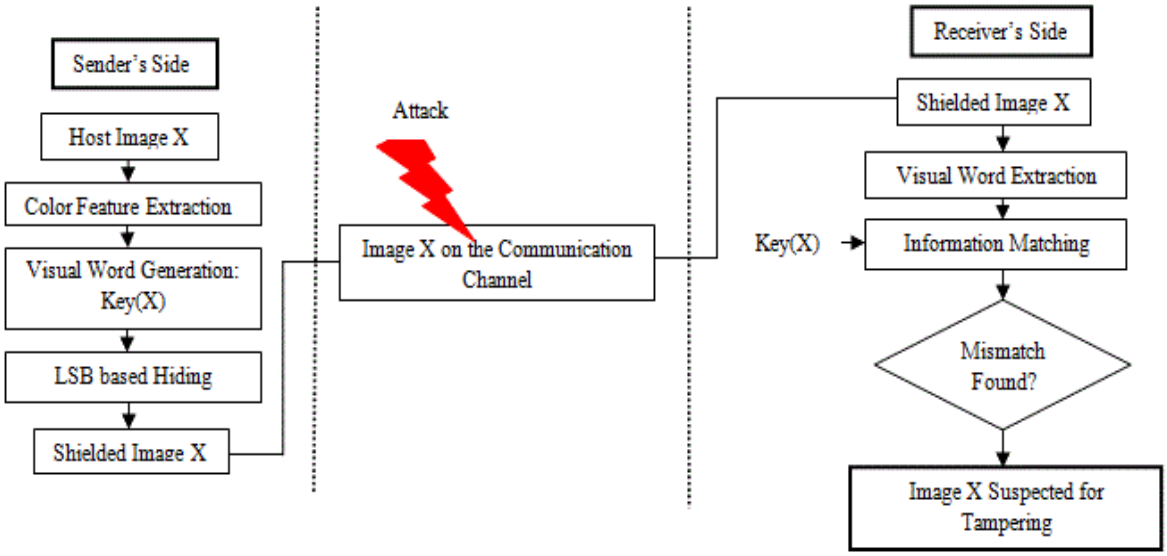

Figure1. Claimant Suspect Model for Tampering Detection

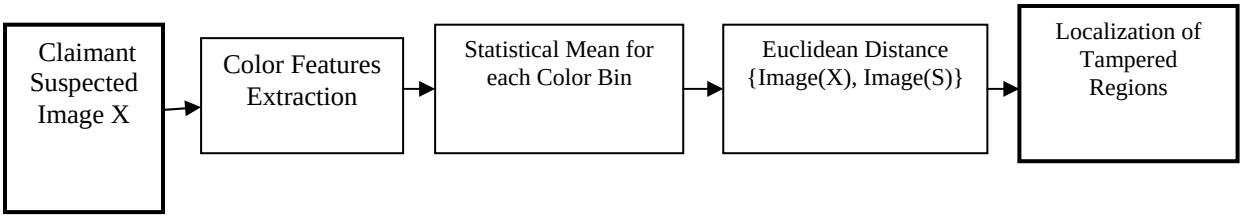

Figure2. Tamper Localization Model on Claimant Suspect Decision Rule

A. *Image Information Shielding*

The color histograms are acquired from the sender host image. Each bin of the histogram provides the number of pixels with the intensity as grouped by the corresponding bin. The statistical mean is calculated for each bin of the color histogram. The feature vectors are generated from each bin based on the calculated statistical means of each bin giving,

$$FV = < \mu_1, \mu_2, \mu_3 \ldots \mu_n >$$

Here 'n' represents total colors in the image. The feature vector represents the mean values of RGB intensities used in the formation of each unique color in the image. This feature vector thus forms a descriptor providing unique information about the image. Each feature vector is coded into ASCII format to form Visual word. These visual words are stored in the bag of features each for "Bag_of_Red", "Bag_of_Green" or "Bag_of_Blue" corresponding to the color band type. Suppose one of the colors in the image is white which is formed from equal intensities of red, green and blue. So the visual word corresponding to each will be stored in all the three bags. This information of the image is stored in the database. Also a cumulative visual word is generated taking from each bag the corresponding word of length 128 bit. This descriptive word is hidden in the lower least significant bits of the image randomly bitwise. The shielded image is then sent to the receiver.

B. *Claimant Suspect Tampering Decision Rule*

The Recipient of the Image extracts the hidden cumulative visual word. The secret information of visual word generation is known to the recipient. The key for generating cumulative word is provided in the extracted word in the form of tag information. The recipient performs matching for the retrieved cumulative visual word using the two secret information pieces. A mismatch indicates suspicion for tampering. The recipient then generates suspicion parameters as follows,

$$\textbf{Suspicion Parameters(X)} = \{key(X), (VW_c), X_t\}$$

Here key(X) is the key used for generation of cumulative visual word of image 'X', 'VW_c' is the cumulative visual word and 'X_t' is the tamper suspected image.

C. *Tampering Localization*

The Suspected Image is subjected for forgery localization along with suspect parameters generated by the claimant as described above. A set of descriptive features are obtained from the suspected parameters as follows.

$$\textbf{Bag\_of\_Features}(Xt) = key^{-1}(X).\{VW_c\} => "Bx_t"$$

An inverse algorithm as described above is applied to obtain each bag of features. After which, Euclidean distance is calculated on

$$D^E = \sqrt{(Bx - Bxt)^2}$$

Here 'Bx' represents Bag of features of the Sender image and 'Bxt' represents bag of features of the tampered suspected image. The Euclidean distance is calculated for each bag thus giving tampered blocks of the suspected image.

IV. RESULTS AND EVALUATION

The algorithm is designed in Java 2.0 and Mat lab is used as a tool for Verification of results. The proposed technique is innovative and results show good accuracy. The results for experimental analysis are tested using three different dataset of images. Some images were purposely tampered in order to check detection of various attacks as discussed in table-1. The following types of test images are taken into datasets. The statistical analysis shown in the table-1 gives fruitful evaluation of cropping based and rotation transformation based attacks. The parameters specified in the table were used for creation of forgeries to test the localization.

Here are some of results of localization of various attacks shown.

TABLE I.

Training Dataset	Attacks Detection				
	Deformation Induced		Statistics-Based Analysis		
	Cropping	Rotation	Mean	Standard Deviation	Histogram Intersection
Dataset 1	f(x) = 5%	(90°, 15, 20)	56.013e to 63.116e	15.33 to 16.12	0.45 to 1.5
Dataset 2	f(x) = 10 %	(45°, 25, 15)	43.229e to 33.117e	12.45 to 16.89	0.65 to 1.76
Dataset 3	f(x) = 15%	(35°, 10, 15)	23.244e to 37.665e	13.56 to 14.57	0.69 to 1.80

Different combination of transformations applied to the dataset and the range of statistical mean, standard deviation and values of histogram intersection obtained on them.

1. Image Splicing Detection

The proposed technique is utilized in the context where splicing operation is done. The technical meaning of splicing attack is that a part of an image is captured to perform transformations over it. The altered region is then pasted into another image to construct a new image with malicious semantics. The following shows the result of localization of splicing. The player is pasted into the original image.

Original image Tampered Image Tamper Localization

2. Copy-paste Forgery Detection

The following shows one of the results of localization of copy-paste attack from various images tested for this purpose. The portion in white shows copy-pasted part.

Original Image Tampered Image Tamper Localization

3. Transformed Images

The following shows one of the results for testing the localization capacity when the image is geometrically transformed using various parameters. The flower image shown is rotated 90°. Then the result of this transformation is tested for tampering localization.

Original Image Transformed Image Localization of Transformation

V. Conclusion And Discussion

A novel scheme for claimant suspect based tampering detection and localization has been proposed. The scheme shows accurate results as tested under different scenarios. As per the results of analysis, the scheme shows 98% true positives detection and the false positive detection rate is nearly negligible. The scheme shows localization of copy-paste attacks, transformation-based attacks and splicing based attacks as tested over various datasets. The method is tested over three datasets specially designed for testing the above listed attacks. The scheme has fruitful scope for third party authentication of raw images. The scheme will be enhanced for making recovery of tampered regions in near future.

References

[1] Hong-Jie He, Jia-Shu Zhang, Fan Chen, "Adjacent-block based statistical detection method for self-embedding watermarking techniques", Signal Processing 89 (2009) 1557–1566.

[2] Zhong wei He, Wei Lu, Wei Sun, Jiwu Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain", Pattern Recognition 45 (2012) 4292–4299

[3] Irene Amerini, Lamberto Ballan, Roberto Caldell, Alberto Del Bimbo, Luca Del Tongo, Giuseppe Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage", I. Amerinietal./SignalProcessing:ImageCommunication28(2013)659–669

[4] Guangjie Liu, Junwen Wang, Shiguo Lian, Yuewei Dai, "Detect image splicing with artificial blurred boundary", a Mathematical and Computer Modelling 57 (2013) 2647–2659

[5] Likai Chen, Wei Lu, Jiangqun Ni, Wei Sun, Jiwu Huang, "Region duplication detection based on Harris corner points and step sector statistics", J. Vis. Commun. Image R. 24 (2013) 244–254

[6] Yu Qian Zhao, Miao Liao, Frank Y. Shih, Yun Q. Shi, "Tampered region detection of inpainting JPEG images", Optik 124 (2013) 2487– 2492

[7] Kyung-Su Kim, Min-Jeong Lee, Ji-Won Lee, Tae-Woo Oh, Hae-Yeoun Lee, "Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging", Computer Vision and Image Understanding 115 (2011) 1308–1323

[8]Amit Phadikar , Santi P. Maity , Mrinal Mandal , "Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images", J. Vis. Commun. Image R. 23 (2012) 454–466

Authors' Details:

Deepali Pande is pursuing M. Tech in Computer Science and Engineering from GHRIETW Nagpur, affiliated to RTMNU, India. She has received the B.E degree in Computer Technology in 2010 from Yeshwantrao Chavan College of Engineering, RTMNU. She is an Assistant Professor in the department of Information Technology at KDKCOE, Nagpur.

Her research area includes electronic security and image processing.
Contact Details:
zivyi.77@gmail.com,
+919595488948

Antara Bhattacharya has received the M Tech degree in Computer Science and Engineering and B.E degree in Information Technology. She is currently working as a faculty for academics in M Tech computer science department at GHRIETW affiliated to RTMNU, Nagpur, MH, and India.

Her area of research includes Data Mining, Cryptography and Network Security.
Contact Details: antara.bhattacharya@raisoni.net
+919822713698

A.R. Bhagat Patil is an Associate Professor and Head of the Department of Computer Technology at YCCE, Nagpur, MH. India.
He is pursuing PhD and has received M.Tech degree in Computer Science and Engineering. His additional qualifications includes B.A. (Add.), Sociology, B.A.(Add) Political Science, D.I.A.M.S. His area of expertise includes Computer Networks and Security.
He has performed various R&D activities in multidisciplinary/Industry based Projects Industry Aligned Professional Electives (Infosys, Global logic), Research in thrust area, Computer and Network Security. He has published in 7 international journals, 9 international conference and 6 national conferences.
Contact Details:
arbhagatpatil@gmail.com
+919422827345