AN OVERVIEW OF SEGMENTATION-BASED IMAGE COPY-MOVE FORGERY RECOGNITION

MR.KOLKURE V.S.

Dept. Of Electronics,Bharat Ratna Indira Gandhi College Of Engineering,Solapur affiliated to Solapur university.

MS. PAWAR REKHA H.

PG student,Dept of Electronics,Bharat Ratna Indira Gandhi College Of Engineering,Solapur affiliated to Solapur university.

ABSTRACT
The digital data is continuously increasing since last decade. The development in the gadgets and the low cost internet leads to the wide use of the information in digital form. With these developments the cases of the data theft and misuse have been increasing continuously. The image copying and modifications leads to misuse of it, to address this problem there is the need of system which provides security to the images and also proves its authenticity. The Overview of the system for recognizing the image is discussed in this paper. The key point comparison and image segmentation plays very vital role in image security.

KEYWORDS: Image quality, segmentation, key point comparison, image detection, etc.

INTRODUCTION
The experiment is carried out to with segmentation of test picture in to independent patches. This method helps in detection of copy move section [1].Image exploitation are very common now a days. The feature is to be added to reduce the illustration superiority of the image upon copying it. The SIFT classification is found useful to address this problem. Identifying the copied images is really very important [2]. Multimedia communication development leads to the development of security to the digital data. The privacy of the user is very important when using the systems online and offline. Stolen data is misused several times and may results in loss of money, time and privacy [3]. Image segmentation is required for identification of images. The modification in the images with bad intentions are noticeable is recent time. The images should not be copied without the permission of the original owner of the image. The digital evidences are considered legal in many criminal cases now days and hence the images are really important [4]. The digital data in any patterns should be preserved and protected. Many valuable information is shared and stored in digital form and hence its necessity of time to protect the data [5]

The basic block diagram of the proposed system is shown below in figure1. The segmentation of the image is carried out before the feature extraction and this feature differentiates the proposed system from other present methods. After extraction the patch matching is carried out this is followed by transform estimation and transform matrix.
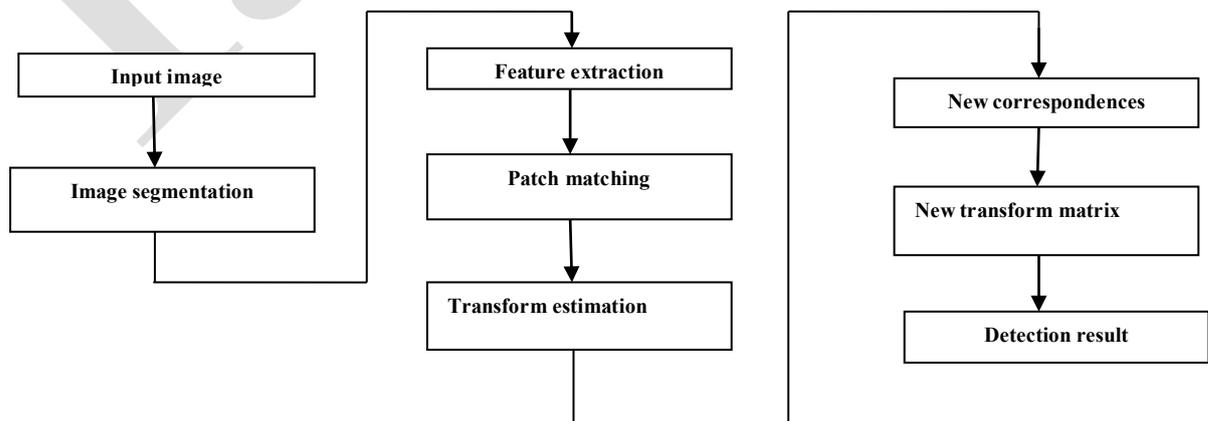
Basic block diagram of the proposed system

STEPS

Since the copied part is from the same image, the color character, noise components and the other properties will be compatible with the rest of the image, some systematic approach is needed to detect these forgeries. The general steps involved in copy-move image forgery are

A. Pre-processing

The scope of pre-processing is the improvement of image data and enhances features important for further detection. The image is converted into grey-scale when applicable. In both block-based and key-point based methods necessary pre-processing can be applied.

B. Feature Extraction

For block-based algorithms, feature vectors are extracted for each block. But in key-point based methods, feature vectors are computed only for key-points in the image such as regions with entropy etc.

C. Feature Matching

After feature extraction, the copy-move pairs are identified by searching blocks with similar features. High similarity between feature vectors can be interpreted as duplicated regions. In block-based method sort similar features and calculated approximate nearest neighbour in key-point based methods helps in the feature matching.

D. Filtering

Presence and absence of forgery on the basis of a single similarity criterion cannot be predicted. Filtering methods are used to reduce probability of false prediction. Finally post-processing can be adapted to preserve matches that exhibit a common behaviour

Table 1: Comparison of proposed system with existing system

EXISTING SYSTEM	PROPOSED SYSTEM
EXISTING CONCEPT: • We created a challenging real-world copy-move dataset, and a software framework for systematic image manipulation. • Experiments show, that the features SIFT and SURF, as well as the block-based DCT, DWT, KPCA, PCA and ZERNIKE features perform very well.	**PROPOSED CONCEPT:** • We propose a new framework for CMFD; the test image is first segmented into non-overlapped patches. • The aim of the first stage is to find the suspicious matches, and a transform matrix between them is roughly estimated. Then in the second stage we confirm the existence of CMF by means of refining the transform matrix.
EXISTING TECHNIQUE : • SIFT ALGORITHMS	**PROPOSED ALGORITHM:** • Key point Extraction and Description • Matching Between Patches
TECHNIQUE DEFINITION: Unlike block-based algorithms, SIFT methods rely on the identification and selection of high-entropy image regions. A feature vector is then extracted per key point.	**ALGORITHM DEFINITION:** • In the computer science field of artificial intelligence, genetic algorithm (GA) is a search heuristic that mimics the process of natural selection.
DRAWBACKS: • It takes more time consumption. • As presented, the copied regions are meaningful, i. e. either they hide image content, or they emphasize an element of the picture. • The software allows the snippets to be inserted at arbitrary positions.	**ADVANTAGES:** • It takes less time than existing system. • The block-based methods usually need a huge amount of time to detect an image. • In this regard, the key point-based methods are faster and more favorable than the block-based ones, because the number of the image key points is smaller than that of the divided blocks.

APPLICATIONS

1. To controlled environments like military systems and surveillance cameras.
2. with infringement of copyright, blackmail, insurance fraud and other schemes based on digital forgery
3. Face recognition on out-of-focused photographs, template-to-scene matching of satellite images, in focus/defocus quantitative measurement, etc.

CONCLUSION

The paper presents the overview of the segmentation-based image copy-move forgery recognition. The overview of the research work carried out in recent time is discussed. The proposed system is suitable for addressing the problem of image identification, security and providing the authenticity to the images. The

stoles images are widely used now days. The need of the time is to develop the system which accurately identifies the images and provides the security to images.

REFERENCES

1) Li, Jian, et al. "*Segmentation-based image copy-move forgery detection scheme." IEEE Transactions on Information Forensics and Security 10.3 (2015): 507-518.*

2) Amerini, Irene, et al. "*Counter-forensics of SIFT-based copy-move detection by means of key point classification." EURASIP Journal on Image and Video Processing 2013.1 (2013): 1-17.*

3) Lian, Shiguo, Dimitris Kanellopoulos, and Giancarlo Ruffo. "*Recent advances in multimedia information system security." Informatica 33.1 (2009).*

4) Chierchia, G., et al. "*PRNU-based detection of small-size image forgeries." International Conference on Digital Signal Processing (DSP). 2011.*

5) Lian, Shiguo, and Yan Zhang. "*Multimedia forensics for detecting forgeries." Handbook of Information and Communication Security. Springer Berlin Heidelberg, 2010. 809-828.*

6) I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "*A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6,no. 3, pp. 1099–1110, Sep. 2011.*

7) P. Kakar and N. Sudha, "*Exposing postprocessed copy–paste forg-eries through transform-invariant features," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.*

8) D. G. Lowe, "*Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.*

9) H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "*SURF: Speeded up robust features," Comput. Vis. Image Understand., vol. 110, no. 3, pp. 346–359, Jun. 2008.*

10) Q. Liu, N. Linge, and V. Lynch, "*Implementation of automatic gas monitoring in a domestic energy management system," IEEE Trans. Consum. Electron., vol. 58, no. 3, pp. 781–786, Aug. 2012.*

11) Q. Liu, G. Cooper, N. Linge, H. Takruri, and R. Sowden, "*DEHEMS: Creating a digital environment for large-scale energy management at homes," IEEE Trans. Consum. Electron., vol. 59, no. 1, pp. 62–69,Feb. 2013.*

12) M. A. Fischler and R. C. Bolles, "*Random sample consensus: A para-digm for model fitting with applications to image analysis and automated cartography," Commun. ACM, vol. 24, no. 6, pp. 381–395, Jun. 1981.*

13) R. Hartley and A. Zisserman, "*Multiple View Geometry in Computer Vision", 2nd ed. New York, NY, USA: Cambridge Univ. Press, 2004.*

14) M. Akhin and V. Itsykson, "*Clone detection: Why, what and how?" in Proc. 6th Central Eastern Eur. Softw. Eng. Conf. (CEE-SECR), 2010, pp. 36–42.*