Copy-Move Image Forgery Detection using SVD

Mr. Soumen K. Patra[1], Mr. Abhijit D. Bijwe[2]

[1]M. Tech in Communication, Department of Electronics & Communication, Priyadarshini Institute of Engineering & Technology, Maharashtra, India
[2] Assistant Professor, Department of Electronics & Communication, Priyadarshini Institute of Engineering & Technology, Maharashtra, India

---***---

Abstract - *The authentication of digital images has been questioned, because of the easiness with which these images can be changed in both its origin & content as a result of tremendous growth of digital image editing software. Digital image investigation is the latest research field which intends to authorize the authenticity of images. There are various methods proposed in digital forensics in recent years. Passive digital image tampering detection is one of it, which aims at verifying the authenticity of digital images without any a prior knowledge on the original images. A copy-move forgery detection is one of the passive technique which is created by copying and pasting content within the original image, and potentially post-processing it. In this paper, we use an improved algorithm based on Singular Value Decomposition (SVD) to detect this image forgery. In this method after applying image pre processing operations the image is divided in number of overlapping blocks. The SV features are extracted from each block. All these SV features are then lexicographically sorted so the blocks with similar feature come near to each other. By using Shift vector concept and for each shift vector a counter is incremented as many times as the same shift vector is computed, we can locate the copy move region in the image.*

Key Words: Singular Value Decomposition (SVD), Lexicographic sorting, Shift vector.

1.INTRODUCTION

From time-to-time digital images have been mostly accepted as evidence of the depicted happenings. Because of dominant in computer field, business and many more field, adoption of digital image as authorized document has become frequent .The easiness of use and accessibility of image editing tools and low-cost hardware, makes it very easy to manipulate digital images without leaving any trace of tampering. Therefore we can't take the authenticity and integrity of digital images for granted. This challenges the dependability on digital images in medical diagnosis, as evidence in courts, as newspaper items or as legal documents because of difficulty in distinguishing original and modified contents. Digital Image Forensic is that branch of science which deals to expose the malicious image manipulation. Digital investigation field has developed to combat the problem of image forgeries in many areas like medical images, forensics, intelligence, etc. In fig -1 sample case of image forgery is depicted.

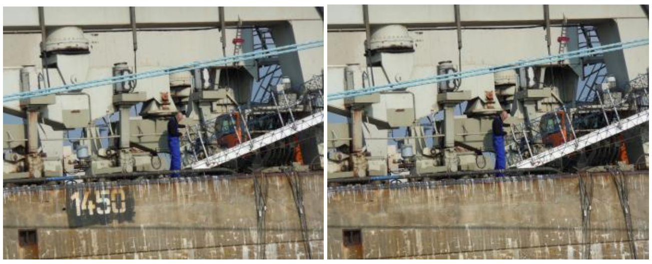

Fig -1: Example of a typical copy-move forged image. Left: The original image. Right: The tampered image.

1.1 Classification of Image Authentication Technique

Forgery detection intends to verify the authenticity of images. Several methods have been developed for verifying authenticity of images. In this paper we broadly classify the forgery detection technique into two classes: Active authentication and Passive authentication [1]. The classification is based on the fact that whether the prior information of original image is available or not. Under each class the methods are further sub-divided. The structure is shown in fig -2.

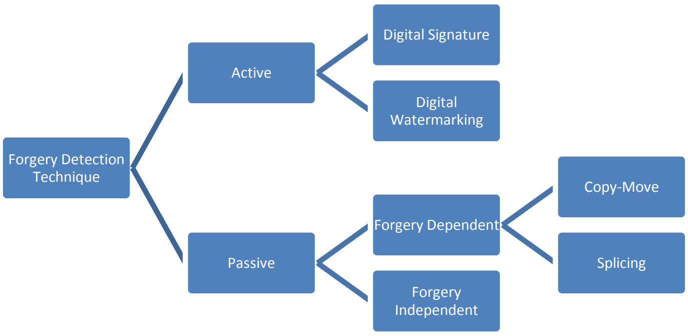

Fig -2: Block Diagram of Image Authentication Technique

In active authentication techniques earlier information about the image is essential to the process of authentication. It is related with data hiding where some code is inserted into the image at the time of generation. Verifying this code authenticates the image originality. Active authentication methods are then divided into two types –'digital watermarking' and 'digital signatures' [4-6]. Digital water marks are enclosed into the images at the time of image acquisition or in processing stage and digital signatures enclosed some secondary information, usually extracted from image, at the acquisition end into the image. A large number of work has been carried out in both the methods digital signatures [4-10] and digital watermarking. The main disadvantage of these approaches remains that they are to be inserted into the images at the time of recording using special equipments thus earlier information about image becomes essential.

Passive authentication is also called as image forensics is the process of authenticating images with no requirement of any past information just the image itself is enough. Passive techniques are based on the consideration that even though tampering of an image do not leave any visual trace but they are much likely to alter the critical statistics of an image. It is these inequality in image that are used to detect the tampering. For passive image forensics an exhaustive research survey has been carried out. Passive techniques are more divided as forgery dependent methods and forgery independent methods.

In Forgery dependent detection methods, it is designed to detect only some type of forgeries such as copy-move and splicing which are dependent on, what type of forgery carried out on the image. While forgery independent methods detect forgeries independent of forgery type but based on the fact that the traces left during process of re-sampling & due to lighting inconsistencies [12].

1.2 Copy–Move Forgery Detection

Copy-move is the most famous and common photo tampering method because it is easy to carry. It involves copying of some region in an image and moving the same to some content in other region of the image. As the copied region belong to the same image therefore the dynamic range and color remains similar with the rest of the image. An example of copy-move forgery is shown in fig -3.

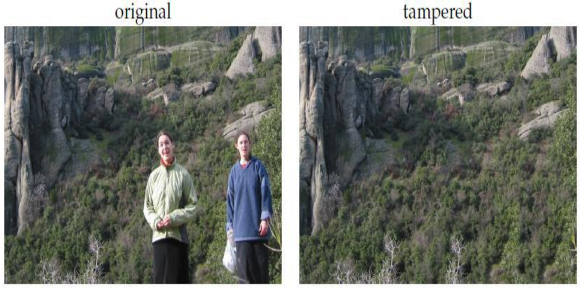

Fig -3: Copy- move Forgery (People in the Image are Masked by Pasting a Region Copied from same Image). Left: Original and Right: Tampered

The original image is altered to get the tampered image; persons in an image have been masked by copying a region from the same image and pasting it over there. Post processing operation like blurring is used to diminish the effect of border inconsistencies between the two images.

In this paper it is proposed to detect copy-move forgery of different post-processing operations on snippet. Our method is a block-based and extracting SV feature.

2.RELATED WORK

Among the initial efforts Fredrich [13] developed methods to identify copy-move forgery. Discrete cosine transform (DCT) of the image blocks were used and their lexicographical sorting is taken to ignore the computational burden. Once sorted the adjacent identical pair of blocks are taken to be copy-moved blocks. Block matching algorithm was used for make balancing between performance and complexity. This method included major drawback that it cannot detect small duplicate regions.

Popescu and Farid [14] suggested a method using principal component analysis (PCA) for the overlapping of the square blocks. The computational cost and the number of computations needed are comparatively get reduced O(NtN log N), where Nt is the dimensionality of the truncated PCA representation and N the number of image pixels. Sutthiwan et al., [15] presented a technique for passive-blind color image forgery identification which is a combination of image features extracted from image luminance by applying a rake – transform and from image chroma by using edge statistics. The technique gives 99% accuracy.

In the paper, Liu et al., [16] suggested use of circular block and Hu moments to detect the sections which have been rotated in the tampered image. Sekeh et al., [17] suggested a method dependent on clustering of blocks implemented using local block matching method. All techniques discussed above are able to detect and localize copy move forgery and cloned regions within an image are computationally complex and require human interpretation of the results.

3.PROPOSED METHOD

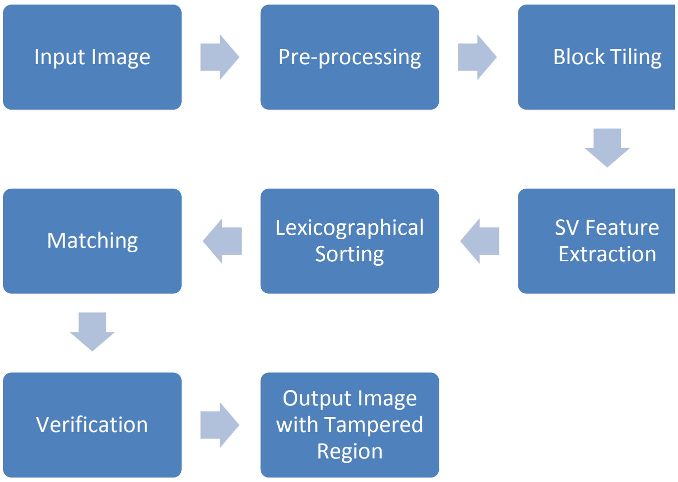

Fig -4: Block Diagram of Proposed Copy-Move Forgery Detection.

The detection method consists of following steps:

a. Initially some pre-processing steps are done on the given input image. These pre-processing step includes like, the conversion of RGB to Grayscale image and many more .

b. Let the input image be of M X N size and the square block of size b X b pixels is slide over entire image starting from upper left corner to lower right corner. For each block the SVD is calculated and SV features are stored. The theory of SVD is as follows:

The Singular Value Decomposition (SVD) is technique used over great extent to decompose a matrix into several component matrices, exposing many useful and interesting properties of the original matrix. It has mainly three properties i.e., scaling property, stability and rotation invariance which represents algebraic and geometric invariant properties of an image. SVD is very utile technique in data analysis and visualization. Let matrix A be any real valued matrix then it can be decomposed into three components i.e., left unitary matrix U, right unitary matrix V and diagonal matrix S having singular values on diagonally. If A is having m x n rows and column then equation 1 is called as singular value decomposition of matrix A.

$$Amxn = Umxm\ Smxn\ Vnxn^{T} \quad ...1$$

Where U = Left Unitary matrix.

V = Right Unitary matrix.

S = Diagonal matrix having singular values, diagonally in descending order.

As U and V are orthogonal matrix then their inverses are equal to their transpose, so the equation 1 can be rewritten as:

$$Smxn = Umxm^{T}\ Amxn\ Vnxn \quad ...2$$

c. The resultant block SV feature is stored as one row in the matrix M. The matrix M will then have (M-b+1)(N-b+1) rows and b columns in proposed algorithm. The (x, y) location of the block in image is stored in different matrix Mi.

d. The rows of the matrix M are then lexicographically sorted so that the similar SV feature vectos would come successively i.e., we can say that the corresponding blocks whose feature vectors come successively would be the candidates of block duplicates.

e. For each similar rows (x1,y1) and (x2,y2) the shift vector is computed as:

$$S = (s1, s2) = ((x1 - x2), (y1 - y2)) \quad ...3$$

As the shift vectors –s and s correspond to the same shift, the shift vectors s are normalized. For each matching pair of blocks, we increment the normalized shift vector counter C by one:

$$C(s1, s2) = C(s1, s2) + 1 \quad ...4$$

f. The shift vector counter greater than some threshold T, is examined and the related matching blocks which contribute to that shift vector are highlighted to mark copy-move forgery. The threshold value T is related to the size of the smallest segment that can be identified by the algorithm. Larger values might cause the algorithm to miss some not so closely matching blocks, while too small a value of T may introduce too many false matches.

4.RESULT AND ANALYSIS

The proposed method was applied to the images from the internet. It contains several original images and various types of post-processed copy-move forgery were applied to snippet of those images. Proposed algorithm method was able to detect the forgeries. The algorithm is implemented in MATLAB software. In fig -5, there are shown few images with copy-move forgery and the output image with detected forgeries by proposed algorithm. Results have shown that proposed algorithm can detect copy-move forgery when the post-processing operations like rotation, scaling, JPEG compression are applied to snippet before pasting. The table 1 shows the comparative analysis with PCA and SVD of the proposed algorithm.

Table -1: Comparative analysis of results

Methods	Copy-Move Forgery by Post-Processing:			
	Rotating snippet	Scaling snippet	Adding Gaussian noise to snippet	Snippet of smooth region
PCA	No	No	Yes	Yes
SVD	Yes	Yes	Yes	Yes

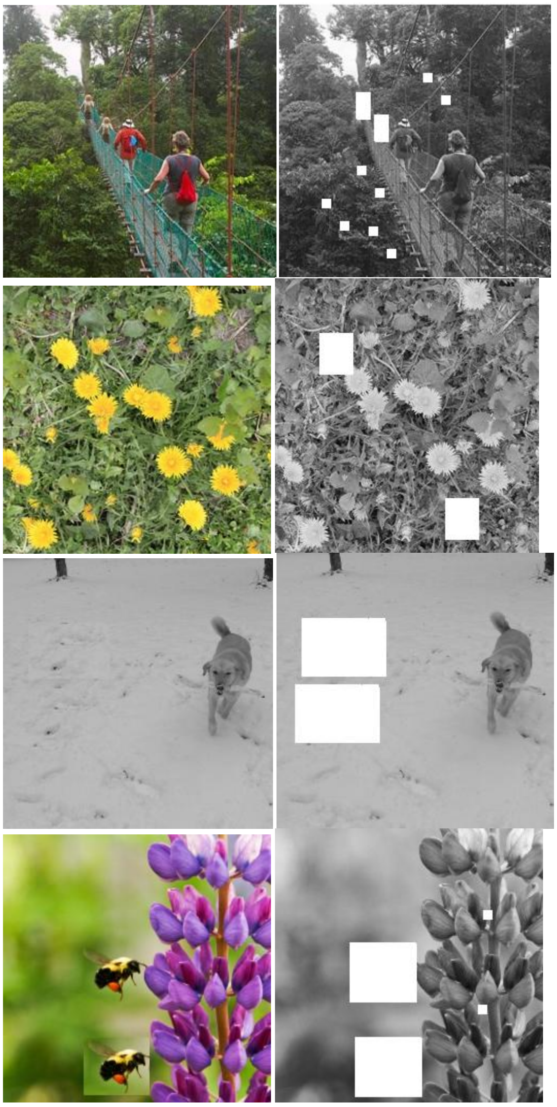

Fig -5: First column images are tampered and second column are the results of forgery detection by proposed algorithm.

5.CONCLUSION

Copy-Move forgery is mostly used technique to create forgery in digital images. To perform indistinguishable copy-move forgery, post-processing of snippet is performed. Proposed algorithm can detect forgery under post-processing operations like rotation, scaling and noise. We have applied sample images from internet which are shown in figure 4 to our algorithm and got desirable output as shown in figure 4. Proposed algorithm (SVD) has given a desirable output which is better than using PCA. SVD algorithm requires lower time than PCA in detection method. But as overlapping block size increases the total time required for detection decreases but false detection increases.

In future, the proposed method can be modified or extended to detect forgery by more post-processing operations on snippet and also can be extended to detect on color image format.

ACKNOWLDGEMENT

I would like to take this opportunity to express my profound gratitude and deep regard to my mentor Mr. A D. Bijwe, for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

I would also like to give my sincere gratitude to my sister Miss. Snehali N. Gadriye and to all my friends who filled in the survey, without which this research would be incomplete.

REFERENCES

[1] Shaba Mushtaq, Azaz Hussain Mir, “Digital Image Forgeries and Passive Image Authentication Techniques: A Survey”, International Journal of Advanced Science and Technology Vol.73 (2014), pp.15-32.

[2] N. Sebe, Y. Liu, Y. Zhuang, T. Huang and S.-F. Chang, “Blind passive media forensics: motivation and opportunity”, Multimedia Content Analysis and Mining, Springer, Berlin/Heidelberg, (2007), pp. 57–59.

[3] G. K. Birajdar and V. H. Mankar, “Digital image forgery detection using passive techniques: A survey”, Digital investigations, (2013), pp. 226-245.

[4] S. Katzenbeisser and F. A. P. Petitcols, “Information Techniques For Stenography And Digital Watermarking”, Norwood, MA: Artec House, (2000).

[5] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital watermarking San Fransisco", CA: Morgan Kaufmann, (2002).

[6] Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey", Digital Investigation 10 (2013) 226–245.

[7] C.-Y. Lin and S.-F. Chang, "Generating Robust Digital Signature for Image/Video Authentication", Multimedia and Security Workshop at ACM Multimedia '98, Bristol, U.K.

[8] C.-S. Lu and H.-Y. Mark Liao, "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme", IEEE transactions on multimedia, vol. 5, no. 2, (2003).

[9] H. Bin Zang, C. Yang and X. Mei Quan, "Image Authentication based on digital signature and semi fragile watermarking", Comput and technol, vol. 9, no. 6, (2004) November.

[10] X. Wang, J. Xue, Z. Zheng, Z. Liu and N. Li, "Image forensic signature for content authenticity analysis", Vis. Commun. Image R., vol. 23, (2012).

[11] K. XiaoBing and W. ShengMin, "Identifying tampered regions using singular value decomposition in digital image forensics", Proc. of International conference on computer science and software engineering, (2008), pp. 926–30.

[12] J. A. Redi, W. Taktak and J. L. Dugelay, "Digital image forensics: a booklet for beginners", Multimedia Tools Appl., vol. 51, no. 1, (2011), pp. 133–162.

[13] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy-move forgery in digital images", Proc. of digital forensic research workshop, (2003), pp. 55–61.

[14] A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515. Department of Computer Science, Dartmouth College, (2004).

[15] P. Sutthiwan, Y. Q. Shi, S. Wei and N. Tian-Tsong, "Rake transform and edge statistics for image forgery detection", Proc. IEEE International conference on multimedia and Expo (ICME), (2010), pp. 1463–8.

[16] G. Liu, J. Wang, S. Lian and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", J Netw. Comput. Appl., vol. 34, (2011), pp. 1557–1565.

[17] M. A. Sekeh, M. A. Marof, M. F. Rohani and M. Motiei, "Sequential straightforward clustering for local image block matching", World Acad. Sci. Eng. Technol., vol. 50, (2011), pp. 774–778.