Framework for Image Forgery Detection

Ms. Kaveri S. Nehe[1], Ms. Sneha R. Birajdar[2], Ms. Madhuri K. Ugale[3], Suwarna S. Ugale[4], Mr. Kishor N. Shedge[5]

[1],[2],[3],[4]BE Student, Dept. of Computer Engineering, SVIT, Nashik, Maharashtra, India.
[5]Head of Department (Internal Guide), Dept. of Computer Engineering, SVIT, Nashik, Maharastra, India.

Abstract - *Video copy-move forgery detection is one of the hot topics in multimedia forensics to protect digital videos from malicious use. Several approaches have been presented through analyzing the side effect caused by copy–move operation. However, based on multiple similarity calculations or unstable image features, a few can well balance the detection efficiency, robustness, and applicability. In this paper, we propose a novel approach to detect frame copy–move forgeries in consideration of the three requirements. A coarse-to-fine detection strategy based on optical flow (OF) and stable parameters is designed. Specifically, coarse detection analyzes OF sum consistency to find suspected tampered points. Fine detection is then conducted for precise location of forgery, including duplicated frame pairs matching based on OF correlation and validation checks to further reduce the false detections.*

***Key Words*: Artificial Neural Networks; GLCM features; Graphical User Interface; Machine Learning; Support Vector Machine.**

1. INTRODUCTION

There is a significant role of digital images in our everyday life. However, image manipulation has become very easy by using powerful software. Without any doubt image authenticity now is a big matter of concern. Two main types of image forensic techniques are available to verify the integrity and authenticity of manipulated image. One is active forensic method and another is passive forensic method and they have been explained in the literature precisely. Watermarking and steganography are two techniques which are used in active methods to insert authentic information into the image. When question arise about the authenticity of an image, then prior embedded authentication information is recalled to prove the authenticity of that image. However, embedding authentication information to an image is very confidential.

Only an authorized individual allows to do it or at the time of creating the image, authentic information could be embedded as well. Requirement of special cameras and multiple steps processing of the digital image are two main limitations which made this technique less popular. To avoid these limitations, the researchers are more interested in developing passive forensic technique as these methods utilize image forgery without requiring detailed previous information. The most popular method to construct forged image is copy-move forgery. It refers to copy one part from image, and paste it inside the same image. Sometime before pasting the copied regions, various post-processing operations like scale, rotation, blurring, intensifying or JPEG compression may be applied. The similarity regions between image clusters is used in this proposed method [4].

2. LITERATURE SURVEY

Generally, digital forensic techniques can be classified into active approaches and passive or blind approaches. Two typical active forensic technologies are watermarking [2] and digital signatures [3], [4], both of which embed specific validation data in visual media during their production; but these methods require specialized hardware, limiting their application. The passive or blind forensic approaches verify the genuineness by exploring intrinsic features in the media left by acquisition devices or manipulation acts, without using any pre-embedded signals. It is a new research field emerging in the last decade, and has been a promising tool in the authentication field of digital visual media [5]. However, most of the passive forensic approaches were devoted to the analysis of still images [6]. In recent years, researchers have increasingly focused on video forensics, not only because the amount of video data is increasing at an explosive speed, but also because video tampering is becoming more and more easy, to which a wide range of possible alterations can be applied, such as frame deletion [5], [7], frame insertion [8]–[10], and video compression [11], [12]. Among them, copy-move forgery to extend or hide specific objects in the same video is one of the common methods. It is fairly easy to operate, but difficult to distinguish since the moved objects or frames are from the same videos. Based on different operational domains, video copy-move forgeries can be classified into regional forgery and frame cloning. Regional copy-move tampering changes only parts of the frame images, which is similar to image copy-move, and can be detected by relatively mature image. forensic techniques [1], [13]–[15]. The second type, frame copy-move, occurs in the time domain. It is performed by copying successive video frames and pasting them to another non-overlapping position, aiming to conceal objects, clone regions, or extend the time of some specific activities to forge the event records. In frame copy-move forgery, cloning and pasting successive frames in the same video improves the imperceptibility and calculation difficulty, making it ineffective to detect the changes of color, shooting parameters, illumination condition, etc. [1], but it leads to abnormal points in the parameter distribution, and creates a high level of correlation between the original and duplicated frames. Based on this idea, different approaches have been developed to detect frame copy-move forgeries, which can be divided into two categories: image feature based and video feature based. Algorithms of the first category extract and explore image features of each frame to detect correlation, including gray values [16], [17], image texture [18], [19], color modes [20], and noise features [21], [22]. In the second category, they exploit the unique features in videos, such as motion features [23]–[25], video compression and coding features (including size, bitrate, and frame type) [26], [27] to analyze the side effect caused by copy-move operation. Although various detection solutions towards video copy move forgery have been proposed, current schemes are faced with the following challenges:

- High computation complexity. Pixel based or directly correlation based approaches generally suffer from high computational burden. It will be quite time consuming to analyze a large number of frames in videos with a bulk of data far greater than that of still images.

- Unstable detection performance. Methods based on image features, including texture, color modes, noise, and pixel gray values, are vulnerable to regular attacks or post-processing on videos, like secondary compression and additive noise. Few of the existing detection approaches take the detection robustness into account, and generally set fixed sensitive parameters for detection.

- Limited applicability. Some methods have restrictions to the detected videos in terms of video formats, number of tampered frames, tampering ways (only for unsmooth manipulation) or shooting ways (only with static camera), which limit the practical applicability in video forensics.

3. PROPOSED SYSTEM

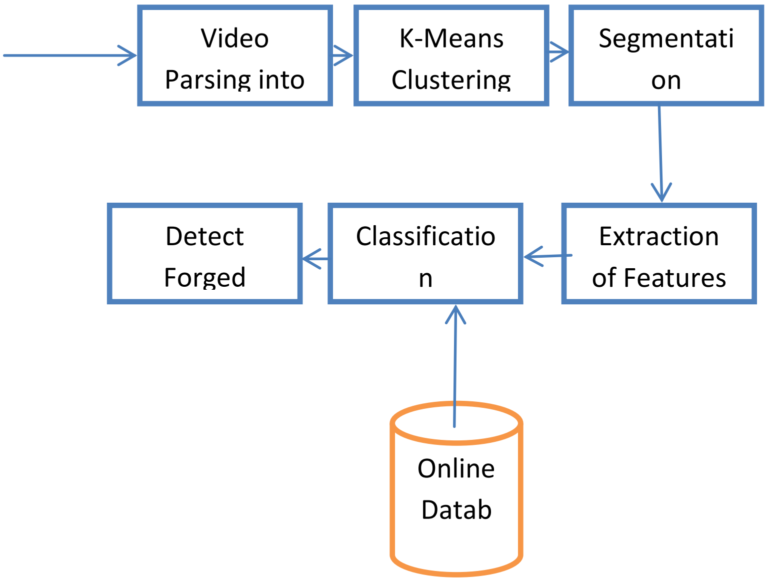

Fig 1: Block Diagram

A. CREATION Of NON-OVERLAPPED BLOCKS In this approach, the detected image is initially divided into overlapping blocks. The basic approach here is to detect connected blocks that has been copied and moved. The copied area consists of many overlapping blocks. The further step would be extracting features from these blocks.

B. FEATURE EXTRACTION TECHNIQUE After the creation of the overlapped blocks, the feature extraction technique is applied on the image to extract the features from specific block of the image. In this work approximation image local binary pattern features method is applied on the block region for extracting the features. AILBP (Approximation image Local Binary Pattern) Initially on the face images, bi-level wavelet decomposition method has been applied, which has been transformed face images into approximation images. Then, on approximation images, local binary patterns (LBP) have been used to extract local features of the face images. AILBP method is a combination of wavelets decomposition along with LBP method which is effective in terms of accuracy and it reduce time computation.

1. Wavelet decomposition Wavelet breakdown method is a occurrence of time and signal analysis method. It can be applied to decompose a forged image into many sub-band images with variation in spatial resolution, characteristic of frequency and directional features [21]. In this method, the approximation and details coefficients are computed by decomposing the face image up to two levels. Approximation coefficients pick the lowest frequency components and details coefficients contain the highest frequency component of an image. Only approximation coefficients are taken for further procedure. Approximation coefficients contain low frequency components of forged image, which contain whole information of the image. The variation of expression and small scale obstruct does not alter low frequency part but the high frequency portion of the image only. More than two steps decomposition of forged image result in information loss and hence, not involved in this work.

C. Identification of the duplicate Rows in a feature matrix In the feature matrix, each rows represents a specific blocks. In order to detect the duplicate rows, first from feature matrix, system finds out number of rows which original feature matrix is being compared with filtered out resultant rows which are duplicates. Hence, such comparison gives blocks which are duplicates in the feature matrix.

D. Detection of the Forged region After the identification of duplicate blocks, the further step is to highlight the duplicate blocks on the digital image, which also gives an indication of forged regions. Hence, system finally detects forged areas in the digital image. The corresponding forgered regions are being highlighted by the system.

Proposed Algorithm:

i. The standard database consists of original, forged and processed images is considered in the performance analysis.

ii. The images in the database are converted to gray scale.

iii. The statistical features are computed on GLCMs developed from the gray scale images.

iv. The Support Vector Machine is trained with those 20 statistical features for every image in the database using RBF kernel.

v. Statistical features of the testing image are obtained in similar process using steps 2 and 3.

vi. The SVM classifier classifies the image either to be authentic or forged

4. CONCLUSION

In the proposed system we are going to use ANN classifier for image forgery detection. ANN classifier gives the more accuracy than existing system.

REFERENCES

[1] R. Sekhar and R. S. Shaji, "A methodological review on copy-move forgery detection for image forensics," Int. J. Digit. Crime Forensics, vol. 6, no. 4, pp. 34–49, 2014.

[2] A. B. Pawar et al., "Data encryption and security using video watermarking," Int. J. Eng. Sci., vol. 4, no. 4, p. 3238, 2016.

[3] C.-S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," IEEE Trans.

Multimedia, vol. 5, no. 2, pp. 161–173, Jun. 2003.

[4] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Featurebased dynamic signature verification under forensic scenarios," in Proc.

Int. Workshop IEEE Biometrics Forensics (IWBF), Mar. 2015, pp. 1–6.

[5] C. Feng, Z. Xu, W. Zhang, and X. Yanyan, "Automatic location of frame deletion point for digital video forensics," in Proc. 2nd ACM Workshop

Inf. Hiding Multimedia Secur., 2014, pp. 171–179.

[6] P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Local tampering detection in video sequences," in Proc. IEEE 15th Int. Workshop Multimedia Signal Process. (MMSP), Sep./Oct. 2013, pp. 488–493.

[7] S. Milani et al., "An overview on video forensics," APSIPA Trans. Signal Inf. Process., vol. 1, no. 1, pp. 1229–1233, 2012.

[8] Z. Zhang, J. Hou, Q. Ma, and Z. Li, "Efficient video frame insertion and deletion detection based on inconsistency of correlations between local binary pattern coded frames," Secur. Commun. Netw., vol. 8, no. 2, pp. 311–320, Jan. 2015.

[9] J. Chao, X. Jiang, and T. Sun, "A novel video inter-frame forgery model detection scheme based on optical flow consistency," in Proc. Int. Workshop Digit. Forensics Watermarking, 2013, pp. 267–281.

[10] J. Yang, T. Huang, and L. Su, "Using similarity analysis to detect frame duplication forgery in videos," Multimedia Tools Appl., vol. 75, no. 4, pp. 1793–1811, Feb. 2016.

[11] X. Jiang, W. Wang, T. Sun, Y. Q. Shi, and S. Wang, "Detection of double compression in MPEG-4 videos based on Markov statistics," IEEE Signal Process. Lett., vol. 20, no. 5, pp. 447–450, May 2013.

[12] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in Proc. 8th Workshop Multimedia Secur., 2006, pp. 37–47.

[13] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Sci. Int., vol. 233, nos. 1–3, pp. 158–166, 2013

BIOGRAPHIES

Name: Kaveri S. Nehe
Educational Details:
B.E. Computer (Pursing.)

Name: Sneha R. Birajdar
Educational Details:
B.E. Computer (Pursing.)

Name: Madhuri K. Ugale
Educational Details:
B.E. Computer (Pursing.)

Name: Suwarna S. Ugale
Educational Details:
B.E. Computer (Pursing.)

Name: Mr. Kishor N. Shedge
Educational Details:
PHD (Pursing.)