A Review on Different Techniques of Video Tampering Detection

Sagar U Solanky[1] Prof. Hardik Patel[2]
[2]Professor
[1,2]Parul Institute of Engineering and Technology, Vadodara

Abstract— Video tempering , also known as video forgery, is a technique for generating fake videos by altering, manipulating, combining or creating new video contents. The recent development of video editing techniques enables us to create realistic synthesized videos .With the availability of different video editing tools ,technologies and softwares various types of videos are created from different perspectives As video editing tools are getting very complicated, modified videos are hard to detect. While using this advance tools for video falsifying it is very difficult to detect the forged or the manipulated videos.It is very important to detect the video forgery in some cases like low related cases .so, here we are Analysing the different techniues for the video tempering detection.

Key words: Blind detection technique, Correlation of noise residue, MPEG double compression, Tamura texture features

I. INTRODUCTION

In recent days due to easy availability video and image editing softwares it is difficult to authenticate the video or document . with high-quality data processing tools and algorithms, has made signal acquisition and processing accessible to a wide range of users.so, the single video and image can be process many times by the different users. Important details can be removed, ,deleted ,erased and hidden from the original video. and the true original source of the multimedia material can be concealed. validation of the legal property of multimedia data may be difficult since there is no way to identify the original owner.

There are basically two types of tempering detection techniques:

Active technique and Passive technique. In the active technique, a watermark is used to detect tampering. However, this scheme needs a facility to embed the watermark . On contrary, the Passive technique extract some intrinsic characteristics of image/video to detect the tampered regions.

In this paper we discussed about the different passive video tempering detection techniques. Here we are analyzing the different technique of video tempering dection like Blind detection method, MPEG double compression Method, Correlation of noise Residue method.

II. RELATED WORK

A. *Correlation of noise residue Method*

In this method block based technique is used . In this method concept of overlapping block is used. This approach is understand by following steps.

1) Step 1: Take forged video as input.
2) Step 2: video converted into frames
3) Step 3: Noise residues are extracted for each frame by subtracting the original frame for its noise free version
4) Step 4: Divide each frame into N×N blocks.
5) Step 5: Calculation of block level noise correlation value. The correlation value calculated by the below equation[1]. Where r is the correlation coefficient n(i,j) is the noise residue anh t is the frame –t is the mean of the t.

$$r = \frac{\sum_i \sum_j \left(n_{i,j}^{t} - \overline{n}^{t}\right)\left(n_{i,j}^{t-1} - \overline{n}^{t-1}\right)}{\sqrt{\sum_i \sum_j \left(n_{i,j}^{t} - \overline{n}^{t}\right)^2 \sum_i \sum_j \left(n_{i,j}^{t-1} - \overline{n}^{t-1}\right)^2}}$$

6) Step 6: Determine a particular threshold value.
7) Step 7: Thresholding via bayesian classifier.
8) Step 8: Forged region detected.

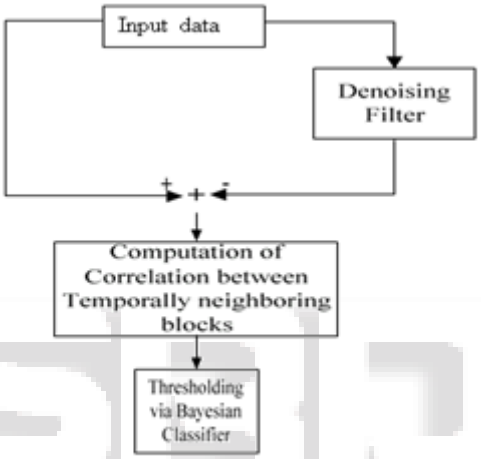

Fig. 1: Block diagram of Correlation of noise residue Method

B. *Blind Detection Method:*

In the first step of blind detection method video is converted into the frames.

Once the video is converted into the frames, the block matching is done between the two frames of the video then zero connectivity labelling is applied on block pairs to yield matching degree feature for all blocks in the forged region and construct ascending semi trapezoid membership function. Finally, the tempered regions are identified using a cut set.

The major weakness of this approach is that it is currently only applicable to uncompressed images and video.

The future work is proceed to detect forged video created by other inpainting techniques, so that blind video forencics can used in various forgery circumstances.

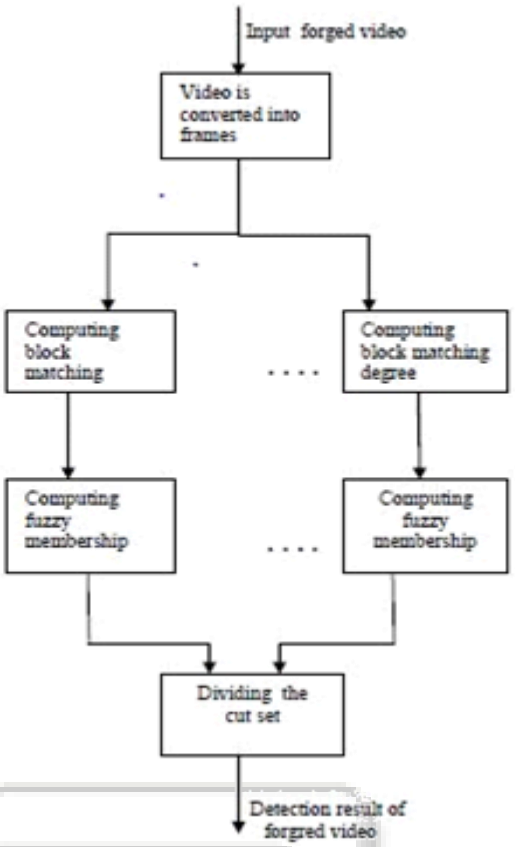

Fig. 2: Block diagram of blind detection method

C. MPEG Double Compression Detection Algorithm:

Machine learning framework is adopted to enhance accuracy due to sensitive nature of first digit distribution to video content and target bit rate, Fig. 3 as in demonstrates the algorithm architecture. The detailed process described in is as follows:

1) Extract the first digit distribution of quantized AC coefficients for both query and training video.
2) Test the first digit distribution with parametric logarithmic law. Three goodness-to-fit statistics are calculated, including squares due to error (SSE), root mean to zero, R-square closer to one means a good fit.
3) Compose a 12-D feature by combining the first digit probabilities and goodness-to fit statistics. Consider only I frames as the fitting results for intra frames are better than that for non-intra frames.
4) Detection unit comprises of each GOP with a 12-D feature, so the SVM classifier judges on a GOP basis. Define the GOP proportion D as $D = n / N$. Where n stands for the number of GOPs which are labeled as double compression, and N means the total number of GOPs. If D passes the threshold T, it is extremely possible that the video has gone through double compression. Over here T is adaptive according to the demand of TNR and TPR. Generally T might be set as 0.50.

Original bit rate estimation algorithm taking a closer look towards fitting results of doubly compressed MPEG video, the difference between situations of decreasing and increasing target bit rate is noteworthy. This acts as trigger for a more detailed classification. The serial SVM architecture for this estimation is shown in Fig. 2 as in [9]. If target bit rate is larger than original bit rate then obviously the violation of the parametric logarithmic law will be much more. So SVM1 classifies the bit rate increasing situation and SVM2 focuses on original video and the judgment of bit rate decreasing situation. For results, the probability p = C / N is calculated. Where C stands for the number of GOPs which are labelled as a certain class and N is the total number of GOPs in a video. p is confidence index.

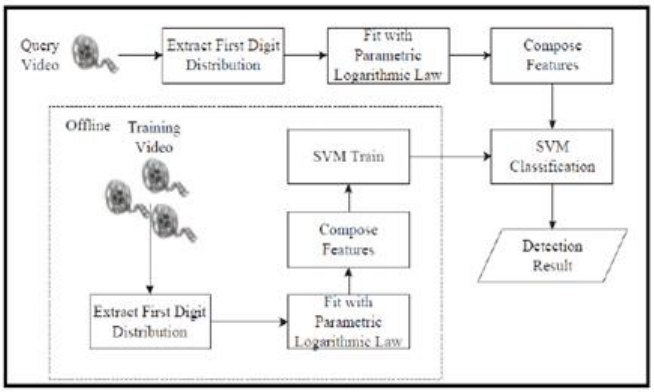

Fig. 3: MPEG double compression

D. Video copy move forgery detection using tamura texture features

Fig. 4: Block diagram of Tamura texture feature method

- Step 1: In the first step the features are extracted .The features are extracted based on the contrast orientation and roughness. After the feature extraction matrix composed of corresponding feature vectors.
- Step 2: we have to measure the similarity of two frames by calculating the Euclidean distance of their corresponding feature vectors to determine whether they are duplicates.
- Step 3: If the value of the similarity between two frames is greater than the threshold then consider those frames are candidate frames. We have to set another threshold for the distance to avoid the false selection of the frames. Record the frames which are meet this two thresholds . so, we can get the candidate frames that might be forged. Here the similarity calculate by the below equation.
- Step 4: After getting some no of pairs as a candidate pairs, the forged frames are detect based on that the forged frame are destroyed the continuity of the video. While for the original
- Step 5: In the original sequence, due to the continuity of the content in a video, highly similarity exists between the first and last frame of the sequence and their corresponding adjacent frames. For the duplicated sequence destroyed the continuity of video, so the corresponding value of similarity will be relatively low. If the pair of sequences are i~j and i+n~j+n by calculating the similarity between the first and last frame of two

sequences with the adjacent frame respectively, to distinguish which one is the duplicated sequences. The video sequences check by the below equations

$$\Delta d_1 = d(i,i-1)$$
$$\Delta d_2 = d(j,j+1)$$
$$\Delta d_3 = d(i+n,i+n-1)$$
$$\Delta d_4 = d(j+n,j+n+1)$$

If the below equation satisfy than the original sequence is i+n~j+n and the duplicated sequence is i~j, otherwise, the original sequence is i~j and the duplicated sequence is i+n~j+n, thus we have located the location of duplicated sequence.

$$\Delta d_1 + \Delta d_2 > \Delta d_3 + \Delta d_4$$

III. Conclusion

Here we are observed the different video tempering techniques. This paper mainly focused on different techniques used for detecting of forgery in video. Algorithm used over here gave good detection accuracy under unfavorable operations such as compression, scaling and filtering for spatial forgery detection while compression and filtering for temporal forgery detection.Although the video forencics is the wast domain and for the digital video tempering detection there are more effective and advanced method is still required to detect the forgeries done by the advance video editing tools.

Acknowledgment

I would like to express my cavernous thanks to Prof Anuradha gharge (HOD, electronics and communication engg dept. , VADODARA) for their constant support.

References

[1] Hsu, Chih-Chung, et al. "Video forgery detection using correlation of noise residue." Multimedia Signal Processing, 2008 IEEE 10th Workshop on. IEEE, 2008.
[2] Subramanyam, A. V., and Sabu Emmanuel. "Video forgery detection using HOG features and compression properties." Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on. IEEE, 2012.
[3] N. Dalal and B. Triggs, “Histograms of oriented gradients for human detection,” in Proc. CVPR’05, 2005.
[4] Wang, Weihong, and Hany Farid. "Exposing digital forgeries in video by detecting duplication." Proceedings of the 9th workshop on Multimedia & security. ACM, 2007.
[5] Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detecting copy-move forgery in digital images: a survey and analysis of current methods." Global Journal of Computer Science and Technology 10.7 (2010).
[6] Chen, Wen, and Yun Q. Shi. "Detection of double MPEG compression based on first digit statistics." Digital Watermarking. Springer Berlin Heidelberg, 2009. 16-30.
[7] J. Fridrich, D. Soukal, J. ukáš, “Detection of copy-move forgery in digital images,” In: Proc. Digital Forensic Research Workshop, Cleveland, OH, 2003.
[8] Asok De, Sparsh Gupta, Himanshu Chadha “Detection of forgery in digital video”, 2009.
[9] R. C. Gonzalez and R. E. Woods - Digital Image Processing; New Delhi: Prentice Hall of India Pvt. Ltd., 2005.

