VIDEO TEMPERING DETECTION AND RETRIEVAL USING IMAGE QUERIES

Shweta Bhagawati , Namrata Thombre, Sakshi Patil , Pranita Mhatre

Assistant Professor Mr. Swapnil Waghmare

Mahatma education society,Pillai HOC College of Engineering,Rasayani
shwetabhagawati95@gmail.com
Mahatma education society,Pillai HOC College of Engineering,Rasayani
namrata5851thombre@gmail.com
Mahatma education society,Pillai HOC College of Engineering,Rasayani
sakshipatil880@gmail.com
Mahatma education society,Pillai HOC College of Engineering,Rasayani
pranitamhatresp@gmail.com

Abstract : In this generation, videos are widely used in every field of transaction, security, conveyor so accuracy and reliability is very important. This paper proposes a new method to detect forgeries of video with statics background. In general, adjacent frames in a video with the same background have strong correlation. If the video being tampered, the continuity of the frames correlation will be disturbed. original video editing techniques can be used to tamper videos such as supervision camera videos, defeating their potential to be used as evidence in a court of law. Video forgery acts have been increasing in recent years due to the easy convince of sophisticated video editing software. Criminals may be using video tampering as a way to get acquitted on the basis that the video evidences presented in court could not prove that they have performed the crime at a particular time or place. For high profile criminal court cases, it is likely that a video that is altered slightly will be considered as unacceptable. A highly accurate forgery detection system can therefore help in ensuring the authenticity of the video evidences.

Keywords: Tempering video detection, ,Phase correlation ,forgery detection, Feature Extraction, Matching Algorithm

I. INTRODUCTION

Due to the prevalence of video editing software that can be easily accessible nowadays, it is not uncommon for crime perpetrator to easily carry out video forgery acts. The extensive usage of surveillance camera in security-critical buildings, together with the notion that recordings of surveillance video can typically be used as forensic evidence in court cases, video forgery attacks are often associated with video surveillance sequences[1]. One of the forgery techniques associated with surveillance video could be to replace or remove certain video frames to deliberately hide the existence of certain crime or to hide the entering of a certain crime perpetrator in a highly secured building. While another forgery technique may be to insert or introduce new video frames at a surveillance video recording deliberately in order to create a false notion that the crime perpetrator was in a different location than the crime scene[3].

In general, forgery acts can be classified to two categories: intra-frame and inter-frame forgeries. The first is associated with frame-wise forgery attacks within an individual frame while the second is associated with sequence-wise forgery attacks in which neighboring frames within a video sequence are being tampered. The main examples of inter-frame forgery are frame insertion and deletion forgeries[2].

II. PROBLEM DEFINITION

Video sequences are often believed to provide stronger forensic evidence than still images, e.g., when used in lawsuits. However, a wide set of important and easy-to-use video manufacturing tools is today available to anyone. Therefore, it is possible for an attacker to harmfully forge a video sequence, e.g. by removing or inserting an object in a scene. These forms of manipulation can be performed with different techniques.For example, a part of the original video may be replaced by either a still image repeated in time or, in more complicated cases, by a video sequence[5].

Moreover, the attacker might use as source data either a continuum region of the same video, or a region taken from an external sequence. Our Project tries to address the first problem of video forgery by replacing patches of video frames with continuum regions from the same video. The proposed algorithm is able to detect whether a continuum region of a sequence (i.e., a block of connected pixels in the continuum domain) was replaced by a portion of the same video taken from a potentially different time interval. This type of forgery is also referred to as video based attack and requires understanding of motion ques to detect forgery. Apart from that we would also like to retrieve the original video in our database by using a frame from the forged video as a query image and matching its features with the same frame of original videos and retrieve the video which has maximum number of matched features[2].

III. LITREATURE SURVEY

Digital video inter-frame forgery detection for MPEG-1,2,4 and H.264/AVC encoded videos. Analysis of footprints left when tempering with a video sequence, an propose detection algorithm that allows a forensic analyst to reveal video forgeries and localized them in the spatiotemporal domain[3].

A method to detect video tempering and distinguish it from common video processing operations such has recompression, noise and brightness increase, using a practical watermarking scheme for real time authentication of digital video[4]. A nov Multi-Level Subtraction(MLS) approach was propose for video frame insertion forgery detection achieving a recall rate of 93.92% and precision rate of 100% on a forensically realistic video database. Detect forgery in MPEG videos by analyzing the frame's compression noise characteristics.The compression noise is extracted for spatial domain by using a modified Huber Markov Random Field(HMRF) as a prior for image[8].

IV. SYSTEM FLOW

The following steps detail our forgery detection and video retrieval system architecture:

The user selects a folder which contains all the image frames from the videos. These folders contain frames of 9 original sequences as well as 9 forged sequences.

These frames have been acquired using MIT open source software called FFMPEG which can convert any type of multimedia format to any other multimedia format old or new.

After extracting the frame we extract motion residuals from our video frames. This is done by taking absolute difference of successive video frames.

These video frames are then converted into blocks of equal size. In our case the frames are converted into image blocks of 4x4 with image height and width of 80x60 per block.

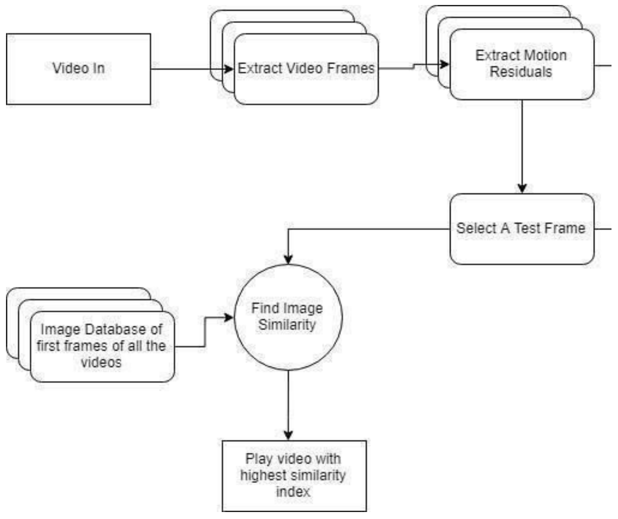
Then using a slider the user selects the video frame in which it wants to detect forgery. The motion residual of the corresponding frame is selected by the program and then that motion residual is also converted into 4x4 blocks.

Then phase correlation is performed between each block of the test frame and all the blocks of the video frames and the blocks which give phase correlation greater than 0.6 or 0.7 are considered to be forged copies of the moving object.

After finding the blocks in the test with phase correlation greater than 0.6 or 0.7 in other frames this blocks are considered to be forged ones are visualized on the GUI with a bounding box around that block. If none the blocks has phase correlation greater than 0.6 or 0.7 it means video is untempered.

After finding the forgery is detected we move on to image retrieval. We have already saved the first frames of the image in our database we extract SURF features from those images and surf features from the first frame of input video are extracted and the database image which has maximum matching features gets its video played.

V. SYSTEM ARCHITECTURE



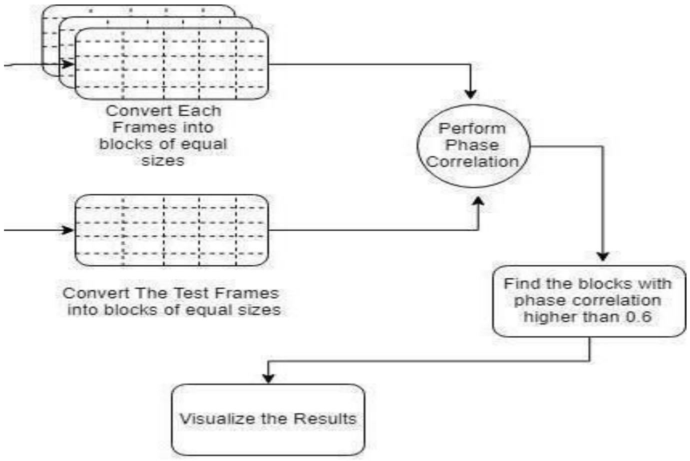

Convert Each Frames into blocks of equal sizes
Perform Phase Correlation
Convert The Test Frames into blocks of equal sizes
Find the blocks with phase correlation higher than 0.6
Visualize the Results

Fig1: Video tempering detection and retrieval using image queries

VI. PHASE CORRELATION ALGORITHM

In image processing, phase correlation is a method of image registration, and uses a fast frequency-domain approach to calculate the relative translative offset between two same images.

The result of correlation between two images is an image which has apex intensities at locations where the two images match the best. Fig1:Video tempering detection and retrieval using image queries The insight behind correlation is that the resulting image will have the maximum value when the hills and troughs of the images match up, i.e. when the contents of the images match up exactly.

Phase correlation between two images f and g is given by:

$$p(x,y) = \mathbb{F}^{-1}\left[\frac{F^*(u,v)G(u,v)}{|F^*(u,v)G(u,v)|}\right]$$

Where F and G are discrete fourier transform of f and g 2D images, F* is the conjugate of the the transform and F is the inverse fourier transform. By dividing the product of two DFTs' with the magnitude of DFT we can normalize the peaks of the transform[6].

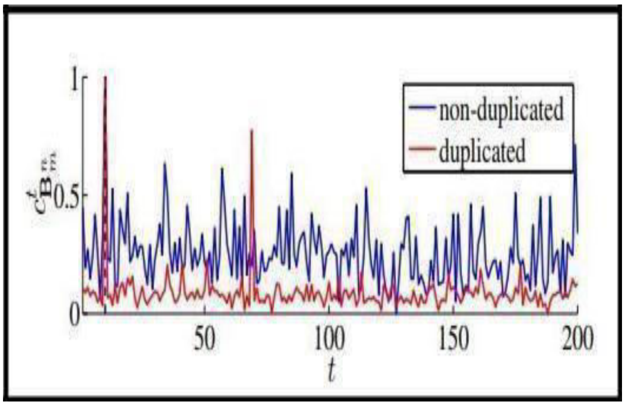


Fig 2: Phase Correlation Diagram

VII. SURF

The SURF descriptor is based on Haar wavelet responses and can be calculated efficiently with integral images. The SURF descriptors are robust to rotations and an upright version. The SURF descriptor describes an interest area with size 20s. The interest area is divided into 4 × 4 subareas that is described by the values of a wavelet response in the x and y directions. The wavelet response in the x and y direction is referred to as dx and dy respectively[7].

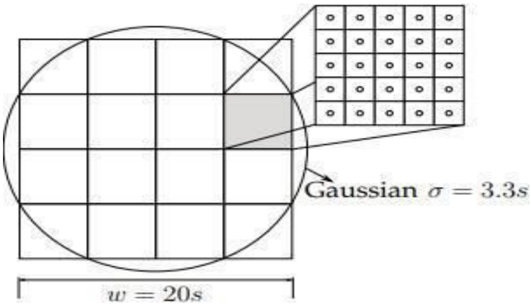


Fig 3: Image conversion into 4 x 4 blocks

VIII. RESULT ANALYSIS

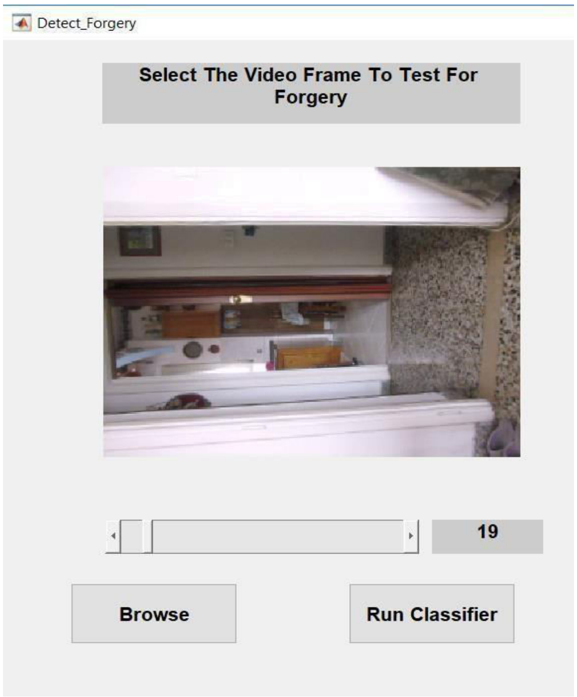


Fig 4: Select video from database

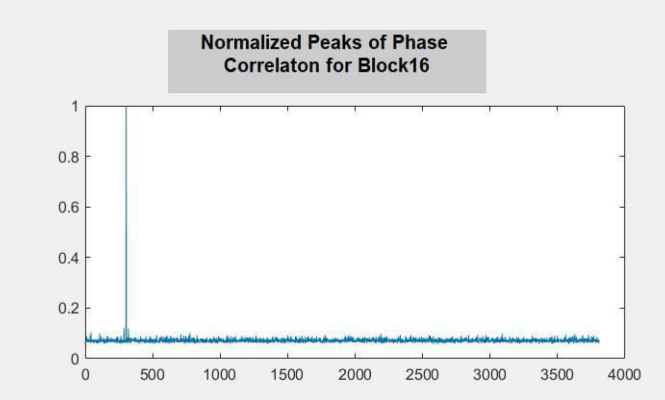


Fig 5: normalized peak of phase correlation

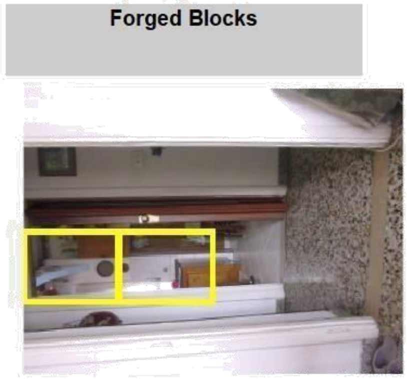
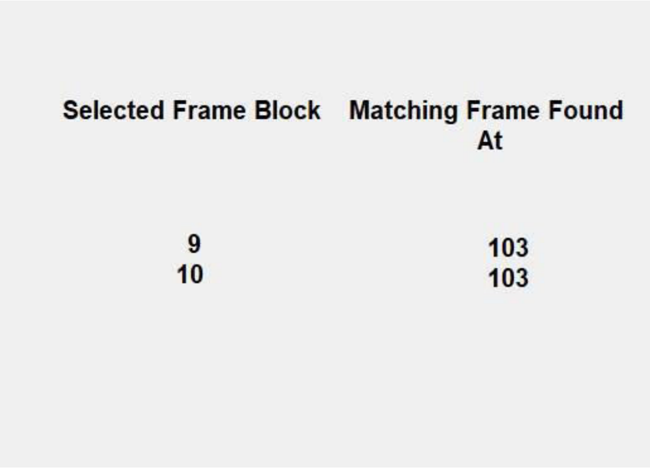


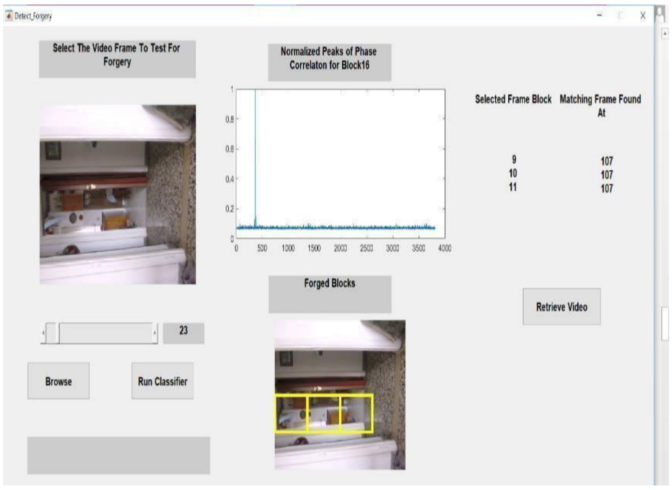
Fig 6: Display forged block



Selected Frame Block	Matching Frame Found At
9 10	103 103

Fig 7: Result of block matched frame

Fig 7: Result of block matched frame


Detect_Forgery
Select The Video Frame To Test For Forgery
Normalized Peaks of Phase Correlaton for Block16
Forged Blocks
23
Browse
Run Classifier
Retrieve Video

Selected Frame Block	Matching Frame Found At
9	107
10	107
11	107

Fig 8: Video tempering detection and retrieval using image queries

IX. CONCLUSION

In all above specified tampering detection algorithm a video dataset is used during processing. A method is developed which will identify find temporal motion residuals. These temporal motion residuals are then used to construct a model which tries to match the motion quest within the video, which then can be used to find if the object in the video is forged or not. Content based retrieval was performed in which we tried to extract various feature information from the video frame and tried to retrieve original video sequence.

Future works may target the detection of other possible attacks. As an example, we should consider more complex video in painting techniques. Moreover, we should study the possibility of developing anti-forensics techniques that aims to reduce the detector accuracy.

X. REFERENCE

[1] J. Zhang, Y. Su, and M. Zhang, “Exposing digital video forgery by ghost shadow artifact,” in Proc. 1st ACM Workshop on Multimedia in Forensics, (MiFor 09), pp. 49–54, 2009.

[2] V. Conotter, J. OBrien, and H. Farid, “Exposing digital forgeries in ballistic motion,” IEEE Trans. Inf. Forensics Security,

vol. 7, no. 1, pp. 283–296, 2012.

[3] R. Chen, G. Yang, and N. Zhu, “Detection of object-based manipulation by the statistical features of object contour,” Forensic Science International, vol. 236, pp. 164–169, 2014.

[4] Tan, Shunquan & Chen, Shengda & Li, Bin. (2015). GOP based automatic detection of object-based forgery in advanced video. 719-722. 10.1109/APSIPA.2015.7415366.

[5] S. Milani, P. Bestagini, M. Tagliasacchi, and S. Tubaro, “Multiple compression detection for video sequences,” in 2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP), 2012.

[6] P. Bestagini, A. Allam, S. Milani, M. Tagliasacchi, and

S. Tubaro, “Video codec identification,” in 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012.

[7] D. Vazquez-Padin, M. Fontani, T. Bianchi, P. Comesana, A.

Piva, and M. Barni, “Detection of video double encoding with GOP size estimation,” in 2012 IEEE International Workshop on Information Forensics and Security (WIFS), 2012.

[8] A. Subramanyam and S. Emmanuel, “Video forgery detection using HOG features and compression properties,” in 2012 IEEE

14th International Workshop on Multimedia Signal Processing (MMSP), 2012.