ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Tool for Video Forgery Detection in Video Sequences

A.S.C.I Piyumalie, L.L.T Pubudini, B.U.S Senarathne, K.M Thilakarathne, Saminda Premaratne
Faculty of Information Technology
University of Moratuwa
Katubedda, Moratuwa, Sri Lanka

Abstract : Because of the vast development of the video editing tools, the digital videos are playing main role in todays' context. Because of the variety of techniques available, it is very easy to alter and edit original content of a video. So paper describes about implemented system for video surveillance which could apply for tamper detection. As an inputs system is getting the videos which are needed to be tested. System could use, for law enforcements, CCTV (Closed-circuit television) videos, for news broadcasting. Mainly this system is considering developing a system for analysing shadow variation with the noise and system recognize an object and extract shadow from the object and for detect moving objects and track objects. After this approach system will identify pattern variations in shadow, motions and create a model by using SimpleKMeans approach as a clustering technique in data mining and frame removed edited videos by using Naïve Bayes classification algorithm in data mining. According to the pre identified model, user input videos will be identified as tampered or not. The model creation was done for 3 CCTV s. From each CCTV system has taken 20 videos .And implemented the model for 5 noise levels, kernel size11, 15,25,55,75 for shadow detection and frames were removed in-between original videos for different time levels. According to model, input video from predefined CCTV gives noise level of the video and error rate of each noise level .And objects are tracked and according to motion vector, the variance of the objects will be calculated. This result is used in data mining and according to that prediction happens.

Keywords: SimpleKMeans, Naïve Bayes, Data Mining, Motion Vector, CCTV, Weka

I. INTRODUCTION

With the wide spread availability of user friendly and low-cost digital video cameras and the availabilities of video sharing websites such as YouTube, digital videos are playing very important role in day today life. [1]Because of this Digital video authentication is very popular subject in current context. Since digital video can be illegally alter, therefore the authenticity couldn't be taken for trustworthy. Authentication of digital video in other form digital video forensic is a process of identifying and proving that the video taken is original and it hasn't tampered content. While it is mostly concern because tamper detection of a video isn't that much easier, but with the advanced, increasingly sophisticated digital video editing software are making it easier to tamper a video, so because of this identification of tampered video is so much important. When it comes to some areas, authenticity and originality of video data is very important. For example in forensic investigations, law enforcement, video surveillance and content ownership. When it comes to court of law, it is very important to establish trustworthiness of any kind of video when it used as evidence.

And in another hand with the video editing technology which is rapidly growing in today's context, developers can easily remove an object from video sequence by simply removing some of frames, insert an object from a different video source or sometimes an object animated by computer graphics. So a video frame could be doctored in a specific way to defame an individual. [2]And also a criminal could be free easily, because a video shows about crime has been edited. In another scenario, a news maker cannot prove that the video played by a news channel is correct, receivers cannot ensure that video coming through a communication channel that video being viewed is really the one that was transmitted These are the instances where modifications can't be tolerated.

Therefore there is a compelling need for video authentication. Because most manipulation techniques are highly available for general public, so video recording is emerging as a serious challenge.

For identification of originality of video contents and to detect malicious tampering and to prevent various types of forgeries, various types of forensics are used on video data. These techniques could detect the types and the locations of malicious tampering. [2]But the case is there are wide range of powerful digital video processing tools which allow maximum access, manipulations and reuse of visual materials. Though video recording devices and close circuit camera systems become more convenient and affordable option in the private and public sectors, using these in criminal investigations are also increasing correspondingly. Because of their ability to detail information in it selves. Most of these are used in investigations. So it would be really necessary to make sure that the given video evidences are authenticated. [1]But there are only a few digital video forgeries have been exposed, such instances are decrease the public trust in video. Therefore, it is urgent for the scientific community to come up with methods for authenticating video recordings. And for methods which could be easily use and applicable for many video formats.

II. RELATED RESEARCH WORK

Watermark and digital signature based techniques have been widely used in last two decades for the purpose of video authentication. .While in digital signature based schemes, the authentication data is stored separately either in user defined field, [3] as like, in header of MPEG sequence or in a separate file. In addition of these two techniques, intelligent techniques have also been introduced for video authentication. Intelligent video authentication techniques are basically learning based techniques which use video databases as sample data for the purpose of learning.

In the digital signature based schemes, the digital signature of the signer to the data depends on the content of data on

some secret information which is only known to signer .But according to position and the source this signature could be distorted. In last two decades, a wide variety of watermark based authentication techniques have been presented by various re-searchers in literature. Based on the application areas, water- marking can be classified in different categories [3], [4] .Once the data is manipulated, these watermarks will also be altered such that the authentication system can examine them to verify the integrity of video data. Intelligent video authentication techniques use video data- bases for learning purpose. The database comprises tampered and non-tampered video clips. Apart from digital signature, watermarking and intelligent authentication techniques, some other techniques are proposed by various researchers in the literature for the purpose of authentication of digital videos.

III. RESEARCH APPROACH

The solution that was proposed is a tool which could give a numerical value to user according to noise level of the video. This isn't 100% accurate value but it gives approximate value to user about the tampering level and user could proceed with caution when using the video. For purpose of having accurate analysis ,system used CCTV videos and to narrow down the scope for this level implementation have used 3 CCTVs .From each CCTV and have used 20 videos and have used those to 4 noise levels which are11,15, 25,55,75.

A. Shadow Detection

According to Wikipedia a shadow is consider as an area which create because of a light from a light source, which has been obstructed by an object. Sunlight causes shadows at day. According to variation of the angle shadow is varying .Shadow length is varying according to the time of the day and also if the object is moving, the shadow casting object will create an image with dimensions and also increase of size of the shadow will also vary according to the light source and its' distance.

User will give an input to the system as showed in Fig. 1, then input will be direct to the shadow detection method implemented in the tool. Need to collect previously available non-edited videos from CCTVS. This could be vary according to the user requirements and if a particular new user needs to know whether a particular video has been edited, then first that user needs to give original videos of different occasions or same occasion of particular CCTV to the system, by using those videos system will create a training dataset. So then if a particular user needs to know that videos of existing CCTV video has been edited or not, then user could input a suspecting video clip to the tool and according to shadow variation with respect to noise then user could identify that additional noise has been added or not .

Implementation process could be described as below. System need to have original videos from a particular CCTV camera to create train data set.

For creating train dataset, below process is happened. Mainly for one original video from source CCTV, there are 5 edited videos, which were created by using noise, as noise system has used Gaussian Blur and Kernel sizes are 11,15,25,55,75.And then both edited and non-edited videos were went through in above process.

1) Extract the foreground from the video

Video extracting process is done by using Gaussian Mixture-based Background/Foreground Segmentation Algorithm [5]. This algorithm is used to identify static objects and non-static objects. Algorithm first identify static objects and then it identified objects which are intruding and those are spotted as the parts of the video which aren't fit the model. When a non-static object entered and suddenly if it became static then algorithm identified those as static too. Because in this model it identify background as large clusters .In a video there could be chances that non static objects become static, for an example a moving vehicle could be stop for an identical time period, then system would recognize that object as part of the background .In background subtraction system is created a foreground mask, it is a binary image contained the pixels which are belonging to the moving objects in the scene.

For the implementation, used two ways of background subtraction methods which could categorize as background subtraction with the non-static objects as showed in Fig. 2 and background subtraction with the shadows and non-static objects [6].

Background subtraction with the non-static objects method isn't consider cast shadow as a moving object and in next approach it detects both self-shadows and cast shadows as moving objects with the objects.

So in these two approaches system had two video sequences of frames which are background subtracted and foreground detected and objects are identified as 0th intensity pixels as black pixels and 255th intensity pixels as white pixels.

2) Extract shadow from the video

Main purpose of this project is to identify variations of shadows to noise levels and determined if a video has been forged or not. So for this system got a subtracted value from the video frames which have non static objects with shadows and frames which only contained non static objects as Fig. 3. So from this system could extract the shadow form the video frame as a binary image sequence.

3) Values of the shadow

From subtracted video frames then next step is to get a number of pixels which contained shadows. So for this system has read values of shadows by putting the Mat object into map and creating a histogram by using that map and then by iterating through the histogram values. For this system could have key values as the pixels and the number of pixels which were under each key value. So after having that system could use those pixel values to determine to which pixel values are most suitable to use as a threshold value to applying training data into data mining for model creation.

4) Draw Graphs

For identification purpose of applying most suitable value to ClassificatinViaClustering system has drawn diagrams for each dataset with different noise levels for all pixel values and have identified that there is a distinct variation between the original video and edited videos in 127th pixel value and System has taken the number of pixels in 127th pixel for each frame for 40 training data sets and used those as inputs to data mining process.

5) Data Mining

In this implementation got data for the each frame for original video and edited video. And then after drawing graphs system has identified that shadow variation is very high in 127^{th} pixel and system has taken is as a value to enter to my data mining algorithm.

So after by going through these processes System has identified appropriate data mining algorithm for use. System has gone through classification and clustering techniques and

chose clustering as the best way to identified pattern in dataset. Because data set could be clustered into two clusters by saying Original video and edited video and pattern of those clusters could be identified using clustering, group of objects which are in similar are clustered into same class and dissimilar objects are clustered into another class. So system has created two clusters as cluster 01 and cluster 02.If the video is original it is assigning to cluster 02 and cluster 01 is assigned for edited video.

It is hard to use Weka with the clustering when using it with java. So for this purpose system has come up with an algorithm for using Weka with the classification. For that system has used ClassificationViaClustering filter, and it has many clustering algorithm s provided. System has gone through many approaches and chose the one which gave highest classified instances and lowest root mean squared error. By having those as the parameters system has chosen the SimpleKmeans algorithm as the best approach to clustering.

Fig. 1. Example of a Original Video Frame

Fig. 2. Example of a Backgroung Subtracted Frame

Fig. 3. Example of a Shadow Extracted Frame

B. Motion Detection And Tracking

As a first step it is going to track moving objects in original video. It is covered by red color rectangle in frame series of Fig. 4. It is shown that a sequences of frames [5].

It is going to background subtraction as the next step. The main purpose of the background detection is foreground extraction. It is commonly used technique for motion segmentation in static scenes. It tries to detect moving areas sub stacking the current image pixel-by-pixel from a reference background image. The pixels where the difference is above a threshold are classified as foreground. After creating a foreground pixel map, some morphological post processing operations such as erosion, dilation and closing are performed to reduce the effects of noise and enhance the detected regions. The reference background is updated with new images over time to adapt to dynamic scene changes.

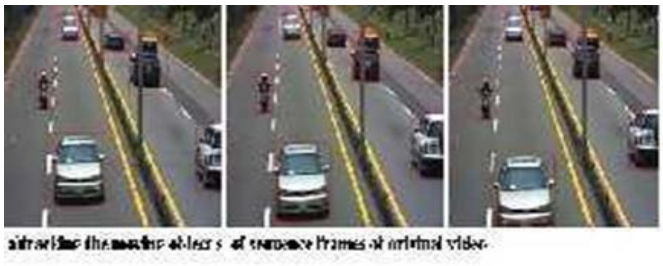

Fig. 4. Example of a Motion Tracking

1) Motion Tracking

1. As the first step user can add any type of video to our system an d at the first frame have to catch good features from video System has used opencv function named as cvGoodFeaturesToTrack().
2. Next Used cvCalcOpticalFlowPyrLK() to find the corresponding locations in second frame which corresponding to founded good points in first frame and also cvCalcOpticalFlowPyrLK() [6]can be used to find point matching or not, feature errors in the corresponding points
3. Then it has to create motion vectors for all points which identify from goodfeatureToTrack function.
4. Then it has to find how points can be missed. Actually System has categorized them into two parts .Actually points can be missed and There is a matching point for captured point but the matching is not 100% correct. It means although the 2 points are matching and but there is a large distance between the two points, so Coded that as
   If (features_found[i] == 0 || feature_errors[i] > MAX_COUNT) when the value of the MAX_COUNT is
   increasing then the unnecessary points become unrecognizable.
5. Then System has to follow an algorithm to found suspicious point in a frame. Suppose V is magnitude of motion vector and theta is the angle of that point measured in x axis anti clockwise
   if (VxSin(Theta)<0)
   {
   if (VxSin(Theta) >= point[i].y) point i naturally eliminated
   else
   point i is suspicious }else if (VxSin(Theta)>=0) {
   if (VxSin(Theta) >= (frmHeight - point[i].y)) point i naturally eliminated
   else

```
point i is suspicious
}else if ( VxCos(Theta)<0)   {
if (VxSin(Theta) >= point[i].x)
point i naturally eliminated
else
point i is suspicious
}else if ( VxCos(Theta)>=0)   {
      if (VxCos(Theta) >= (frmWidth - point[i].x))
    point i naturally eliminated else
point i is suspicious
}
```

Fig. 5.

6. Then System has calculated the ratio among no of suspicious points and all points what we found.

7. System has calculated ratio for every frame and consider it as a sample of population of video. And calculate mean and variance for the video.

$$\text{Mean}(\mu)=\sum \text{ratio of a frame/Number of frames in a video} \quad (1)$$

$$\text{Variance}=\sum(\text{ratio of a frame}/\mu)^2/\text{Number of frames in a video} \quad (2)$$

8. Then System has created train set of data. System has created 15 edited samples from one original video and does the same process as explained above.

IV. EVALUATION

Application can be used for any video format, but the level of accuracy is depending on the CCTV that uses and the level of the noise, after went through different approaches system has recognized that system couldn't find an distinct number of pixel value different between noise level 11, 15, and also noise level 55, 61.So like that shadow variation isn't very high between nearest noise levels. To have a clear distinct value system has to take different level of noise levels(Kernel sizes).System could also edit videos by removing frames for that system has removed frames from 1 original video and created edited videos from that. And system could trained different datasets for different CCTVs and according to CCTV model is changing. So system is giving an approximate numerical output. In Fig. 5 accuracy levels have been demonstrated for each classification and clustering algorithms.

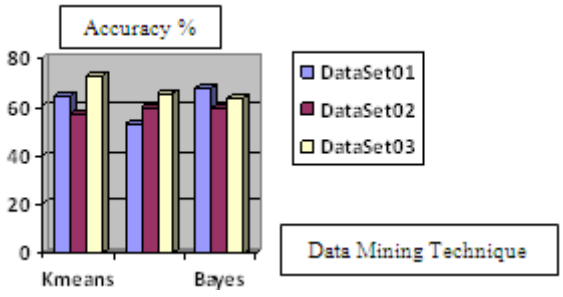

Fig 5: Accuracy Levels of Data Mining techniques

V. CONCLUSION

In conclusion, our research has demonstrated its effectiveness in recognizing tampered video and originality of the video .According to CCTV camera system would give originality of video. Totally 3 CCTV and 20 videos from each CCTV have been used. For clustering has used the SimpleKMean clustering approach and for classification Naïve Bayes algorithm.

VI. ACKNOWLEDGMENT

We would like to thank who guided us in each and every step and our colleagues for their advices and great support. Finally we like to thank to our parents who hold us, helped us and encouraged us.

VII. REFERENCES

[1] Saurabh Upadhyay, Sanjay Kumar Singh,, "Video Authentication-An overview," International Journal Of Computer Science & Engineering Survey(IJCSES), vol. 2, no. 4, November 2011.

[2] Prayag Patel,Saurabh Upadhyay, "A New Technique for Video Survellance," Indian Jouranl Of Applied Research, vol. 3, no. 6, June,2013.

[3] Kusam,Pawanesh Abrol,Devanand, "Digital Tampering Detection Techniques:An review," BVICAM s International Journal of Information Technology, vol. 1, no. 2, July 2009.

[4] Minati Mishra,M.C.Adhikary, "Digital Image Tamper Detection Techniques-A Comprehensive Study," International Jouranl of Computer Science and Business Informatics, vol. 2, no. 1, June 2013.

[5] Yang Shen,Lizhuang ma, "Detecting and Removing the Motion Blurring from Video Clips," Modern Education and Computer Science, vol. 1, pp. 17-23, 2010.

[6] Rupali Yashwant Landge,Rakesh Sharma, "Blur Detection Methods for Digital Images," International Jouranl of Computer Applications Technology and Research, vol. 2, no. 4, 2013.