MAHINE LEARNING BASED COPY MOVE VIDEO FORGERY DETECTION

[1] Rohini Sawant, [2] Manoj Sabnis
[1,2]P.G. Student, Associate Professor, Vivekanand Education Society's Institue of Technology,
Mumbai, India

Abstract: The consumption and utilization of Multimedia in different digital formats is increasing across the globe. The Videos provide immediate and substantial visual and communicational opportunities than any other form of digital media. Thus with it's proliferate use, the chances of its misuse also increase. The Video forgeries are largely affecting the videos available online and offline. A forgery of a single visual element may lead to severe misrepresentation and misunderstanding of the underlying data. Thus detecting video forgeries is of utmost importance in the current scenario. This paper suggests the detection of copy paste forgery using motion and machine learning concepts. This paper concentrates on Motion-Based Multiple Object Tracking, analysis feature coefficients of HOG, Blurriness and Chromaticity, of which feature vectors are generated and given as an input to Support Vector Machine(SVM) for classification as Forged and Original.

Keywords: Video Forgery, Object Tracking, HOG, Blurriness, Chromaticity, Support Vector Machine.

I. INTRODUCTION

In the digital epoch, creation and distribution of Video forgery is easier due to the availability of Video editing software's coupled with high speed internet. Even a usual user can create a forged digital video and proliferate it over the Internet web. Thus Digital video forgeries exploit various attributes like color, brightness, resolution etc. The Video forgery detection aims at authenticating the video by validating its history and content attributes.[1]

There are different types of forgeries which can be basically classified into two types: Whole frame forgeries and Object forgeries. The Whole-frame forgeries include addition, deletion and replication of frames which is easy to perform and restricts the set of forgeries to be performed on the video. Object forgeries alternatively deal with addition or deletion of objects in the video. Object forgeries might even have a straight effect on the observer's interpretation of the video content. They are more sophisticated, flexible and difficult to perform compared to the traditional compression or frame based forgeries. In the context of Video Forgery, Copy-move forgery (CMF) is a simple forgery method that implies copying and moving a part or entire object in the frame to a new location in the same frame accompanied with some post-processing operations. The Copy Move Forgery Detection (CMFD) techniques are computationally expensive and bring about high false positives, and use high correlation between original and forged parts of the video frames to detect and determine copy paste forgery.[2] However since the source and the targets are part of the same video frame the properties like colour, brightness, illumination, noise etc are presumed to be efficiently matched in the forged regions. This characteristic is utilized in many CMFD algorithms [3]

This paper proposes a CMFD method based on the Passive approach for Video Forgery Detection. For this the video is firstly divided into selective key frames by using the concepts of Multiple Object Tracking. From these frames the HOG, Chromaticity and Blur features are extracted based on the physics and statistical properties of each frame. The feature vector thus formed is provided as an input to the machine learning classifiers, SVM(Support Vector Machine) and KNN(K Nearest Neighbor). The Machine learning approaches makes automatic decision regarding the video and classifies it to be genuine or forged. Thus the objective of this paper is to develop a method to detect the copy move forgery and to classify the test samples into Forged or Original.

II. PROPOSED METHOD

A. Motion-Based Multiple Object Tracking

This paper aims at detecting CMF which is a kind of object forgery hence the first step is object detection. Object detection, a pre-requisite for initializing a Motion based object tracking process, refers to locate the object of interest in every frame of a video sequence.[4] Optical Flow, Frame differencing and Background Subtraction(BS) are the three procedures for moving object detection. Here Background subtraction is chosen as it is relatively suitable for motion based object detection from a static background and stationary camera.

The background subtraction algorithm to detect moving objects is based on Gaussian Mixture Models. The BS algorithm divides the video frame into foreground and background. We are interested in foreground as it gives us the required moving objects and helps us in object detection. Noise is eliminated using morphological operations on the foreground mask. Corresponding moving objects are detected using blob analysis. Object detection is based totally based on motion and motion estimation is done by Kalman Filter. It predicts location of tracks and likelihood detection being assigned to each individual track in each frame. Track maintenance is done by the multi Object Tracker object in MATLAB. The output of Motion-Based Multiple Object Tracking is a series of frames of unique tracks. These frames are then used as targets in the experiment for further procedure and analysis.[5]

B. Feature Extraction

Feature extraction aims at extracting the appropriate information from the videos and present it in low dimensional space. Feature Extraction is basically performed when the data to be processed is to huge and redundant.[6] A large video database is converted to a set of features during Feature Extraction. Feature extraction algorithms use a common extraction method which are either by key point based or block based feature extraction mechanisms.

This paper chooses to work on the Block based feature extraction methods. In this method we extract the Histogram of Oriented Gradients (HOG) features and the Blur and Chromaticity features which are the part of the IDA feature vector.[7] The advantage of using HOG features is that they are robust against various signal processing manipulations.[8] In a video frame the blur annoyance can be calibrated by blurring the frame by passing it through a low pass filter and comparing the variations before and after the blurring step. The decision is made based on the interpretation that an elevated variation between the original and blurred frame means that the original frame was sharp and genuine whereas a marginal variation means the original frame was blurred.[9]

Chromaticity Feature extraction can be summed into two simple steps. First is to convert the video frame from RGB to HSV space and second step is to calculate the values of Mean, Deviation and Skewness of each channel. Considering the fact that these three features are counterparts to the three statistical moments in each channel, they are referred to as the Chromatic Moment features.[7]

C. Classification

The feature vector generated from feature extraction is used as an input in the training process to train the classifier. For cross validation, the database is divided in a certain ratio to use a part of it for training and other part for testing. It is ensured that videos sequences if used as a part of training samples will not be a part of testing samples. Two classifiers will be used on this proposed method which are SVM and KNN one after the other. Both the SVM and KNN are non parametric, supervised classifiers. Once the feature values are provided to the classifier, it will train itself about the features and finally classify the target video to the expected result. The classifier aims to develop a model that is build on the training data which will predict the resultant values when given only the test dataset.

After the training process, testing samples are employed to verify the efficiency of the classifier.

D. Proposed Video CMFD

The forgery detection procedure is given below:

1) Divide the Video Database into Training and Testing Sample Sets.
2) Load the Training sample set of videos.
3) Extract the frames from the video sequences using Motion based Multiple Object Tracking.
4) Save the frames to a new folder.
5) Divide the frames into blocks of size nxn and extract the HOG, Blur and Chromaticity features.
6) Generate the Feature vector.
7) Train the Classifier using the feature vector as input.
8) Test the Classifier model by using the Testing Sample set.
9) The Classifier predicts the decision as Forged or Original for the test video sequence.

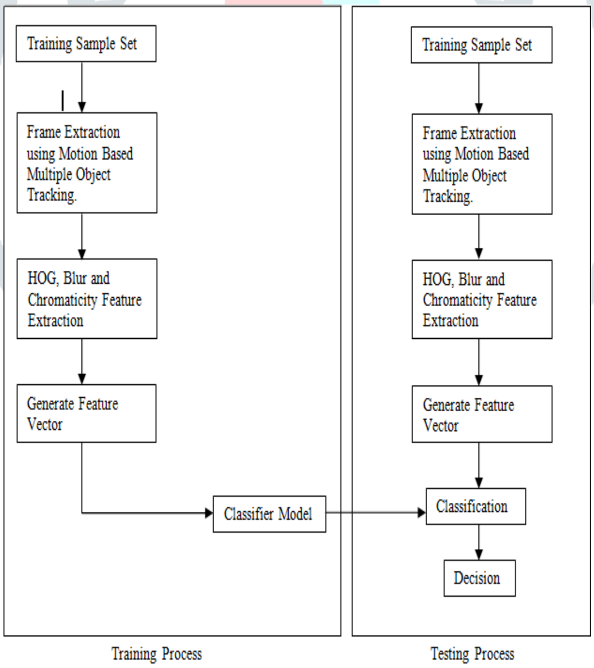
Training Sample Set
Frame Extraction using Motion Based Multiple Object Tracking.
HOG, Blur and Chromaticity Feature Extraction
Generate Feature Vector
Classifier Model
Training Sample Set
Frame Extraction using Motion Based Multiple Object Tracking.
HOG, Blur and Chromaticity Feature Extraction
Generate Feature Vector
Classification
Decision
Training Process
Testing Process

Fig 1: Proposed method of Forgery detection

III. IMPLEMENTATION

The proposed method for video forgery detection was been implement on MATLAB version R2016a using Samsung laptop configured with Intel® Core ™ i3-3110 CPU 2.40GHz with 64-bit Operating System and 4.00 GB RAM.

In this proposed method for CMFD we use the REWIND tampering dataset that was built by Bestagini et al. This dataset comprises of a total of 20 videos of which 10 videos are original and 10 videos are forged ones. Each video sequence has a resolution of 320x240 pixels, and a frame-rate of 30 fps. Some of the original sequences are taken from the SULFA tampering dataset. For Cross validation the training sample set consist of 14 videos comprising of 7 original and 7 forged videos each. The testing samples set consist of 4 videos comprising of 2 original and 2 forged videos each. The details of Training and Testing Sample Sets are given in the below table:

Tab 1: Training and Testing Sample Set

Training Sample Set	Testing Sample Set
02_forged.avi	07_forged.avi
03_forged.avi	09_forged.avi
04_forged.avi	07_original.avi
05_forged.avi	09_original.avi
06_forged.avi	-
08_forged.avi	-
10_forged.avi	-
02_original.avi	-
03_original.avi	-
04_original.avi	-
05_original.avi	-
06_original.avi	-
07_original.avi	-
10_original.avi	-

The Training sample videos are been divided into frames using Motion based Multiple Object detection. The Feature extraction for the HOG, Blur and Chromaticity features is performed and a feature vector is generated.

The training sample set and the feature vectors are used to build the classifier model and then that model is used to test the inferences of the testing sample set.

For classification two machine learning classifiers used are SVM and KNN. The algorithm first is performed using SVM. For SVM the libsvm library is used, where Radial Basis Function (RBF) is997 used as kernel function. Then the proposed method is again implemented using the KNN classifier. The KNN stores the training sample set and when the query testing sample set is provided it will look up to the available k nearest data points and will classify the queried test data to the labelled set that contains majority of the neigbhors. The Testing sample set is been deployed on the classifiers to test performance.

IV. RESULTS AND DISCUSSION

Accuracy can be considered as the rate of correct classification. Higher the accuracy the better is the performance of the classifier. We define accuracy, precision, recall, and F1 score as,[10]

Accuracy = (TP+TN)/(TP+TN+FP+FN)

Precision = TP/(TP+FP) Recall = TP/ (TP+FN)

Score = 2* [(Precision*Recall)/ (Precision+Recall)]

Thus the comparison of performance of the proposed method using both the classifiers is given in the below table:

Table 2: Experimental Results

Classifier	Performance (%)		
	Accuracy	F1 Score	Error
SVM	100	100	0
KNN	75	80	25

The experiments are been performed on the proposed algorithm using two different classifiers i.e SVM and KNN. Both of them perform well on the proposed method. However the proposed method with SVM has outperformed the results of the algorithm with KNN is all categories bring about excellent accuracy, F1 score and nil error rate. Thus from the experimental results it is clear that the proposed algorithm works well with SVM than KNN in Forgery detection accuracy.

V. CONCLUSION & FUTURE SCOPE

Thus we have proposed and implemented a Passive method for Copy Move Video Forgery Detection using the Machine Learning Approach. With this approach the issue of complexity for videos due to large database is reduced using Motion Based Multiple Object Detection. Experimental results confirm that the proposed method performs well in forgery detection. However the algorithm when worked with SVM perform excellent with an accuracy of 100%.Thus we can concluded that proposed method for CMFD using SVM is better option for forgery detection then using the algorithm with KNN.

Future work for this research study may target the detection of other kinds of forgery like the upcoming popular complex Inpainting Forgery. Also due to the diverse and complex nature of digital videos, the study needs support in terms of better databases for training process. Thus the proposed method can we worked and implemented on a better and stronger database. Machine learning algorithms need manual detection of features thus this study can be extended to deep learning concepts.

REFERENCES

[1] Chougule, M. J. (2015). Review of Techniques of Digital Video Forgery Detection. Advances in Computer Science and Information Technology (ACSIT), (pp. 233-236).

[2] GhazaliSulong, O. I.-S. (2015). DETECTION OF VIDEO FORGERY: A REVIEW OF LITERATURE. Journal of Theoretical and Applied Information Technology , 207-220.

[3] Ramesh Chand Pandey, S. K. (2014). Passive Copy- Move Forgery Detection in Videos. 2014 5th International Conference on Computer and Communication Technology (pp. 301-306). IEEE.

[4] Verma, D. R. (2017). A Review of Object Detection and Tracking Methods. International Journal of Advance Engineering and Research , 569-578.

[5] https://in.mathworks.com/help/vision/examples/motion-based-multiple-object-tracking.html

[6] Gaurav Kumar, P. K. (2014). A Detailed Review of Feature Extraction in Image Processing Systems. (pp. 5- 12). IEEE.

[7] Di Wen, H. H. (2015). Face Spoof Detection with Image Distortion Analysis. Transactions on Information Forensics and Security. IEEE.

[8] Aniket Pathak1, D. P. (2014). Review of Techniques for Detecting Vidoe Forgeries. International Journal of Computer Science and Mobile Computing , 438-442.

[9] Frederique Cretea, T. D. (2008). The Blur Effect: Perception and Estimation with a New No-Reference Perceptual Blur Metric. Proceedings of SPIE - The International Society for Optical Engineering.

[10] Shiv Prasad, B. R (2016). Passive Copy-Move Forgery Detection using SIFT, HOG and SURF Features. International Conference On Recent Trends In Electronics Information Communication Technology, 706-710.