Indian Institute of Information Technology, Allahabad

Project Report

On

Video Forgery Detection

Submitted By:
Smiti Maheshwari (IIT2014067)
Bhairavee Bawane (IIT2014070)
Harsh Shah (IIT2014071)
Sandesh Jain (IIT2014104)

Under the Guidance of:
Prof. Anupam Agarwal
IIIT Allahabad

CANDIDATE'S DECLARATION

We hereby declare that the work presented in this project entitled "**Video Forgery Detection**", submitted as a VI Sem IVP project, is an authentic record of our original work carried out under the guidance of Prof. Anupam Agarwal. Due acknowledgements have been made in the text to all other material used.

Place: IIIT Allahabad

Date: 20th March, 2017

Smiti Maheshwari(IIT2014067)

Bhairavee Bawane (IIT2014070)

Harsh Shah (IIT2014071)

Sandesh Jain (IIT2014104)

CERTIFICATE FROM SUPERVISOR

This is to certify that the project work "**Video Forgery Detection**" is a bonafide work of Smiti Maheshwari (IIT2014067), Bhairavee Bawane (IIT2014070), Harsh Shah (IIT2014071), Sandesh Jain (IIT2014104), who carried out the project work under my supervision.

Place: IIIT Allahabad

Prof. Anupam Agarwal
IIIT Allahabad

Date: 15th April, 2017

ACKNOWLEDGEMENT

We acknowledge with much appreciation the crucial role of Prof. Anupam Agarwal for his contribution in this endeavour of ours. His efforts, constant support and perseverance has guided us through this project. His engagement through the process of this project has been precious and irreplaceable.

CONTENTS

I. PROBLEM STATEMENT

The trustworthiness of digital media is decreasing due to the fact that it has become really easy to alter and tamper the digital content flawlessly and thus, there is a need to verify the originality and authenticity of media contents. In view of this problem, we develop a method to classify the object based-forged content.

II. OBJECTIVE

To develop an approach for automatic identification of object-based forged video which is encoded with advanced frameworks based on its GOP (Group Of Pictures) structure.

III. THEORY

Object-based forgery, is a method which adds new objects to a video scene or removes existing objects from it. We must emphasize that object-based forgery is a common video tampering method since the object added into or removed from a video is usually critical to the contents that video conveys.

Generally, videos are in compressed format. Therefore, when a pristine video undergoes some kinds of object-based forgery, the first step is to decompress it to a sequence of individual frames and each frame can be regarded as a still image. Then the frames in the selected segments of the sequence are tampered while the rest frames remain untouched.
After all the manipulations are finished, the resulting frame sequence is

re-compressed to generate a forged version.
To generate a forged video:

1. Decompress the video into individual frames and each frame is regarded as a still image.
2. The frames in the selected segments of the sequence are tampered while the rest frames remain untouched.
3. The resulting frame sequence is re-compressed to generate a forged version.

Some Terminologies-

1. Pristine frames: The frames in a compressed video stream which do not undergo any manipulation.
2. Double compressed frames: The frames in a video stream which have undergone re-compression.
3. Innocent double compressed frames: Those frames do not contain forged contents.
4. Forged frames: Those frames have undergone tampering operations.
5. I-frames (intra-coded frames): An I-frame indicates the beginning of a GOP. It contains the full picture and is independently encoded as a still image.
6. P-frames (predictive-coded frames): P-frames contain motion-compensated difference information relative to the preceding frames.

IV. APPROACH

- Select represent frames and construct their motion residuals.
- Extract feature vector for each motion residual using CC-PEV feature set.

- Feature vector acts as an input to Ensemble classifier which judges an input frame as “forged” or “innocent double compressed”.

A GOP structure is marked as “forged” if all the represent I frames and P/B frames are labeled as “forged” by the “innocent double compressed” vs. “forged” classifier. If there are at least one “forged” GOP structure in the suspicious video clip, it is considered to be a forged video clip, otherwise the suspicious video clips is indeed an innocent double compressed one.

Experiment:

- We have total 10 original and 10 forged videos encoded in H.264 format in our dataset.
- From this videos, we extracted 154 GOPs for both original and forged videos.
- We used 84 untampered and 84 forged GOPs as training set.
- Remaining 70 GOPs were used as testing set.

V. DEPENDENCIES

1. ffmpeg
2. MATLAB
3. Video dataset for training and testing
4. JPEG toolbox (Included)
5. CC-PEV 548 (Included)
6. Ensemble Classifier (Included)

VI. RESULT

Let’s define some basic terms-

1. true positives (TP): These are cases in which we predicted ‘yes’ and the actual answer is also ‘yes’.
2. true negatives (TN): These are cases in which we predicted ‘no’ and the actual answer is also ‘no’.
3. false positives (FP): We predicted ‘yes’, but the actual answer is ‘no’.
4. false negatives (FN): We predicted ‘no’, but the actual answer is ‘yes’.

Hence, the output values of various factors are as follows-

Accuracy = (TP+TN)/total = 0.6012

TP Rate = TP/actual yes = 0.5476

FP Rate = FP/actual no = 0.3452

Specificity = TN/actual no = 0.6548

Precision = TP/predicted yes= 0.6133

Prevalence = actual yes/total= 0.5000

Recall = TP Rate = 0.5476

F-score = 2*(precision * recall / precision + recall) =0.5786

VII. CONCLUSION

We developed an approach for automatic object-based video forgery detection that is encoded with advanced frameworks.

We analyzed the similarity between the object-based video forgery and steganography, and converted the detection of object-based forgery in a video clip into the detection of hidden data in the motion residuals of the corresponding video frames.

Finally, we get an accuracy of 60.12% on training and testing dataset of 5 videos each.

VIII. REFERENCES

[1] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, “Vision of the un-seen: current trends and challenges in digital image and video forensics,”
ACM Computing Surveys, vol. 43, no. 4, pp. 26–40, 2011.

[2] D. Liao, R. Yang, H. Liu, et al., “Double H.264/AVC compression detection using quantized nonzero AC coefficients,” in Proc. SPIE, Media Watermarking, Security, and Forensics III , 78800Q, 2011.

[3] M.C. Stamm, W.S. Lin, and K.J.R. Liu, “Temporal forensics and anti-forensics for motion compensated video,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1315–1329, 2012.

[4] 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.

[5] 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.