IVP Project

Object-based Video Forgery Detection

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.

Challenges

The research on video forensics, and especially on automatic detection of object-based video forgery is still in its infancy.

While some efforts on video forensics have also been made in the last decades, most of the existing video forensic algorithms either expose the evidence of side-effects of forgery or detect the so-called frame-based forgery, which refers to the manipulations that insert or delete frames.

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.

Object Based Video Forgery

Object-based forgery adds new objects to a video scene or removes existing objects from it.

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

- Innocent frames: Those frames do not contain forged contents.
- Forged frames: Those frames have undergone tampering operations.
- I-frames: An I-frame indicates the beginning of a GOP. It contains the full picture and is independently encoded as a still image.
- P-frames: P-frames contain motion-compensated difference information relative to the preceding frames.

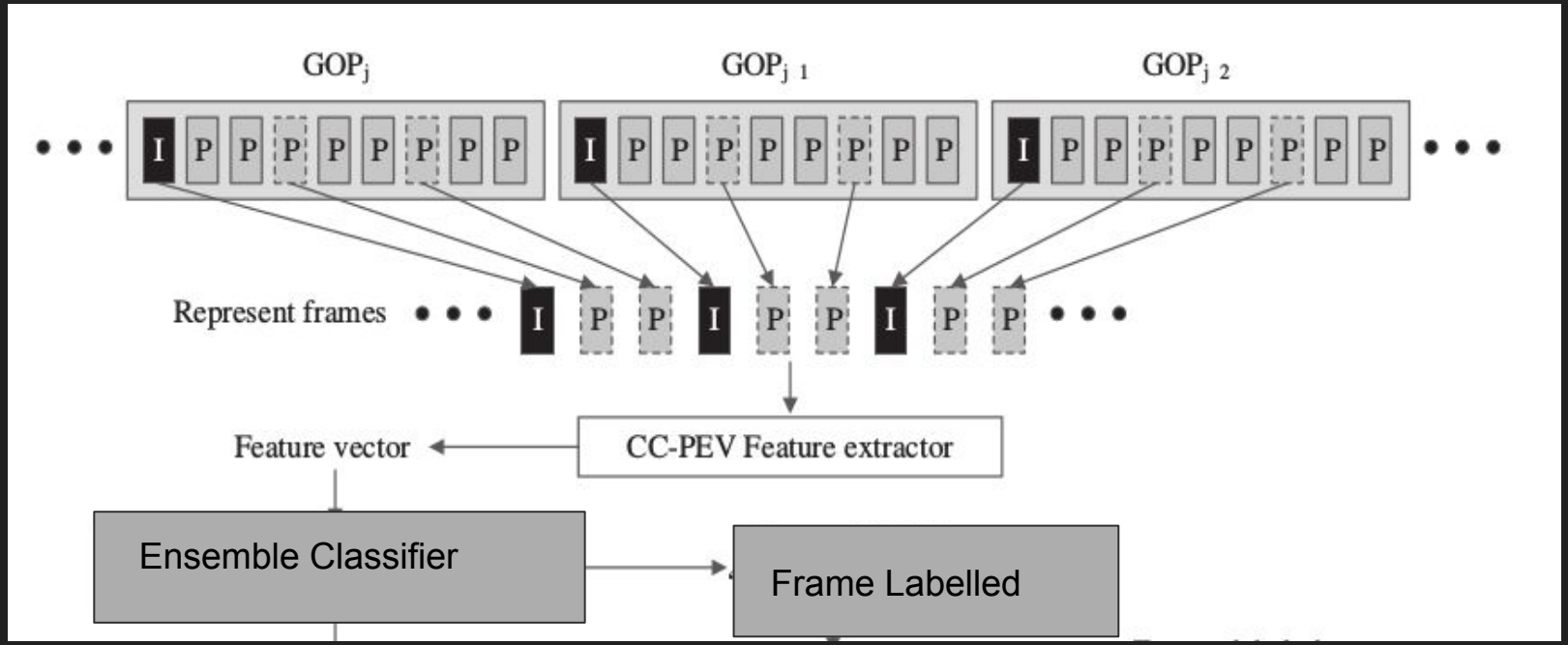
Our Approach

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”. A GOP structure is marked as “forged” if its vector is labeled as “forged” by the ensemble classifier. If there is 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 one.

Our Proposed Approach



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.

Hardware and Software Requirements

- Libraries used - CCPEV-548, Ensemble Classifier.
- Programming Tool - MATLAB
- Dataset - 20 videos, 10 original and 10 forged encoded in MPEG-4 format.

Formulae

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

Results

Based on above dataset we get the following result:

Accuracy	TP Rate	FP Rate	Specificity
0.6012	0.5476	0.3452	0.6548

Precision	Prevalence	Recall	F-score
0.6133	0.5000	0.5476	0.5786

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.

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.

Team Members

Smiti Maheshwari	IIT2014067
Bhairavee Bawane	IIT2014070
Harsh Shah	IIT2014071
Sandesh Jain	IIT2014104

THANK YOU