CHAPTER 1

INTRODUCTION

This chapter discusses the reasons of selecting the topic of digital video forgeries detection, as well as the solution to solve the problem.

1.1 Rationale

Surveillance cameras can monitor public places to control the crime rate. Nowadays, many video editing tools can manipulate video. Attackers can use them to tamper with the video content and falsify facts. However, the authenticity of video content gets more attention if it is supported by primary evidence. The authenticity of videos is difficult to guarantee. The video background consists of static and dynamic scenes. A static scene is a condition where no object is moving or only a static background, and a dynamic scene is a condition where objects are moving. Although the surveillance video has many static scene frames, many attackers have exploited them to hide some information, and the human eyes cannot detect tampering.

Video forgeries have two categories: (i) Intra-frame forgeries, which occur in the spatial domain, such as the removal of an object in a frame or more, and copy-move; and (ii) Inter-frame forgeries, which occur in the temporal domain. Inter-frame forgery consists of frame duplication, insertion, and deletion. It is easy to delete one person entering a room in a surveillance video just by deleting the part of the video where the person appears. However, this forgery can cover up the truth and make people misjudge if the inter-frame forgery is used as a news item or evidence in court. Therefore, a digital video forensic technique can prove the authenticity of video content. Many researchers have developed a forensic system to expose inter-frame forgery. The existing methods Fadl, et al. in [2], Yang, et al.in [12], and Wang. et al. in [10] only identified duplication forgery. The research Fadl, et al. in [3], Zheng, et al. in [13], Wang, et al. in [11], and Fadl, et al. in [1] can identify not only frame duplication forgery but frame insertion and deletion. Furthermore, Fadl, et al. in [1] developed the proposed method to detect frame shuffling forgery. This work concerns the identification of inter-frame forgery because it is a common forgery in surveillance videos and is easy to apply. However, they have the limitation of being unable to detect inter-frame forgery in static scenes.

This work proposes an efficient method to discriminate against inter-frame forgery in static and dynamic scenes. In order to identify the static scene, optical flow is considered to be applied because the method can extract motion features that represent frame conditions effectively. Based on the observation of various scene datasets, we propose a threshold formula to classify static scenes.

1.2 Problem Formulation

The existing methods still have many problems. Their methods fail to detect forgery in static scenes (namely only the background frame, no moving objects). In fact, the forgery occurs in a static or silent (no moving objects) scene. In crime case, however attacker can remove evidence by deleting some clips as though nothing occurred. Wang, et al. in [11] perform optical flow changes to detect forgeries. Their method fails to detect the forgeries in static frames. Therefore, it is necessary to develop a robust method to identify frame deletion, insertion, and duplication in various scenes.

1.3 Objective and Hypothesis

This research aims to identify interframe forgeries, such as frame deletion, insertion, and duplication, as well as in various scenes. Hence, this research performs segmentation of scenes to discriminate between static and dynamic scenes and thus detect outliers in each scene efficiently. In order to discriminate various scenes, optical flow is considered to be applied because the method can extract motion features such as magnitude, velocity component (V_x, V_y), and orientation. These features represent conditions effectively in a frame, for example, objects moving or static scenes. The differences between this research and Wang, et al. in [11] are as follows:

1. This research concerns static scene forgeries by classifying static and dynamic scenes based on threshold, which has not been discussed by Wang, et al. in [11].
2. This research utilizes datasets with various background places to represent video forgery in real life, while Wang, et al. in [11] has only two background places.

1.4 Assumption

This research begins by assuming that the forged video dataset does not have distortion, so it does not have to overcome distortion. The forged video is taken from an existing dataset, so it does not have to build and develop the dataset by using video editing tools. The video frame intensities between frames are assumed to be constant, so the brightness does not have to be processed. All video datasets are assumed to be fragments of the original video that has a long duration, so the first and last frame are ignored and are not considered an anomaly point or forgery candidate.

1.5 Scope and Delimitation

This problem's scope limitation must be determined in order to ensure that the scope of this issue does not extend to an unrelated aspect. The scope limits of the problem in this study are as follows:

1. Focus on video forgery in interframe forgery: frame duplication, insertion, and deletion
2. The video datasets are only single-shot and static cameras.
3. Only one type of manipulation emerges in each video (single varian).

1.6 Related Works

Fadl, et al. in [2] proposed duplication forgery detection by computing the entropy of DCT coefficients for each selected residual frame after using the standard deviation and the similarity between all pairs of feature vectors for subsequence windows. Yang, et al. in [12] performed an effective two-stage method based on similarity analysis for detecting frame duplication.

Wang and Farid in [10] proposed duplication forgery detection by computing the spatial and temporal correlations among sequential video frames. The method was unsuitable for detecting the forgery in static scenes. Fadl, et al. in [3] calculated differential energy of residual between frames. However, this method requires an original video to identify the forgeries, and the detection fails for deletion forgery in a static scene. The method has detected inter-frame forgery (deletion, insertion, and duplication).

Zheng, et al. in [13] utilized block-wise brightness variance descriptor (BBVD) for detecting video inter-frame deletion and insertion but had a low precision rate in the localization of forgery. Their method detects inconsistency of the BBVD ratio at equal time intervals if forgery occurs forgery.

Wang, et al. in [11] identify inter-frame forgery (i.e., frame deletion, insertion, and duplication) by using optical flow and anomaly detection. Their method denotes discontinuity points in the optical flow variation sequence depending on the type of forgery. They fail to detect the forgeries in static frames.

Fadl, et al. in [1] proposed HOG features to identify insertion and deletion forgery. In addition, they calculate the MEI of edge images to detect duplication and shuffle forgery efficiently with high accuracy and low running time. However, they fail to detect frame deletion for silent scenes because the frame correlations are high in these scenes.

Some of the existing systems are most related to interframe video forgeries described in Table 1.1.

Table 1.1: The Details of Several Studies Related to Interframe Video Forgeries

Author	Forgery Type	Proposed Method	Strengths (+)	Limitations (-)
[10], W.Wang, Hany Farid (2007)	Interframe Forgery (Frame Duplication) And Intraframe Forgery Region Duplication.	Correlation coefficient in duplicate frames and Fourier transform.	The method is effectively to detect duplication region and frame.	It is not robust to detect tampering with small region size.
[3], Fadl, S.M., Han, Q., Li, Q (2018)	Interframe Forgery: Frame Duplication, Insertion and Deletion	Extracts residue data from video stream and apply spatial energy (SE) and temporal energy (TE) to capture anomalies in a video stream.	The method is effectively to detect temporal tampering and can locate the position of forgery efficiently with an acceptable running time	When some frames are deleted from a static scene, anomalies are not captured and detection fails.
[2], Fadl, S.M., Han, Q. and Li, Q (2017)	Interframe Forgery: Frame Duplication	The entropy of DCT coefficients is performed for each selected residual frame and using correlation coefficient between all pairs of feature vectors.	The method can detect the inter-frame duplication efficiently with a low computational time.	It fails when the duplicated clip occurred in a static scene.
[11], Wang, W., Jiang, M., Sun, T (2013)	Interframe Forgery: Frame Duplication, Insertion and Deletion	Optical flow and anomaly detection to identify the inter-frame forgery process	The method is effectively to detect frame duplication, insertion and deletion.	It fails to detect frame deletion for static scenes
[1], Fadl, S., Qi Han, and Li Qiong. (2020)	Interframe Forgery: Frame Duplication, Insertion Shuffling and Deletion	HOG features to detect anomalies and localize FI and FE, MEI of edge images for each video shot to reveal FD and FDS.	The method can detect interframe forgery and locate the position efficiently with high accuracy and low running time.	It fails to detect frame deletion for silent and scenes fast moving content.