Video Authentication

Amar Parkash, Yash Seth, Nikhil Shekhawat, Richa Singh, Mayank Vatsa

IIIT DELHI, INDIA

Introduction

The algorithm proposed under the project aims to detect video tampering by using a combination of many techniques to facilitate our requirement. The technique proposed in our algorithms manages to eliminate most of the practical tampering issues such as , Frame addition and deletion, Frame swapping and Object alteration .
We propose two different algorithms under this project, one with reference and other for videos with no reference.

Motivation

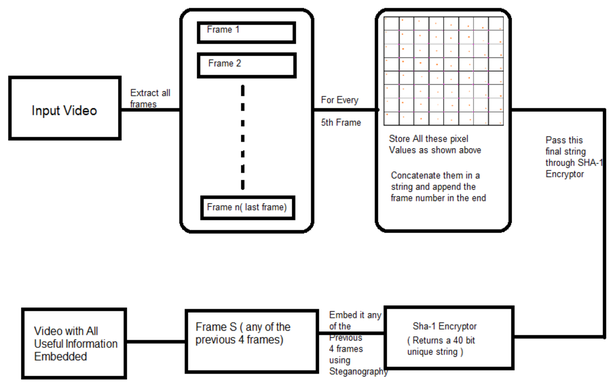
In a world where video surveillance has become the need of the hour, its authentication still poses to be a major issue. Be it a surveillance video or any other video recording, its genuineness remains to be the concern of many. These videos, especially when used for legal issues, have to be ensured to be tamper- free. With plenty of tools available which can change or alter the contents of a video by a mere click, this problem becomes more severe and of utmost importance.
Given below are some examples showing some basic forms of attack on a video.

Proposed Algorithms

Two Different Algorithms

- **With Reference Approach**: Some useful information embedded on the video and later retrieved for authentication purpose.
- **No Reference**: Given a video without any previous information embedded, determine the authenticity of the video using its frames and their data.

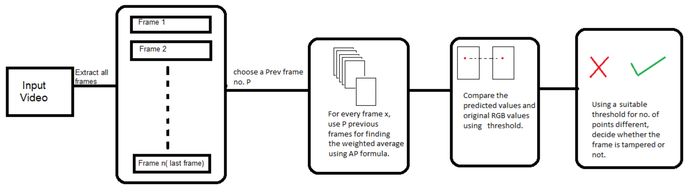
With Reference Algorithm



Authentication

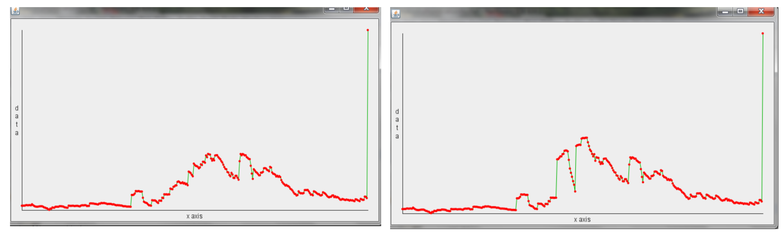
- Again follow the above process to get the 40 bit encrypted string.
- Extract previously embedded information and compare the two to check whether any frame is tampered or not.

No Reference Algorithm Using Change Detection



Authentication

- If the number of frames in a video show a huge variation in the number of tampered points then the video is considered to be tampered.
- Given below is a graph depicting the number of different points versus the frame. A sudden variation in between depicts a tampering in the video.



Graph 1 depicts an original surveillance video , Graph 2 is showing a tampered video in which almost 20 frames have been deleted

Database and Results

Database and Experimental Results

- The database prepared by the authors comprises of more than 70 high definition videos and over 8 hours of surveillance videos.
- The HD videos were used for Referenced algorithm where as the surveillance videos were used for the No-reference algorithm testing.
- The Reference algorithm showed 100% results on all the mentioned attacks and even showed the frame no at which the tampering had occurred.
- The No-Reference algorithm testing was done by deleting or swapping a minimum of 15 frames (1/2 sec) and clearly depicted the point tampering.
- By considering all the points in the frame, the No-Ref technique resulted in detecting object alteration as well but increases the time complexity.

Conclusion

- Change Detection serves as a good basis for detecting any possible tampering in videos.
- This HD database along with the tampered videos will be available to the research community