Self Embedding Watermarking System

Project Proposal

Project Advisor:

Dr. Asif Mahmood Gilani

Group Members:

Arbab Hamd Rizwan	18L-0756
Usama Aslam	18L-0972
Aashar Naseem	18L-1131
M. Hunzlah Malik	18L-1139

National University Of Computer and Emerging Sciences
Department of Computer Science
Lahore, Pakistan

1. Abstract

The availability of editing tools and the simplicity of changing content has made it imperative to protect digital content, the authenticity of media such as images and videos is a major concern nowadays. Our work will be focused on developing a watermarking system for multimedia as a solution to this problem. Images will be watermarked using a variety of encoding techniques especially using fragile watermarking methods. Which can assist in the detection of manipulation and the reconstruction of altered images. Furthermore, a similar technology will be used to detect video tampering to reconstruct tampered videos using keyframes retrieved from a frame window (a frame window consisting of similar frames), followed by watermarking the discovered keyframes

2. Introduction

In the last decade, editing software has gone a long way. As a result, the general public now has access to advanced editing tools, which make manipulating any sort of digital media, such as images and videos, much easier. This raises serious doubts about the veracity of any media that is presented. Image tampering mainly focuses on manipulating it as a whole. Whereas, video consists of many frames which can be considered as individual images. Therefore, video tampering has been categorized into two types: [1]

1. Temporal tampering which refers to interframe editing manipulation. This type of tampering includes adding, removing or changing the sequence of frames in a video.
2. Spatial tampering which includes manipulation of objects within a frame and is referred to as intraframe manipulation.

Image alteration, CCTV footage, or medical data manipulation might pose a severe threat in fields like video surveillance, forensics, and law enforcement, as well as content ownership.

The process of watermarking can be used to detect tampering attacks. The detection and restoration of these modified images and videos will be the focus of our project. Watermarking of images involves breaking them into smaller portions and inserting data in their LSB, which can subsequently be used to identify manipulation and even restore the original image. In research publications, numerous methods are explored, which vary depending on the number of blocks the image is divided into and the watermarking method [3, 4, 5]. This method can

also be used on video, by first detecting the keyframes and then processing those frames as if they were images [1].

3. Goals and Objectives

The goals of this project are to detect the tempering of image and video and their restoration so that it can help in law enforcement and content ownership.

- Watermarking an image.
- Detecting image tampering using watermarking.
- By using self embedded watermarking, reconstructing the image.
- Identifying the key frames in a video
- Watermarking the identified key frames in a video.
- Video tampering detection.
- By using self embedded watermarking of the key frames, restoring the video.

4. Scope of the Project

The project mainly focuses on image and video tampering detection and reconstruction. So the area of work here is to use Digital Image Processing and Computer Vision for watermarking an image and video. A watermarked superimposed into an image directly however in a video the key frames are first detected using Artificial Intelligence and then these key frames are watermarked. In this project the data encryption algorithms used are SHA-256 hash function, pixel-wise authentication-based self-embedding fragile watermarking method and finally self-embedded fragile watermarking method. So, our goal is using these above methods to find an optimal solution to our problem.

5. Initial Study and Work Done so Far

For image tampering detection and reconstruction, the main method applied was fragile watermarking with different methods for embedding data in the image. All of the techniques embed data in the LSB (Least Significant Bits), which ensures that the image quality is not adversely affected. The image is divided into four 16x16 blocks, which are further fragmented into smaller blocks, and data is then embedded in the LSB. As a watermark, the SHA-256 hash function is utilized, which gives a 256-bit value [3]. Another comparable approach employs the same concept but separates the image into 16 main blocks, which are then further divided

into 4x4 partner blocks, after which the data is embedded into the last two LSBs using a 128-bit hash value [5]. The most refined method process image pixel wise and divides into 2x4 or 4x2 sub-blocks according to block type and generates pixel position bits which can also be used in the recovery process. For video authentication and recovery, the main method was to identify the key frame in a frame window and then treat it like an image by watermarking it using any of the feasible watermarking methods. The main concern in video authentication is the processing time due to the large number of frames, which is tackled by compressing the keyframes [1]. Until now, the mentioned methods for detection and reconstruction used active forensics. However, one of the research papers applied passive forensics for video tampering detection. This method also requires a dataset that is preprocessed before training. Moreover, in this method tampering was detected through 3D CNN. A consecutive number of odd frames were inserted into the model to classify the frames as pristine or forged frames. If any of the frames was classified to be forged, the video would be identified as a tampered video [2].

6. References

[1] V. Amanipour and S. Ghaemmaghami, "Video-Tampering Detection and Content Reconstruction via Self-Embedding," in IEEE Transactions on Instrumentation and Measurement, vol. 67, no. 3, pp. 505-515, March 2018, doi: 10.1109/TIM.2017.2777620.

[2] Q. Yang, D. Yu, Z. Zhang, Y. Yao and L. Chen, "Spatiotemporal Trident Networks: Detection and Localization of Object Removal Tampering in Video Passive Forensics," in IEEE Transactions on Circuits and Systems for Video Technology, doi: 10.1109/TCSVT.2020.3046240.

[3] Gul, E., Ozturk, S. A novel hash function based fragile watermarking method for image integrity. Multimed Tools Appl 78, 17701–17718 (2019). https://doi.org/10.1007/s11042-018-7084-0

[4] Gul, E., Ozturk, S. A novel pixel-wise authentication-based self-embedding fragile watermarking method. Multimedia Systems 27, 531–545 (2021). https://doi.org/10.1007/s00530-021-00751-3

[5] Gul, E., Ozturk, S. A novel triple recovery information embedding approach for self-embedded digital image watermarking. Multimed Tools Appl 79, 31239–31264 (2020). https://doi.org/10.1007/s11042-020-09548-4