An Improvement of Forgery Video Detection Technique using Error Level Analysis

Hitesh C Patel
Department of Computer Science
Parul Institute of Technology
Vadodara, Gujarat, India

Mohit M Patel
Department of Computer Science
Parul Institute of Technology
Vadodara, Gujarat, India

ABSTRACT

Nowadays, videos are core part of live entertainment in television and movies, and they are breathing of real entertainment world. People believe movies and video snaps in everywhere of digital media. Digital Photo images are everywhere: on the covers of magazines, in newspapers, in courtrooms, and all over the Internet. We are exposed to them throughout the day and most of the time, we trust what we see. Trusting unbelievable video may create sensation over the news and gossip media world. The identified telecasted and forecasted video's truthfulness is challenging in multimedia. We propose methodologies to identify the forgery region frames from given input video by using EXIF image tag information.

Keywords

Digital photo image, video analysis, image forgery/doctored images, image tag analysis.

1. INTRODUCTION

Today, we are seeing doctored images and videos regularly. While these images might tarnish the public opinion of a celebrity, cases involving manipulated images with more serious implications have arisen in science and law. The art of making an image/video forgery is as old as photography itself. Forgeries are not new to mankind but are a very old problem. In the past it was limited to art and literature but did not affect the general public. Now a day, due to the advancement of digital image processing software and editing tools, an image can be easily manipulated and modified [1]. It is very difficult for humans to identify visually whether the image is original or manipulated. There is rapidly increase in digitally manipulated forgeries in mainstream media and on internet. Thus problem indicates serious vulnerabilities and decreases the credibility of digital world.

The developing techniques to verify the integrity and authenticity of the digital video is very important, especially considering that the images/video are presented as evidence in a court of law, as news items, as a part of medical records, or as financial documents. In this sense, forgery detection is one of the primary goals of image forensics [3].

Digital images/video offer many attributes for a tamper detection algorithm to take advantage of, specifically the color and brightness of individual pixels as well as an image’s resolution and format. These properties allow for analysis and comparison between the fundamentals of digital forgeries in an effort to develop an algorithm for detecting image tampering in a video.

Main goal of this paper is:

i. To introduce various techniques of image forgery detection.

ii. Review of some recent and existing techniques in forgery detection.

iii. Comparative study of existing techniques with their pros and cons.

iv. To Identified Fraud video evidence in social crime or digital media.

Image forgery detection techniques are classified into active and passive approaches.

The active scheme image such as watermark embedding or signature generation first; otherwise the tampered detection process will fail. This limits their application in practice [3].

Second approach passive techniques do not need any embeds any watermark or digital signature. The passive schemes extract some intrinsic fingerprint traces of image/video to detect the tampered regions.

In this paper, we are proposing passive forgery detection method in a digital video based on EXIF image tag (Extended Image Format) the EXIF tag the property of mainstream media. We Propose to analyze the temporal difference of each frame set in given input video and successfully identified the tampered region by using EXIF tag.

2. WORK ON VIDEO FORGERY

Currently, most acquisition and manipulation tools use the JPEG and MPEG standard for image and video compression. As a result, one of the standard approaches is to use the blocking fingerprints introduced by MPEG compression, as reliable indicators of possible image tampering. Not only do these inconsistencies help determine possible forgery, but they can also be used to detect the anomalies in adding or removing frames in video sequence, tampered in region forgery or mask the content in objects in frames videos that method of forgery was used.

Many passive schemes have been developed based on JPEG images, blue screen special effects in videos, detection duplication, photograph image forgery techniques, detecting double quantization, double MPEG compression, Correlation noise residue, histogram equalization based contrast enhancement techniques, luminance level techniques, frame add/delete techniques in MPEG video The good detection results, it's described as very complicated and high time processing.

1. Pixel based techniques - cloning (copy move), resampling (resizing, stretch, splicing, statistical).
2. Format based techniques - JPEG Quantization, Double JPEG, JPEG Blocking (difficult to detect forgery but these techniques can detect forgery in the compressed image).

3. Camera Based techniques - We capture an image from a digital camera, the image moves from the camera sensor to the memory and it undergoes a series of processing steps, including quantization, color correlation, gamma correction, white balancing, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may vary on the basis of camera model and camera artifacts. These techniques work on this principle. Chromatic aberration, Color filter Array, Camera Response, Sensor noise.

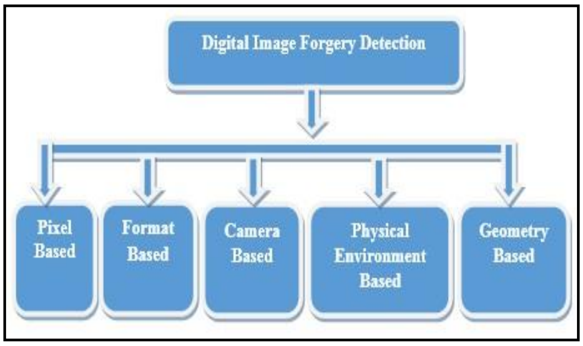

Fig 1: Passive Scheme Techniques

4. Physical environment Based Techniques - Lighting is very important for capture images these techniques work on the basis of the lighting environment under which an object or image is captured Light direction 2-D, Light direction 3-D, Light Environment.
5. Geometry based techniques - Principal point, metric measurements

3. METHODOLOGY OF VIDEO FORGERY DETECTION

Today, almost everyone has a digital camera. Literally billions of digital images are taken. JPEG is a standard in photography.

The JPEG Extension format is endless source of data that can be used for detecting forged images purposes. JPEG Format Analysis stored in the many technical meta-tags available beginning of each JPEG file. The tags contain information about quantization matrixes, chroma sub sampling, Huffman code tables, and many other parameters version of the full image. The content and sequence of those tags, as well as which particular tags are available, depend on the image itself or the device that captured it or software that modified it.

In additional to technical information, JPEG tags important information about the photo including ambient light levels, shooting conditions and parameters such as aperture and shutter speed information, model of the camera and lens the image was taken with, lens focal length, flash was being used or not, color (RGB, CMY) profile information, X-Y Resolution, YCbCr Positioning, Sample per pixel, Compression, F-Number, ISO speed rating, Contrast, Saturation, Sharpness and so on and so.

The basic analysis method verifies the EXIF tags in the first attempt to find discrepancies of image. The e.g. may include checks for EXIF tags at the post-processing by certain editing tools, checks for capturing date and time vs. the date and time of last modification, Frame Number, ISO Speed rating, X-Y Resolution and so on. EXIF tags can be easily forged at the time of editing or any manipulation action time so easily in fact that while we can treat existing EXIF discrepancies as a positive sign of an image being altered, the fact that the tags are “in order” does not bring any useful information.

Our solution makes discrepancies between the original image and available EXIF image tag information, comparing the actual EXIF tags information against tags that are typically used by capturing device (Capturing device specified the corresponding EXIF tag information). We collected EXIF tag information database and the comprehensive database of EXIF tags produced by a wide range of digital cameras model, Video recorder including many Smartphone models. We’re also actively adding information about new models as soon as they become available. EXIF tag the image are a clear indication of image manipulation software used for editing the image, also the original image date and time or other parameter does not match last modification image tag information data. The EXIF data contains Lake Amount of information about image.

4. RESULT

4.1 Error Level Analysis

This technique detects forge objects paste the original image by analyzing quantization tables of blokes of pixels in image. The quantization of certain injected objects or drawn in any editor software may differentiate from other parts of the forge image, especially if either or both the original image or forge image were previously compressed in JPEG Format.

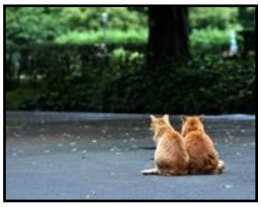

Fig 2: Original Image

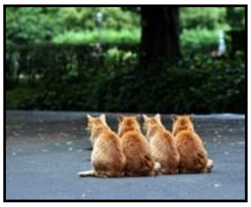

Fig 3: Forge Image

Above example, it still makes clearly identified which of the two cats were originally in the image, and the forge image were pasted two cats on the left during editing.

4.2 Image Quality

JPEG is a lossy Format. Each time the same image is opened and saves in JPEG Format, Some Visual quality is lost and some bluer or artifacts appear. The JPEG image file produce the issue by opening-editing a JPEG image file, saving image file, Closing image file, and opening and saving again the image file. Repeat several times, see the noticing the difference if higher compression levels are specified.

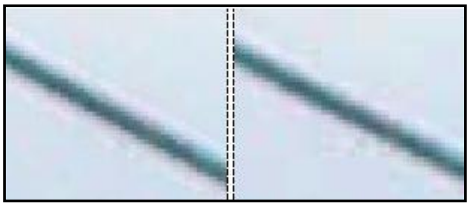

Fig 4: Image Quality

Above two image similar or same image, the last pictures are saved from the original with 90%, 70% quality reduces respectively. The higher the level of compression of file is the more visible blocking artifacts become. JPEG file blocks sized 8x8 pixels, and these blocks sized become more and more clearly visible when the JPEG image file is re-saved.

4.3 Double Quantization Effect

The Double Quantization Effect Techniques is based on certain quantization appearing when applying JPEG File compression more than once time. If the JPEG file was opened, edited, then saved, certain quantization compression artifacts will inevitably appear. In order to determine the double quantization effect, and creates histograms of image the containing discrete cosine transform values.

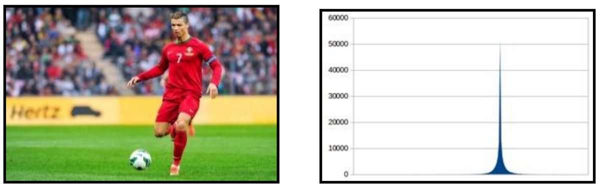

Fig 5: Original image histogram without open any graphic software

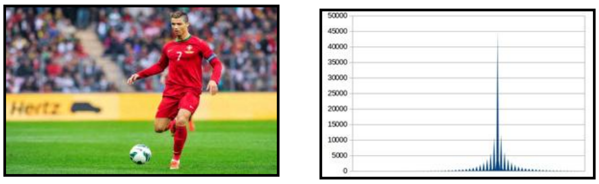

Fig 6: Image was open in graphic software make the difference clearly identified in histogram

These above two images identified the second image was opened in a graphic editor software so easily identified this image was edited/manipulated.

5. CONCLUSION

A wide range of techniques available in detecting the video tampering in digital world is very difficult to analyze and test the knowledge of forgery level in publishing in digital video world. Current system detect forgery video frames using mean frame comparison technique includes method based on mean and pixel comparison of each frame in video data frame using unknown data source. Proposed method used error level analysis for forgery frame detection. If original image/frame is not available, in that condition it can also detect the forgery image/frame. Proposed method ignores the necessity of having original frame for detecting forged frame.

6. REFERENCES

[1] Govindraj B. Chittapur, S. Murali, H. S. Prabhakara and Basavaraj S. Anami “Exposing Digital Forgery in video by mean frame comparison techniques” Springer India 2014.

[2] Murali S, Anami B S, Chittapur GB “Detection of photo-forgery detection techniques” Int J Mach In tell. ISSN: 09752927 EISSN: 09759166: 2012.

[3] Stamm MC, Ray Liu KJ “Anti-forensics for frame deletion/addition in MPEG video” IEEE international conference on acoustics, speech and signal processing, 2012.

[4] Murali S. Anami B S, Chittapur G. B. "Digital Photo Image Forgery Techniques" International Journal Of Machine Intelligence ISSN: 0975-2927&E-ISSN: 0975-9166:2012.

[5] Xu J et al “Detection of blue screen special effects in videos” Phys Procedia, 33:1316–1322, 2012.

[6] Murali S, Chittapur GB, Anami BS “Detection Of digital photo image forgery” IEEE international conference on advanced communication and control technology. ICACCCT. 2012.

[7] V. Conotter, G. Boato and H. Farid “Detecting Photo Manipulation on Signs and Billboards” International Conference on Image Processing, Hong Kong, 2010.

[8] W. Wang and H. Farid “Exposing Digital Forgeries in Video by Detecting Double Quantization” ACM Multimedia and Security Workshop, Princeton, NJ, 2009.

[9] Chih-Chung Hsu, Tzu-Yi Hung, Chia-Wen Lin and Chiou-Ting Hsu “Video Forgery detection using correlation of noise residue” Department of Electrical Engineering Tiwan, 2009.

[10] Alan C Bovik, Handbook of “Image and video processing”, Access Online via Elsevier, 2008.