Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 02, Issue 06, June - 2015

Forgery Frame Detection From The Video Using Error Level Analysis

Hitesh C Patel[1], Mohit M Patel[2]

[1]Research Scholar, Computer Science and Engineering Department, Parul Institute of Technology, Vadodara, Gujarat
[2]Computer Science and Engineering Department, Parul Institute of Technology, Vadodara, Gujarat

Abstract *— Field of Data mining is consists of verity of area like data processing, data classification, cluster analysis, Spatiotemporal databases, Multimedia mining. There are different kind of operations in multimedia mining for i.e. image recognition, image sharpening, image retrieval, image compressing, video analysis, video compressing, video processing and video quality enhancement etc. now a days you can see many kind of tampered images/videos or say forge image/video it is possible just because of image/video manipulation has become more common in digital camera and editing software package and high resolution capturing device. i.e. combination of multiple image produce single image. Following report discuss about problem occurs due to forge image/video as well as how to classified the original frame and forge frame. Proposed method show how to detected forge frame form the sequence of frame of video without having original video frames.*

Keywords- *Digital photo image, Video analysis, Image forgery/Doctored image, image tag analysis.*

I. 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 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 days, due to the advancement of digital media technology, image processing software, and editing tools, and image can be easily manipulated and modified. It is very difficult for humans to identify visually whether the image is original, duplicate 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 digital video is very important, especially considering that the images/videos are presented as evidence in 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 [Stamm MC, and Ray Liu define Anti-forensics for frame deletion/addition in MPEG video, 2012].

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

Main goal of this paper is:

A) To introduce various aspects/techniques of image forgery detection.
B) Review of some recent and existing techniques in forgery detection.
C) To identified fraud video evidence in social crime or digital media.
D) Comparative study of existing techniques with their pros and cons.
E) Forensics investigations.

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. An active scheme technique which is limits their application [Ng TT, Chang SF, Lin CY, Sun Q “Passive-blind image forensics”, 2006]. Second approach passive techniques do not need any embeds any watermark or digital signature. The passive schemes extract some intrinsic fingerprint traces of image to detect the tampered regions.

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 frame tampering. Not only do these inconsistencies help determine possible forgery, but they can also be used to detect the anomalies in adding, removing frames in video sequence, duplicate frame in video sequence, tampered region or mask the content in objects in video sequence that method of forgery detection was used.

Many passive schemes have been developed based on JPEG images, blue screen effects in videos, detection duplication, photograph image forgery techniques, detecting double quantization, 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, its described as very complicated and high time processing.

II. FRAME ANALYSIS

JPEG is a standard in digital photography. Most digital cameras can produce JPEGs, and many can only produce files in JPEG format. The JPEG format is an endless source of data that can be used for the purposes of detecting forged frame. The JPEG Format Analysis makes use of information stored in the many technical meta-tags available in the beginning of each JPEG file. These tags contain information about quantization matrixes, Huffman code tables, chroma sub sampling, and many other parameters as well as a miniature version (thumbnail) of the full image. The content and sequence of those tags, as well as which particular tags are available, depend on the image itself as well as the device that captured it or software that modified it.

In addition to technical information, JPEG tags contain important information about the photo including shooting conditions and parameters such as ambient light levels, aperture and shutter speed information, make and model of the camera and lens the image was taken with, lens focal length, whether or not flash was being used, color profile information, and so on and so forth. Every JPEG made from a camera has a great deal of information held within the data in the form of JPEG headers. This data, called EXIF (Exchangeable Image File Format) contains.

- Time and date picture was taken
- Integral low-res EXIF thumbnail
- Camera F-stop number
- Flash used (yes/no)
- Frame resolution
- Camera make and model
- Shutter Speed
- Distance camera was focused at
- Focal length and calculate 35 mm equivalent focal length
- GPS info, if stored in image. (IPTC Header)

Now a day's technology is more growth day by day the latest camera included many features such as location of capturing video (GPS Location), hybrid autofocus, Video editing tool also share the video in internet.

IPTC Photo Metadata properties have photo specific definitions that are widely supported by imaging software. IPTC Photo Metadata aligns with other IPTC metadata standards that are made for media items of any media-type. Following one properties describe Location:(City, County ISO-Code, Country Name, State, Sub location, World region, Current Owner Name (Artwork or Object detail)

2.1. Error Level Analysis

This method detects foreign objects injected into the original image/frame by analyzing quantization tables of blocks of pixels across the image. Quantization of certain pasted objects (as well as objects drawn in an editor) may differ significantly from other parts of the image, especially if either (or both) the original image or injected objects were previously compressed in JPEG format.

Figure 1: Original image

Figure 2: Altered image

Figure 3: ELA image

ELA highlights the altered portions of the image that represent higher ELA values, and a bright white color. Note that in the outline of objects in high frequency areas, they usually have higher ELA values than the rest of the image. In fig.3 the golden coines high contrast as compare to the frog because the coine is pasted to the original image so contrast creates a high frequency edge.

2.2. Double Quantization Effect

This technique is based on certain quantization artifacts appearing when applying JPEG compression more than once. If a JPEG file was opened, edited, then saved, certain compression artifacts will inevitably appear. In order to determine the double quantization effect, the histograms containing discrete cosine transform values. Certain quantization effects will only appear on these histograms if an image was saved in JPEG format more than once. If the effect is discovered, we can definitely tell the image was edited (or at least saved by a graphic editor) at least once. However, if this effect is not discovered, we cannot make any definite conclusions about the image as it could, for example, be developed from a RAW file, edited in a graphic editor and saved to a JPEG file just once.

Figure 4: Original image

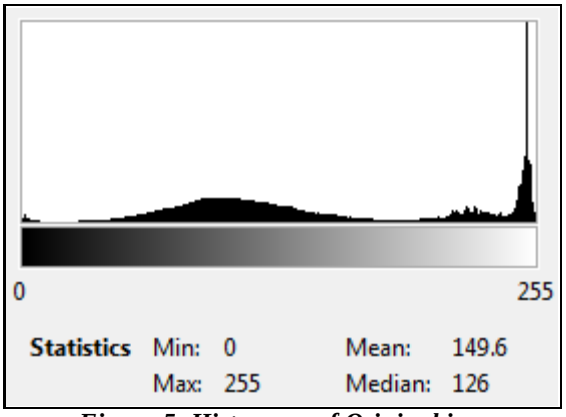

Figure 5: Histogram of Original image

Figure 6: Original image opens in graphic editor tools

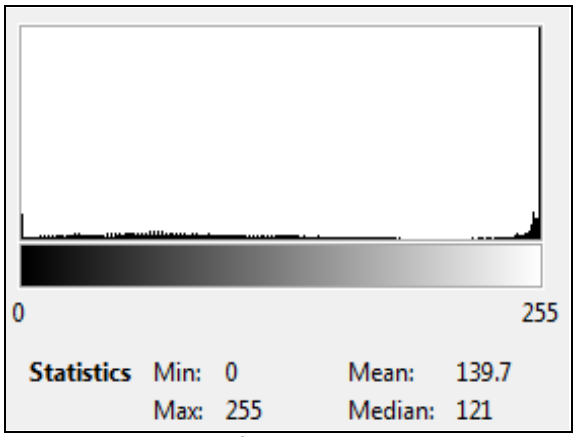

Figure 7: Histogram of graphic editor tools open image

2.3. Clone Detection

An extremely common practice of faking images is transplanting parts of the same image across the picture. For example, an editor may mask the existence of a certain object by "patching" it with a piece of background cloned from that same image, copy or move existing objects around the picture. Quantization tables of the different pieces will look very similar to the rest of the image, so we must employ methods identifying image blocks that look artificially similar to each other.

Figure 8: Original image

Figure 9: Clone image

The fig.8 is original image and the fig.9 is clone image the pasted object is scaled to appear larger (closer). The fig.9 image outlines matching points that allow detecting the clone image.

III. EXPERIMENT RESULTS

Dataset consist of different kinds of parameter like video resolution, frame rate, length and size of video etc., parameter tested for the getting the good quality of result. Every parameter which is considered in dataset can make effect on the results. Videos are taken from different camera or with different resolutions.

Figure 10: Original Video Frame of Star Sports channel

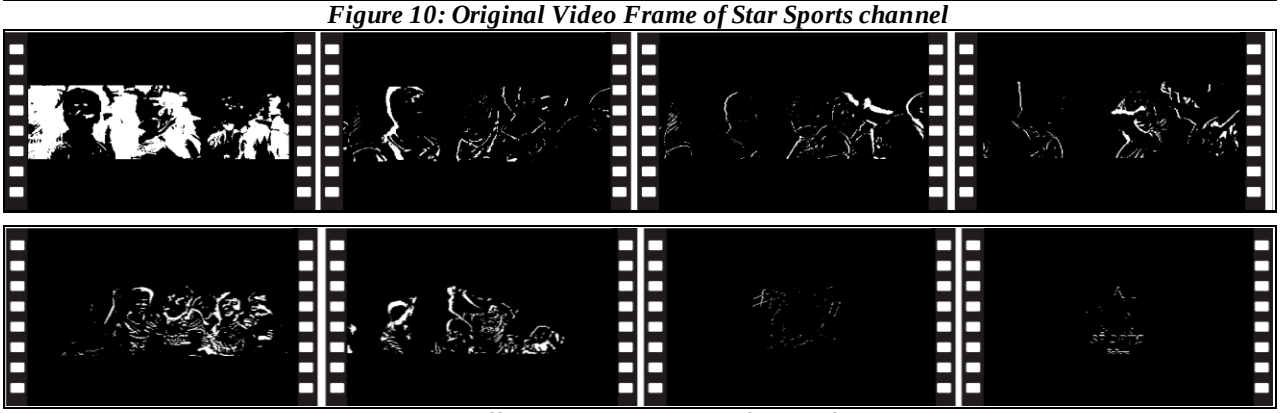

Figure 11: Binarized Difference original video frame of Star Sports channel

Figure 12: Duplicate Video Frame of hotstar channel

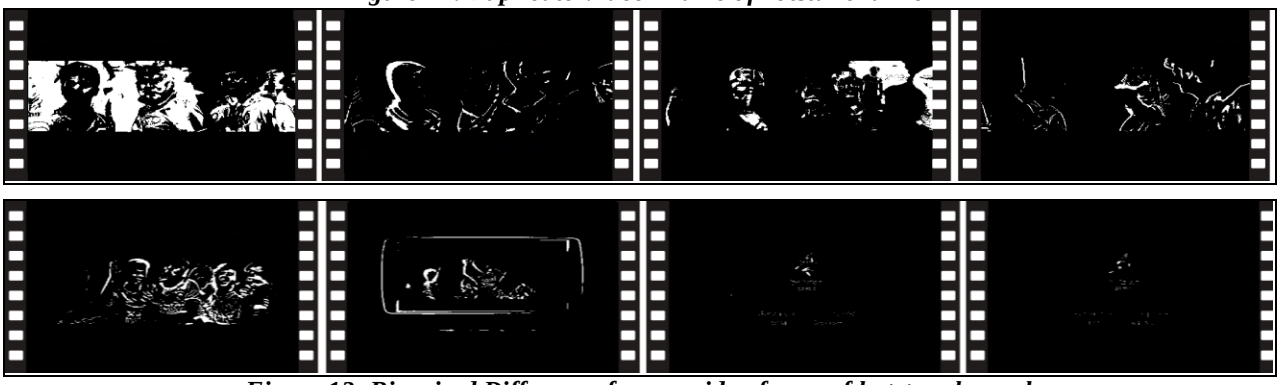

Figure 13: Binarized Difference forgery video frame of hotstar channel

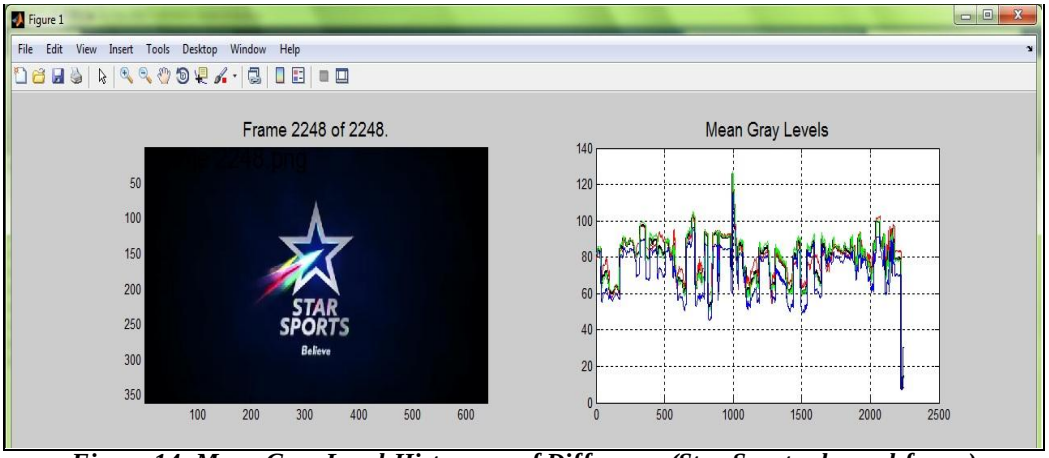

Figure 14: Mean Gray Level Histogram of Difference (Star Sports channel frame)

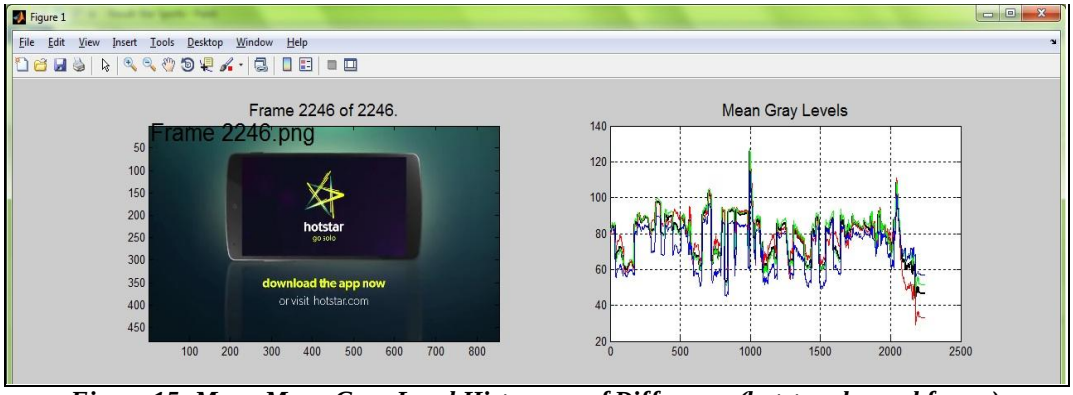

Figure 15: Mean Mean Gray Level Histogram of Difference (hotstar channel frame)

In Figure.14 shows that original video of Starspot channel histogram and Figure.15 forged video of hotstar channel histogram difference is identified, The Binarized difference of original video of Starspot channel is Figure.11 and forged video Binarized difference Figure.13 identified last three frame are modified in video and forgery video stream last two frame Starspot channel logo appear clearly. So, hotstar video is forgery video or doctored video.

Table 1: Comparison of original video and forgery video

EXIF Meta tage Information	Scene 1		Scene 2	
	Original[a]	Forgery[b]	Original[c]	Forgery[d]
Time Length	00:01:30	00:01:30	00:01:03	00:00:56
Frame Rate	25 fps	25 fps	23 fps	25 fps
No. of Frame	2248	2246	1449	1400
Data Rate	2607 kbps	823 kbps	6923 kbps	32292 kbps
Resolution	1920 x 1080	854 x 480	1920 x 1080	1920 x 1080
Bit Rate	125 kbps	125 kbps	159 kbps	Not Available
Total Bit Rate	2732 kbps	948 kbps	7082 kbps	32292 kbps
Audio Chanel	2 Stereo	2 Stereo	2 Stereo	Not Available
Audio Sample Rate	44kHz	44kHz	48 kHz	Not Available
Protected	Yes	No	Yes	No
Video Quality	High Quality	Poor Quality	High Quality	Poor Quality

Camera Based Editing Detection	No	No (Software Based Editing)	No	Yes
Size	29.3 MB	10.2 MB	53.2 MB	217 MB

Original[a] : Mauka Mauka (India vs Bangladesh) ICC Cricket World Cup 2015 Starsport channel original video

Forgery[b] : Mauka Mauka (India Vs Bangladesh) hotstar channel forgery video

Original[c]: Xperia HD Landscapes-Smartphone (Sony Z Ultra C6802) Original Video

Forgery[d] : Xperia HD Landscapes forgery video

IV. CONCLUSION AND FUTURE WORK

A wide range of passive 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 frame is not available, in that condition it can also detect the forgery frame. Proposed method ignores the necessity of having original frame for detecting forged frame. The tag information detection based on ELA and IPTC Meta tag properties.

We can more precisely; it is possible to divide video forensic techniques into three macro-areas concerning the acquisition, the compression, and the editing of the video signals. Moreover, anti-forensic interesting issue in order to identify those techniques that fined malicious user in order to hide alterations information on the signal and how to prevent them.

REFERENCES

[1]. Hitesh C. Patel, Mohit M. Patel, "An Improvement Of Forgery Video Detection Technique Using Error Level Analysis" IJCA February 2015.
[2]. 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.
[3]. A. Gironi, M. Fontani, T. Bianchi, A. Piva, M. Barni, "A Video Forensic Technique For detecting frames deletion and insertion" IEEE 2014.
[4]. Govindraj B. Chittapur, S. Murali, "Digital Doctored Video Forgery Detection Techniques" IJATER 2014.
[5]. P.G.Gomase, N.R.Wankhade, "Advanced digital image forgery detection" ICAET 2014.
[6]. Mohd Dilshad Ansari, S. P. Ghrera and, VipinTyagi, "Pixel-Based Image Forgery Detection" IETE 2014.
[7]. Amanpreet Kaur, Richa Sharma, "Optimization of Copy-Move Forgery Detection Technique" IJARCSSE 2013.
[8]. Vimal Raj V, Lija Thomas, "A Novel Approach for Forgery Detection of Images" IJAIEM 2013.
[9]. Alexey Kuznetsov, Yakov Severyukhin, Oleg Afonin, Yuri Gubanov, "Belkasoft Evidence Search and Analysis Software for Digital Forensic Investigations" 2013.
[10]. Murali S, Anami B. S, Chittapur G B, "Detection of Digital photo Image forgery" IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) 2012.
[11]. S.Murali, Govindraj B. Chittapur, Prabhakara H. S, Basavaraj S. Anami, "Comparison and analysis of photo image forgery detection techniques." IJCSA 2012.
[12]. Stamm M C, Ray Liu K J, "Anti-forensics for frame deletion/addition in MPEG video" International conference on acoustics, speech and signal processing, IEEE 2012.

