International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 8, Issue 12 [December 2019] PP: 19-22

DETECTION OF FAKE DIGITAL VIDEOS

S. Vishal, S. Subramanian

ABSTRACT: Digital video is commonly used by news organizations and evidence of specific events by law enforcement. Many surveillance systems record footage using digital video rather than film due to the ease with which digital video can be stored. These types of footages are made fake by some criminals thus by cheating the government. In order to provide a satisfactory solution for this problem fake video detection concept is introduced. In this concept, we use a set of techniques for evaluating the performance of anti-forensics operations in order to analyze the interplay between a forensic investigator and a forger. Thus if any changes are made in a digital video, it could be easily detected thus providing a truthful evidence to the government.

I. INTRODUCTION

To verify the authenticity of digital video files, digital forensic techniques have been developed to detect video manipulation and to identify digital video forgeries. This verification process mainly includes the processes like detection of video frame deletion or addition of new frames and recompression. Frame deletions are mainly performed by a video forger in order to remove a certain portions of a video sequence such as a person's presence in surveillance video etc. To prevent digital forgers from gaining an upper hand, the digital subframes community must develop and study anti-forensic operations. By doing so, forensic investigators can be made aware of weaknesses/ demerits in the existing forensic techniques and a better knowledge about the results could be given to the investigators.

In addition to this, it is likely known that the anti-forensic operations leave behind an evidence of their use which is just as a digital editing operations do. If anti-forensic operations are developed and studied by digital forensic researchers, different innovative techniques could be developed which are capable of detecting the use of anti-forensic operations. When a video sequence is captured, there is typically a great deal of redundancy between each frame of video. The video compression exploits this redundancy by predicting certain frames in the video sequence from others, then encoding the residual error between the predicted frame and the actual frame. Because the prediction error can be compressed at a higher rate than a frame in its entirety, this leads to a more efficient compression scheme. Performing compression in this manner has its drawbacks, however, because error introduced into one frame will propagate into all frames predicted from it.

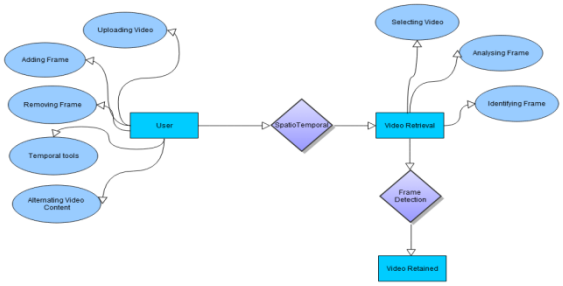
II. EXISTING SYSTEM

In the existing system a set of statistical tools for detecting traces of digital tampering in the absence of any digital watermark or signature. The nature of statistical correlations that result from specific forms of digital tampering, and have devised detection schemes to reveal these correlations. The tools that, in the same spirit of those presented here reveal statistical correlations that result from a variety of different manipulations that are typically necessary to create a convincing digital forgery. Analyzing the sensitivity and robustness to counter-attack of each of the schemes outlined. While digital forensic techniques are designed to identify digital forgeries even when the forgery is perceptually undetectable by humans. They do not consider the possibility thata forger may design and use anti-forensic operations to remove forensic evidence of their forgery. Though a variety of different video compression, a great deal of redundancy exists between video frames. The prediction error can be compressed at a higher rate than the frame allowing for smaller file sizes.

III. PROPOSED SYSTEM

We propose an anti-forensic technique designed to fool video forensic techniques and develop a method for detecting the use of anti-subframes. To verify the authenticity of digital video files, digital forensic techniques have been developed to detect video manipulation and identify digital

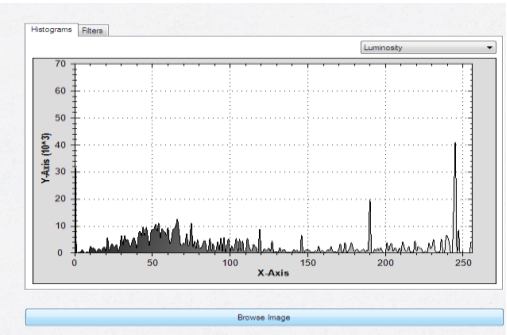
video forgeries. One of these techniques is targeted towards video codecs that use fixed length GOPs (Group of Picture) when compressing the video. We propose an anti forensic technique capable of hiding frame deletion or addition in digital videos. In order to prevent the propagation of channel and decoding errors, not all frames are predicted. Instead the video sequence is segmented into sets of frames known as GOP. In order to design an automatic frame deletion or addition detection technique as well as an anti forensic method to remove, recompressing and viewing it as the deletion of a negative number of frames.



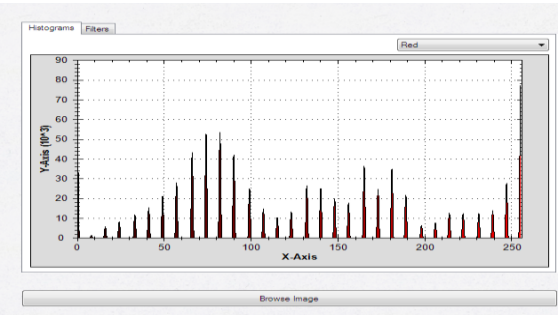
IV. ALGORITHM

SIFTScale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images. For any object in an image, interesting points on the object can be extracted to provide a "feature description" of the object. This description, extracted from a training image, can then be used to identify the object when attempting to locate the object in a test image containing many other objects. To perform reliable recognition, it is important that the features extracted from the training image be detectable even under changes in image scale, noise and illumination. Such points usually lie on high-contrast regions of the image, such as object edges.

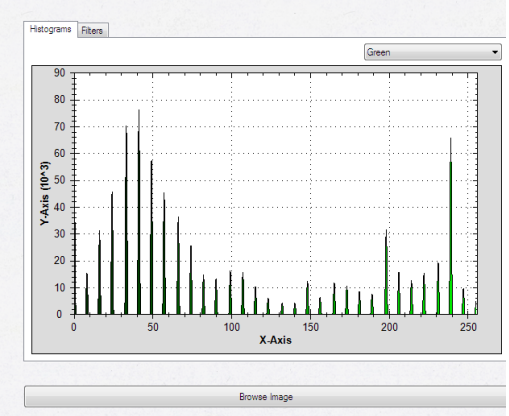
Histo value:



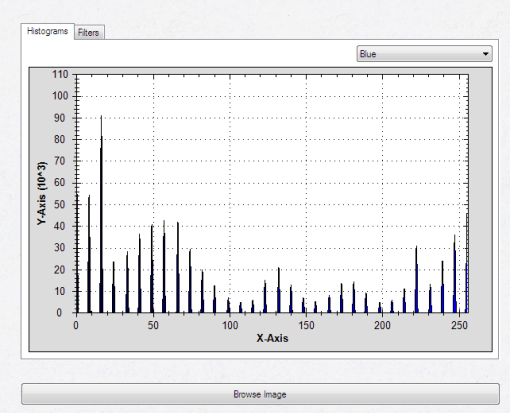
Histo red:



Histo green:



Histo blue:



VOTE BASED

This alignment can be used not only for aligning non-overlapping sequences, but also for handling other cases that are inherently difficult for standard image alignment techniques.

V. FINGERPRINT

Temporal fingerprinting scheme based on local spatio-temporal features. The spatio-temporal interest point detector is first exploited to detect local regions in the input video clips. For each local region, contrast content histogram (CCH) is then used to calculate the intensity differences, and a unit vector obtained by normalizing CCH is used as the local fingerprints.

VI. ADVANTAGES

- This concept of detecting the changes in digital videos gives more accurate results than the old and existing system.
- If there is any repeatation in the frame, it can be easily detected using phoney video exposure techniques whereas in existing it is not possible to identify the repeated frames.
- This technique of detecting the fake videos minimizes the procedure.
- The main difference between the existing system and the phoney video exposure is that when a frame is compressed, the quality of the frames will not be affected.

VII. CONCLUSION

This study of fake video detection suggests that domain-specific knowledge improves the results thus ensuring that no information is lost over time. In this technique, the anti-forensic operations are capable of removing the temporal fingerprints that arises in video sequences when any frames are added or deleted which is followed by recompression. The key factor behind this phoney video exposure is the identification of temporal fingerprint and using these to model the effect of

frame deletion or addition of frames on the P-frame prediction error sequence. Digital images have an inherent amount of noise introduced either by the imaging process or digital compression which also supports the detection of forgeries in digital videos.

REFERENCES

[1]. A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in Proc. 6th Int. Workshop Information Hiding, Toronto, Canada, 2004, pp. 128–147.

[2]. M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[3]. A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf.* Forensics Security, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[4]. I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "A classifier design for detecting image manipulations," in Proc. IEEE Int. *Conf.* Image Processing, Oct. 2004, vol. 4, pp. 2645–2648.

[5]. M. C. Stammand K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics

[6]. *Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010.

[7]. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 37–47.

[8]. W. Wang and H. Farid, "Exposing digital forgeries in interlaced and de-interlaced video," IEEE Trans. Inf. Forensics Security, vol. 3, no. 2, pp. 438–449, Jun. 2007.

[9]. M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Source digital camcorder identification using sensor photo response non-uniformity," in Proc. SPIE Electronic Imaging, Photonics West, Feb. 2007, vol. 6505.

[10]. C. Kraetzer, A. Oermann, J. Dittmann, and A. Lang, "Digital audio forensics: A first practical evaluation on microphone and environment classification," in Proc. 9th Workshop on Multimedia and Security, New York, 2007, pp. 63–74, ACM.

[11]. D. Garcia-Romero and C. Y. Espy-Wilson, "Automatic acquisition device identification from speech recordings," in Proc. IEEE Int. Conf.Acoustics, Speech, and Signal Processing, Mar. 2010, pp. 1806–1809.

[12]. C. Grigoras, "Digital audio recording analysis: The electric networkfrequency (ENF) criterion," Int. J. Speech Language and the Law, vol. 12, no. 1, pp. 63–76, Mar. 2005.

[13]. M. Kirchner and R. Böhme, "Hiding traces of resampling in digital images," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 582–592, Dec. 2008.

[14]. T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?," in Proc. 15th Int. Conf. Multimedia, 2007, pp. 78–86.

[15]. M. C. Stamm, S. K. Tjoa,W. S. Lin, and K. J. R. Liu, "Anti-forensi,cs of JPEG compression," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Mar. 2010, pp. 1694–1697