Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.438 – 442

REVIEW ARTICLE

Review of Techniques for Detecting Video Forgeries

Aniket Pathak[1], Dinesh Patil[2]

[1]PG Scholar, Department of CSE, SSGBCOET Bhusawal, Maharashtra, India

[2]Associate Professor, Department of CSE, SSGBCOET Bhusawal, Maharashtra, India

[1] aniketpathak89@gmail.com; [2] dineshonly@gmail.com

Abstract— In today's fast and speedy life the role of multimedia has increased in considerable manner, in which the use of digital images and videos has increased. With the availability of advance digital video processing technologies, various kinds of videos are produced from different perspectives. In Legal cases in court hearings it's observed that changes done have been made to accept videos from digital cameras as witnesses. As a result there is a growing interest in forensic analysis of video content where the integrity of digital images and videos need to be checked. In this respect it has become essential to analyze whether a particular video is an original-real one or one that has been tampered using any technique. As video editing techniques are getting very complicated, modified videos are hard to detect. However, when a video is modified, some of its basic properties get changed. Then to detect those changes it is needed to use complex and video processing techniques and algorithms, in this paper we review the various existing methods that are used to find whether the video is real one or not.

I. INTRODUCTION

In recent years due to easy availability of video and image editing tools it has become a difficult task to authenticate the multimedia content. Due to the availability of inexpensive and easily-operable digital multimedia devices (such as digital cameras, mobiles, digital recorders, etc.), together with high-quality data processing tools and algorithms, has made signal acquisition and processing accessible to a wide range of users. As a result, a single image or video can be processed and altered many times by different users. This fact has severe implications when the digital content is used to support legal evidences since its originality and integrity cannot be assured. Important details can be hidden or erased from the recorded scene, and the true original source of the multimedia material can be concealed. Moreover, the detection of copyright infringements and the validation of the legal property of multimedia data may be difficult since there is no way to identify the original owner.

Digital videos and images having fraudulent content are used for illegal activities. Therefore, integrity of digital content needs to be verified. This can be done by analysing the properties of the digital media. There are various techniques which have been developed to detect various method of forgery or we say tampering. Video frame duplication, video double MPEG compression, Image region duplication and Image double JPEG compression are some of them. It is often advantageous to verify if a digital video has been altered by the above methods.

The contribution of this paper relies in providing an overview of the main techniques that have been designed to detect the forgery in video. Section 2 deals with the detection using HOG features and compression properties. In section 3 detection using MPEG double compression. Detection using correlation in noise is addressed in Section 4. Detection using statistical tools is discussed in Section 5. Finally we conclude indicating summary of issues in the relevant field of video forgery detection.

II. DETECTION USING HOG FEATURES AND COMPRESSION PROPERTIES

In this video forgery detection technique mainly useful to detect the spatial and temporal copy paste tampering. As it is challenging to detect this type of tampering in videos as the forged patch may invariably vary in terms of size, compression rate and type (I, B or P) or other changes such as scaling and filtering. The algorithm as in [1] is based on Histogram of Oriented Gradients (HOG) feature matching and video compression properties. The advantage of using HOG features is that they are robust against various signal processing manipulations. Image or frame can be represented by using a set of local histograms [2]. These histograms count the number of occurrences of gradient orientation in a local spatial region of the image known as cell. Typically, a cell size may vary as 4x4, 6x6 or 8x8 pixels. In order to extract the HOG features, first the gradients of the image are computed followed by building a histogram of orientation at each cell. Finally the histogram obtained from each cell in a block is normalized which gives the HOG descriptor of that block, where a block may comprise of 2x2 or 3x3 cells.

In this section we review copy-paste forgery detection scheme in brief. In the spatial forgery detection, First of all, apply mechanism for image thresholding which is used to set the cell size. Then the HOG features are generated for each block and simultaneously find matches for individual block descriptors. Then next is the temporal forgery detection. Here, based on compression properties frames in a GOP are selected. Then the HOG features are generated block-wise. Finally, these descriptors are compared with the spatially co-located descriptors to find if a match exists as in [1].

III. DETECTION BY MPEG DOUBLE COMPRESSION

Recently digital video recording systems are widely used. It is important to reliably authenticate the trueness and validity of a given video. Some good results were obtained in the field of digital forgery detection, as in [3][4]. But a lot of them have focus on the detecting image tampering, as in [5]. Digital videos were usually compressed with MPEG-x or H.26x coding standard. The tampering has to be operational in uncompressed domain to accomplish frame deletion, frame inserting, etc. Considering factors that includes size and format, the tampered video has to be re-encoded. Thus, the occurrence of double compression may expose digital forgery. Ref. [6] proposed use of periodicity of the artifacts introduced into the Discrete Cosine Transform (DCT) coefficient histograms as evidence of double compression. A parametric logarithmic law, i.e. the generalized Benford’s law was first modeled to detect JPEG double compression in [7]. Ref. [8] validated the feasibility of this principle in MPEG coded video.

A. MPEG double compression detection algorithm

Machine learning framework is adopted to enhance accuracy due to sensitive nature of first digit distribution to video content and target bit rate, Fig. 1 as in [9] demonstrates the algorithm architecture. The detailed process described in [9] is as follows:

1) Extract the first digit distribution of quantized AC coefficients for both query and training video.
2) Test the first digit distribution with parametric logarithmic law. Three goodness-to-fit statistics are calculated, including squares due to error (SSE), root mean to zero, R-square closer to one means a good fit.
3) Compose a 12-D feature by combining the first digit probabilities and goodness-to fit statistics. Consider only I frames as the fitting results for intra frames are better than that for non-intra frames.
4) Detection unit comprises of each GOP with a 12-D feature, so the SVM classifier judges on a GOP basis. Define the GOP proportion D as $D = \mathrm{n} / N$. Where n stands for the number of GOPs which are labeled as double compression, and N means the total number of GOPs. If D passes the threshold T, it is extremely possible that the video has gone through double compression. Over here T is adaptive according to the demand of TNR and TPR. Generally T might be set as 0.50.

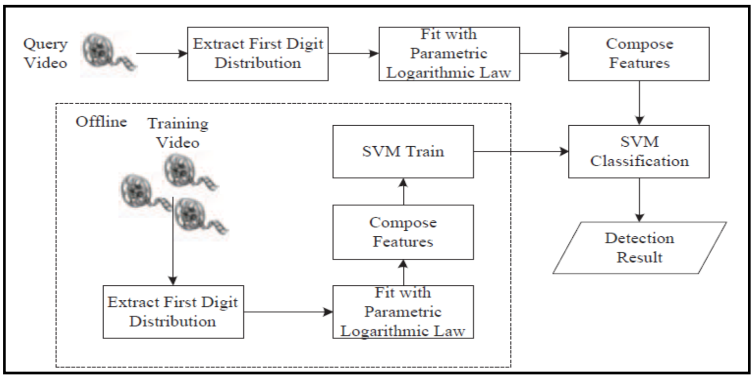
Query Video
Extract First Digit Distribution
Fit with Parametric Logarithmic Law
Compose Features
Offline
Training Video
SVM Train
SVM Classification
Compose Features
Detection Result
Extract First Digit Distribution
Fit with Parametric Logarithmic Law

Fig. 1 Double compression detection algorithm architecture

B. *Original bit rate estimation algorithm*

Taking a closer look towards fitting results of doubly compressed MPEG video, the difference between situations of decreasing and increasing target bit rate is noteworthy. This acts as trigger for a more detailed classification. The serial SVM architecture for this estimation is shown in Fig. 2 as in [9]. If target bit rate is larger than original bit rate then obviously the violation of the parametric logarithmic law will be much more. So SVM1 classifies the bit rate increasing situation and SVM2 focuses on original video and the judgment of bit rate decreasing situation. For results, the probability p = C / N is calculated. Where C stands for the number of GOPs which are labelled as a certain class and N is the total number of GOPs in a video. p is confidence index.

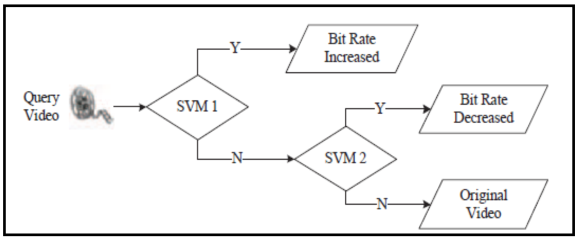

Fig. 2 Serial SVM architecture for original bit rate estimation

IV. Detection Using Correlation of Noise

In this section we review an approach for locating forged regions in a video using correlation of noise residue. In this method, as a feature for classification the block-level correlation values of noise residual are extracted. The distribution of correlation of temporal noise residue in a forged video is modelled as a Gaussian mixture model (GMM). We have a two-step scheme to estimate the model parameters. Also the optimal threshold value is found using a Bayesian classifier based on the estimated parameters. The bottom-up approach is used for locating the forged/inpainted regions of a video based on block-level temporal noise correlation. The flowchart of the video forgery detection algorithm is shown in Fig. 3. In the first step, following the same process as proposed in [11], by subtracting the original frame from its noise-free version the noise residue of each video frame is extracted. To obtain the noise-free image the wavelet denoising filter proposed in [12] is used.

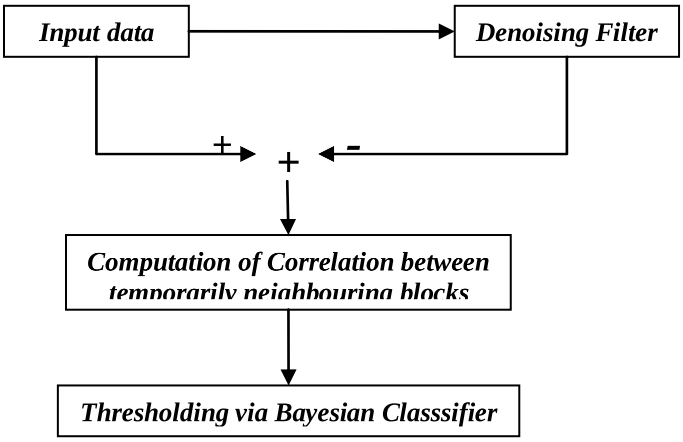
Input data
Denoising Filter
+
+
-
Computation of Correlation between temporarily neighbouring blocks
Thresholding via Bayesian Classsifier

Fig. 3 Flowchart of method for forgery detection using correlation of noise

In the second step, first partition each video frame into non-overlapping blocks of size N × N. Compute as illustrated in Fig 4 as in [10] the correlation of the noise residue between the same spatially indexed blocks of two consecutive frames is then.

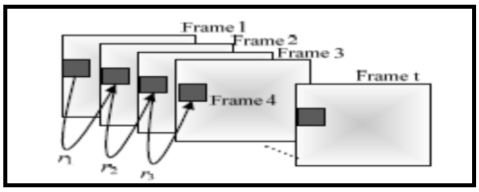

Fig. 4 Illustration of computing the correlations of the noise residue between every two temporally neighboring video blocks

In final step locate tampered blocks by analysing the statistical properties of block-level noise correlations. In the first part of this step, to obtain a coarse classification a simple thresholding scheme is exploited. A GMM (Gaussian Mixture Model) model is applied to characterize the statistical distributions of block-level temporal noise correlations for tampered and non-tempered regions, respectively based on the coarse classification. The GMM model parameters are then estimated using the EM algorithm so that optimum thresholds can be derived accordingly using the maximum-likelihood (ML) estimation and Bayesian classifier.

V. DETECTION USING STATISTICAL TOOLS

In this section we review a class of statistical techniques used for detecting traces of tampering in the absence of any watermark or signature. All these approaches mainly work on the assumption that although digital forgeries may leave no visual clues of having been tampered with but they may or may not alter underlying statistics of an image. Consider, for example as in [13], the creating a digital forgery that shows a pair of famous film stars, rumoured having a relationship. Such a photograph could be created by splicing together individual images of each film star and overlaying the digitally created composite onto a sunset beach. To create a convincing match, it is necessary to (1) Re-size, rotate, or stretch portions of the images (e.g. re-sampling) (2) Apply luminance non-linearities (e.g., gamma correction) to portions of the image in order to adjust for brightness differences; (3) Add small amounts of noise to conceal evidence of tampering; and (4) re-save the signal image (typically with lossy compression such as JPEG). Although these manipulations are often unnoticeable to the human eye, they might be introducing specific correlations into the image, which when detected can be used as confirmation of digital tampering. After quantifying statistical correlations that result from each of these specific forms of digital tampering, work out detection schemes to reveal the correlations. The effectiveness of these techniques can be shown on a number of simple synthetic examples and on perceptually credible forgeries.

VI. CONCLUSION

This paper mainly focused on different techniques used for detecting of forgery in video. In forgery detection technique using HOG features and video compression properties we had the parameter cell size of the HOG feature generation set adaptively which increased the detection accuracy for spatial forgery detection and in temporal forgery detection, the frames with high correlation for duplicated regions compared to authentic regions are selected for detection purpose. Algorithm used over here gave good detection accuracy under unfavorable operations such as compression, scaling and filtering for spatial forgery detection while compression and filtering for temporal forgery detection. This algorithm performed better when dealing with the copy-paste tampering. We also studied a digital video forgery detection scheme in which there was a statistical classification scheme based on a GMM model and the Bayesian classifier. This technique is useful for Digital videos are usually compressed with MPEG-x or H.26x coding standard. Thus after reviewing different techniques it can be concluded that as an interesting research area with many methods available a new approach can be still devised to give a better result in detection to all type of tampering done with digital or multimedia content. To propose such a method still remains a challenging issue for researcher.

REFERENCES

[1] Subramanyam, A. V., and Sabu Emmanuel. "Video forgery detection using HOG features and compression properties." *Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on*. IEEE, 2012.

[2] N. Dalal and B. Triggs, "*Histograms of oriented gradients for human detection*," in Proc. CVPR'05, 2005.

[3] Wang, Weihong, and Hany Farid. "Exposing digital forgeries in video by detecting duplication." *Proceedings of the 9th workshop on Multimedia & security*. ACM, 2007.

[4] Kobayashi, Michihiro, Takahiro Okabe, and Yoichi Sato. "Detecting forgery from static-scene video based on inconsistency in noise level functions." *Information Forensics and Security, IEEE Transactions on* 5.4 (2010): 883-892.

[5] Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detecting copy-move forgery in digital images: a survey and analysis of current methods." *Global Journal of Computer Science and Technology* 10.7 (2010).

[6] Wang, Weihong, and Hany Farid. "Exposing digital forgeries in video by detecting double MPEG compression." *Proceedings of the 8th workshop on Multimedia and security*. ACM, 2006.

[7] Fu, Dongdong, Yun Q. Shi, and Wei Su. "A generalized Benford's law for JPEG coefficients and its applications in image forensics." *Electronic Imaging 2007*. International Society for Optics and Photonics, 2007.

[8] Chen, Wen, and Yun Q. Shi. "Detection of double MPEG compression based on first digit statistics." *Digital Watermarking*. Springer Berlin Heidelberg, 2009. 16-30.

[9] Sun, Tanfeng, Wan Wang, and Xinghao Jiang. "Exposing video forgeries by detecting MPEG double compression." Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on. IEEE, 2012.

[10] Hsu, Chih-Chung, et al. "Video forgery detection using correlation of noise residue." *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*. IEEE, 2008.

[11] Bayram, Sevinc, et al. "Source camera identification based on CFA interpolation." *Image Processing, 2005. ICIP 2005. IEEE International Conference on*. Vol. 3. IEEE, 2005.

[12] Mıhçak, M. Kıvanç, Igor Kozintsev, and Kannan Ramchandran. "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising." *Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on*. Vol. 6. IEEE, 1999.

[13] Popescu, Alin C., and Hany Farid. "Statistical tools for digital forensics."*Information Hiding*. Springer Berlin Heidelberg, 2005.