RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

A Review on Video Authentication and Statistical Feature Detection

KEYWORDS: Video authentication, Authentication Techniques, Feature Detection Techniques, Edge, Corner, and SIFT

Tushar P. Lakhani	Prayag M. Patel
ME (CSE Student), S. P. B. Patel Engineering College, Mehsana, Gujarat	Assistant professor, CE Department, S. P. B. Patel Engineering College, Mehsana, Gujarat,

ABSTRACT A video authentication is a process of that verify the given digital video is authentic and exactly same as when captured. In current scenario different types of digital and multimedia editing software used to manipulation of video sequence frames and object motion very easily. In this paper, Feature detection techniques such as Edge, Corner, and Scale invariant feature transform (SIFT). An also include these all feature detection techniques comparison and drawbacks. SIFT local invariant feature has many applications in different fields such as image retrieval, strong matching ability and machine vision. In this paper analyze the various Low level feature detection methods and main aim at computing image information and detect every image point.

I. INTRODUCTION

In today's digital era, communication and compression techniques simplify sharing of Multimedia data such as image and video [1]. The increasing complexity of computing devices and its equipments have made digital manipulation of video sequences very easy to perform [1]. In some applications the authenticity of video data is of vital interest such as in video investigation, forensic investigations, law enforcement and content rights [1]. For example, in court of law, it is important to found the faith value of any video that is used as confirmation so, video authentication is a process which establishes that the content in a given video is original and correct same as when captured. In paper, Different Types of Feature detection include Edge detection, Corner detection, and Scale invariant Feature transform (SIFT) local feature detection used in image detection. These features are very useful in image processing for retrieve various image features. SIFT features could hardly detect the duplications of regions.

II. AN AUTHENTICATION TECHNIQUE

By definition, authenticity means sometimes "as being in accordance with fact, as being true in substance", or "as being what it professes in origin or authorship, as being genuine"[1].

Basically video authentication techniques are broadly classified into four categories: Digital Signature based techniques, watermark based techniques, intelligent techniques, and other Authentication techniques [1]

1) Digital Signature

The digital signature method introduced by Diffie and Hellman in 1976 [2]. The digital signature depends on the content and secret information which is only known to the signer [4].Therefore, it cannot be artificial, and the evaluator can verify whether the content of video information matches the information contained in the digital signature. In other words, we can trust the signer as well as his/her digital signature to verify the data integrity [4].

Two types of robust digital signatures are used for video authentication in different kinds of situations. The first type of authentication signature is used in situation where the GOP (Group of Pictures) configuration of the video is not modified, after transcoding or editing processes. The situation, where the GOP structure is modified and only the pixel values of picture are preserved, a second type of digital signature is used [3].Digital signature methods have taken few research directions message authentication code, visual hash, robust hash and digital signature itself [4]. These techniques follow a common technique for authentication: feature extraction and subsequent use of the features for later authentication [4]. A technique for image authentication is proposed by [4] in a semi fragile way to detect the tampered pixels of an image.

2) Watermarking

Watermarking is the process that embeds data called a watermark into an image or audio or video. Watermarking is a technique to embed copyright or other information into the underlying data [5]. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking. The approach of watermarking has been employed to protect intellectual property of audio, images and video data [5]. An invisible watermarking technique in spatial domain is suggested and in wavelet domain is suggested in [5].

Visible watermarking technique in frequency domain is suggested in whereas dual domain technique is suggested in for images and for audio in [6]. Invisible watermarks can be mostly divided into two types, robust and fragile, most of the research and applications focus on strong watermarks.

According to the type of documents to be watermarked, the watermarking techniques can be divided into four types: Image Watermarking, Video Watermarking, Audio Watermarking and Text Watermarking. Digital images can be produced from many sources, such as everyday photographs, Satellite pictures, medical scans, or computer graphics. Watermarks for natural images typically modify pixel strengths or transform coefficients, although it is possible that a watermark could alter other features such as edges or textures. An image may be Viewed for an lengthy period of time, and it may also be subject to a countless deal of manipulation, such as filtering, cropping, geometric transformations, Compression and compositing with other images, and violent attacks.

3)Intelligent Techniques

Intelligent techniques for video authentication use database of video sequences. The database includes authentic video clips as well as tampered video clips. As in [1], authors

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

proposed an intelligent technique for video authentication which uses characteristic video information for authentication, thus making it useful for real world applications. An Intelligent technique basically includes the video authentication by using machine learning algorithms. Here the machine learning algorithm uses Support Vector Machine (SVM) for the classification of the tampered and authentic videos. SVM [1] is a powerful methodology for solving problems in nonlinear classification, function Estimation and density estimation [1]. In fact SVM is a nonlinear classifier that performs classification tasks by creating hyper planes in a multi-dimensional space and separates the data points in different classes.

4) Other Authentication Techniques

other authentication system for digital video is introduced which is based on motion trajectory and cryptographic secret sharing [1]. In this system, the given video is firstly segmented into shots then all the frames of the video shots are mapped to a trajectory in the feature space by which the key frames of the video shot are added. Once the key frames are evaluated, a secret frame is computed from the key frames information of the video shot. These secret frames are used to construct a hierarchical structure and after that final master key is obtained. This master key is used to identify the authenticity of the video.

III.FEATURE DETECTION

Transforming the input data into the set of features is called feature detection. If the features detection are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation in place of the full size input. Feature detection can be divided into three categories namely edge, corner, and Local Invariant Feature SIFT. However, some combine more than one technique to obtain a superior result.

1) Edge Detection

Edge detection is a basic tool used in image processing, basically for feature detection and extraction, which aim to identify points in a digital image where brightness of image changes sharply and find gaps [7]. The purpose of edge detection is meaningfully reducing the amount of data in an image and conserves the structural properties for further image processing. In a grey level image the edge is a local feature that, with in a area separates regions in each of which the gray level is more or less uniform with in different values on the two sides of the edge [8]. Edge detection is a process that detects the existence and location of edges established by sharp changes in color brightness of an image In the ideal case, the result of applying an edge detector to an image may lead to a set of connected curves that indicate the boundary of objects, the boundary of surface markings as well curves that related to discontinuities in surface orientation [9].

The other well-known techniques for edge detection are grouped mainly in two categories [10]: search based techniques and zero crossing algorithms. In zero crossing detectors, second order derivative is computed for edge detection while in case of search based methods first order derivatives are computed. The most well-known conventional methods like Sobel, Canny, Prewitt, and Laplacian belong to one of the above classes.

The advantages and disadvantages of various edge detection techniques are explained as following [10]:

Operator	Advantages	Disadvantages
Classical operators like Sobel operator	Simplicity	Inaccurate, sensitive to noise
Laplacian of Gaussian (LoG)	Test wider areas around the pixels, Find the correct places of edges	Does not function properly at the corners and curves where the intensity abruptly changes
Zero Crossing operators like laplacian	Have fixed characteristics in all directions	Sensitive to noise, Respond to some of the already existing edges
Gaussian operators like Canny	Improved signal to noise ratio, Shows better detection in the noise conditions	Complex computations, Takes more time.

1) Corner Detection

Corner looks for sharp image features while blobs look for smooth image features. Corner detection is classified under interest point detection since it has those properties. They can be divided into two categories: feature based (or direct) corner detectors and geometry-based corner detectors. Feature-based corner detectors design a set of feature templates and similar features in sub-windows of a gray level image. Geometry-based corner detectors rely on measuring the different geometrical shapes of corners. Some of them are widely used in a variety of applications.

Basically three Types of Corner detection include in image processing following: The Wang-Brady Corner detection, the Plessey Corner detection and the Smallest Univalue Segment Assimilating Nucleus (SUSAN), Corner detection. The Plessy algorithm was found to have good stability and accuracy, but suffered from a large computational cost. The SUSAN method required the least computational resources and would therefore be suitable for implementation on a simple Field Programmable Gate Array (FPGA) platform. The Wang-Brady method was originate to have better stability than SUSAN but worse than the Plessy algorithm while having a worse computational cost than Plessy and a greater cost than that for SUSAN.

2) Scale Invariant Feature Transform (SIFT)

SIFT key points of objects are first extracted from a set of reference image and stored in a database. The SIFT descriptor is invariant to translations, rotations and scaling transformations in the image domain and robust to moderate perspective transformation and illumination variation.

SIFT is a method of extract characteristic invariant features from images. In SIFT include key point and local feature descriptor and there are different kinds to compute these features as follows [12]: select person for feature extraction by searching points in the scale space from difference of Gaussian (DoG) function, locate key points using measures of their stability, Assign directions based on local image incline path and calculate the local image key point descriptors based on the set of close image gradients. SIFT technique has some disadvantages. It is based on histogram which expresses grads differences in every scale and feature direction. The complex of time is very difficult.

In current techniques of copy move image detection can classified into different methods as [13] Block based

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

methods and key point based methods. Block based method used to identify the forged area and the image is divided into small overlapping blocks. The key point based method is that in using SIFT algorithm to detect the copy move forgery and is strong post processing on the images [13].

Basically SIFT algorithm used to finding the key point, key point detection and feature descriptor apply on different images [14]. In SIFT feature first detect key points in an image and compute the SIFT features for such key points. SIFT consist of the different stages include as [14] scale space extreme detection, key point localization, orientation assignment and key point descriptor.

IV. CONCLUSION

Video authentication is a very critical problem and high importance in various applications such as video surveillance and presenting video evidence in court of law. Intelligent authentication techniques can recognized by using any statistical feature of the video frames and a large numbers of video database and collections are detect and verify these processed video frames are or authentic or not. In this paper analyzes different video retrieval features detection techniques. Based on the analysis, we use local invariant feature of SIFT and it is widely used to describe video frames and digital image retrieval. The SIFT based technique is dependent on feature extraction by using key point detection and after apply feature matching of overall image key points and matching points. This method is widely used to detect different video frame features and also detection of malicious manipulation in case of digital image copy move attack.

REFERENCE

[1]. S.Upadhyay, S.K.Singh, M. Vasta, and R. Singh, "Video authentication using relative correlation information and SVM", In Computational Intelligence in Multimedia Processing: Recent Advances(Springer Verlag) Edited by A.E.Hassanien, J.Kacprzyk, and A.Abraham,2007. | [2]. W. Diffie and M.E.Hellman, "New Direction in cryptography", IEEE Trans. On Information Theory, Vol.22, No. 6, pp.644-654, November 1976. | [3]. Ching-Yung Lin, Shih-Fu Chang, "Issues and solutions for authenticating MPEG Video", SPIE electronic Imaging 1999, San Jose. | [4]. Ching-Yung Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection", Ph.D. Thesis, Columbia University, December. 2000. | [5]. W. Zhu, et al., "Multi-resolution Watermarking for Images and Video", IEEE Tran. On circuits & Systems for Video Technology, Vol.9, No. 4, June 1999, pp.545-550. | [6]. I.J.Cox, et al., "secure Spread Spectrum Watermarking for Multimedia" IEEE Trans. On Image Processing, Vol.6, No.12, December 1997, pp.1673-1687. | [7]. Rashmi, Mukesh kumar, and Rohini Saxena, "Algorithm and Technique on Various Edge Detection: A Survey", Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.3, June 2013. | [8]. Rohit Patel, Puspendra Kumar Vashishtha, Priyanka Sahni, Ashwini Kumar, "Survry On Image Processing With Edge Detection Techniques", Indian Journal Of Research, Vol.3, Issue: 5, may 2014. | [9]. G.T.Shrivakshan, DR.C.Chandrasekar, "A Comparison Of Various Edge Detection Techniques used in Image processing", International Journal Of Computer Science (IJCSI), Vol. 9, Issue 5, No. 1, September 2012.| [10]. Komal Sharma, navneet Kaur, "Comparative Analysis of Various Edge Detection Techniques", Internatational Journal of Advanced Research in Computer Science and Sofeware Engineering, Vol.3, Issue 12, ISSN:2277 128X, December 2013. | [11]. Li Jing, Chao Shao, "Image Copy Move Forgery Detecting Based On Local Invariant Feature", Journal Of Multimedia, Vol.7, No.1, February 2012. | [12]. Salam A. Thajeel, Ghazali Bin Sulong, "State Of The Art Of Copy-Move Forgery Detection Techniques: A Review", Internationational Journal Of Computer Science Issues, Vol.10, Issue 6, No.2, November 2013. | [13]. Swapnil H. Kudke, A.D.Gawande, "Copy-Move Attack Forgery Detection by using SIFT", International Journal Of Innovative Technology and Exploring Engineering (IJITEE), Vol.2, Issue 5, April 2013.