IJCSC 0973-7391 Volume 7 • Number 1 Sept 2015 - March 2016 pp. 210-218 available online at www.csjournalss.com

Video Based Face Detection and Tracking for Forensic Applications

Ritika Lohiya, Pooja Shah
Assistant professor at Silver Oak College of engineering and technology, Assistant Professor at Nirma University ritikalohiya.ce@socet.edu.in, pooja.shah@nirmauni.ac.in

Abstract: Today in the emerging era of technology where every other day a new software or tool is born to tackle the wide field of computer science, gives rise to the need of its security, as in day to day life, crime is becoming a big issue so to avoid and to protect from crime computer forensics is needed. Digital forensics is a branch of forensic science dealing with investigating, collecting, analysing and reporting on some digital information. It is used in the detection and prevention of crime and in any dispute where evidence is stored digitally. This paper discusses about forensic science investigation and different tools and practices in it.
Index Terms: science investigation, digital forensics.

I. INTRODUCTION

Forensic Science is the process of scientifically gathering and examining the information about the past. Forensic Science in itself is the widespread domain consisting of many types of forensic analysis in different fields such as Digital forensics including the forensic analysis of the data in digital form , Network forensics including the forensic analysis of the data and the devices in the network, Cyber forensics including forensics analysis of the computer related and computer generated crimes, Enterprise forensics including the forensic analysis of the computer tools, Mobile forensics including the forensics analysis of the mobile devices and mobile data etc.. In this paper my main focus would be in Digital forensics. Digital forensics is the branch of forensic science that involves the application of scientific methods to the investigations of the artifacts present in one or more digital devices or digital data. Digital forensics is the multi staged process involving the acquiring of data, examine the facts and features, analyzing the acquired data and documenting it for the future use. It has emerged as an independent field due to the increasing rate computer based crimes and internet. In early days, it was referred to has computer forensics since the evidence collected were related to the computer only, but now this is not the scenario. With the extensive use of the internet today, the doors for the computer related crimes have also increased to a great extent and so to refer to this widespread domain it is generalized to Digital forensics.

The Digital Forensic Research Workshop (DFRWS) Technical committee [3] has defined *digital forensic science* as below:

"*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.*"

One of the major applications of Forensic Science which adds an advantage to its processing is evidence collection is Biometrics. Biometrics which is used for the process of authentication, privacy and security for verifying the person that the user who is requesting a resource is who he/she claims to be. Biometrics uses many means for this purpose it may be fingerprint matching, irisrecognition, DNA matching or face recognition etc. Biometrics systems mainly utilizes the property of the human itself for verification and identification for instance structure of the finger prints are used for veri_cation of an individual, structure of the DNA are matched for the identification etc. By comparing the existing data with available data recognition process could be carried out. Biometric systems are mainly used for the security reasons. For example law enforcement firms use these systems for evidence collection. We have automated finger prints matching system which keeps the track of the finger prints of the criminals which can be used as evidence against them in the court of law. Also now trending is the face recognition system which matches the features of the face stored in the database to the available ones. The main advantage of going for face recognition is that for other biometric system analysis like finger print and iris matching requires the human participation that is the individual has to be present in personnel for the verification and identification process. Whereas in face recognition no human participation is necessary as mainly the for identification process digital image or video is available from the crime scene and on the basis of that evidence can be collected. And therefore the urge of automated system for face recognition is more in demand. Facial recognition holds several advantages over other biometric techniques. It is natural, non-intrusive and easy to use. In a study considering the compatibility of six biometric techniques (face, finger, hand, voice, eye, signature) with machine readable travel documents (MRTD) [2] facial features scored the highest

percentage of compatibility, see Figure 1 In this study parameters like the enrollment, renewal, machine requirements and public perception wereconsidered.

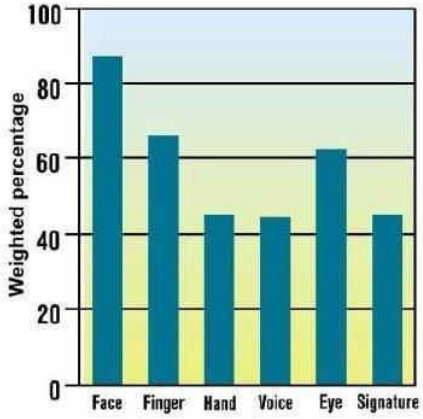

Figure 1: Comparison of machine readable travel documents (MRTD) compatibility with six biometric techniques; face, finger, hand, voice, eye, signature. Courtesy of Hietmeyer[2]

II. TRENDS IN FORENSIC SCIENCE

The role of forensic science is changing with emerging trends in technology. New insights, increasing knowledge in customers, combined with falling costs results in rapid growth of the sector. Today's investigation can extract minute details from the samples in matter of seconds. Forensic science has opened completely new category of investigation as the specialists dig the holes and collect evidences from mobile phones , computers, laptops etc and the evidences collected can be anything from the invisible finger print to the large data set stored in the computer or any digital device. In addition this details can now be produced more quickly then ever thought possible. Due to these developments, rapid and well founded reconstructions of events based on trace patterns found at crime scene are becoming tantalizing possibility. One of the important and the clearest trends in the forensic science sector is its rapid growth over the years. And the major factors driving this growth includes (1) New technology (2) Increased general awareness (3) And emerging newcustomers.

A. New Technology

Technological advancements in any field plays a major role in changing the perspective of the knowledge in the field. In the field of forensics new advancements like pattern recognition, object extraction, trace evidence, image enhancement, image compression, image restoration etc have significantly changed the face of digital forensics. Today, it is almost impossible to prevent leaving digital traces - in cell phones, computers, internet, in surveillance camera and so on. People have a symbiotic relationship with both the physical and the virtual world. And this is only because everything we do leaves a trace in these worlds.

B. Increased General Awareness

The increased growth of forensics is not only due to the new technologies but also due to the increased awareness of what forensics is all about. Existing and potential users are all aware about the extent of forensic capabilities. The awareness of the new technologies and their advancements through the public sector plays a major role. Increasing cyber-crime cases and their proceedings and the results help people know about the surroundings and how the digital medium is used to process the crime. And because of all these factors contributing together, users become more aware of the benefits of the new tools and expertise available and see new ways to use the forensic science.

C. New Customers

Forensic investigation is not only useful for the criminal justice and law enforcement but in fact, a wide range of government organizations involved in everything from defence and intelligence to administrative law and regulatory are using forensic science with a different perspective. This has increased the fragmentation of the forensic sector as a whole.

Thus these are the major trends in the digital forensic science. In the next section we will discuss some of the major challenges in digital forensics.

III. RELATED WORK

We can describe the basic tasks of video analysis as automated extraction, processing, and structuring of essential information from images and image sequences obtained in the real world. These tasks are performed by video analysis algorithms, which define the way computers can see the world. The collection of such algorithms forms the field of computer vision, which is defined by Haralick and Shapiro as science that develops the theoretical and algorithmic basisby which useful information about the world can be automatically extracted and analyzed from an observed image set, or image sequence from computations made by special-purpose or general-purpose computers (Haralick & Shapiro, 1993). In the last decade, computer vision research produced complex, fast, and accurate video analysis algorithms. Such characteristics as complex, fast, and accu- rate are relative to the specific tasks, previous approaches, or our expectations. Todays algorithms are complex in a sense that they are useful in many practical operations of detection, identification, and tracking of objects and events. Algorithms speed is acceptable and is often real-time for conventional video sizes due to the latest advances in computing speed and optimizations in algorithms computations. The improvement in accuracy was inuenced by many openly available datasets containing large collections of practical video and image data for testing of video analysis algorithms. Regularly organized competitions and challenges also motivate further growth of algorithms performance. Therefore, with the latest increases in e_ciency and reliability of video analysis algorithms, it is reasonable to say that computer vision is not only enhancing but is replacing human vision in many practical applications. The number of applications that rely or incorporate video analysis as a part of their core functionality is constantly growing. Traditionally, such applications include security-based applications suchas video surveillance, visual biometric, and personal identification. In recent years, other types of video analysis-based application have emerged. Autonomous vehicles and unmanned aircrafts are good examples of such systems. Social applications such as social networks and photo sharing services started integrating face detection and recognition into their services. Many brands of hand held-photo and video cameras, as well as camera phones also include, at least, a face detection algorithm. Video analysis algorithms are also becoming an important integral part of video conferencing systems, systems for intelligent homes, care and nursery systems that watch over elderly and disabled people, and so on. New generation of video surveillance is one of the most prominent applications relying on video analysis algorithms. The research goal for such systems is to relieve human guard from the constant monitoring task of the surveillance site. Specifically, the aim is to alert the human guard only in situations when an action or a human intervention is required, for instance if video analysis algorithms detect and identify a suspicious person, object or event. According to Wu et al., suspicious events are rare in typical surveillance environment (Wu, Jiao, Wu, Chang, & Wang, 2003b), which makes the goal feasible and achievable, subject to acceptable accuracy and efficiency of video analysis. The recent availability of fast computers, cheap video sensors, and advances in network technology brought the research in surveillance systems closer to this goal. But not only that, it also greatly expanded the range of surveillance applications from being used mainly for conventional monitoring of government or military facilities to an essential part of traffic control systems and integral part of intelligent homes. These advances made video surveillance a commodity easily available to general public.

IV. ALGORITHMS FOR FACE DETECTION AND TRACKING

Face Detection and tracking are important in many computer vision and applications like face recognition, automotive safety or surveillance.

A. CAMShift Algorithm

Detect a face

The cascade object detector uses the Viola-Jones detection algorithm and a trained classification model for detection. By default, the detector is configured to detect faces, but it can be configured for other object types.

Identify Facial feature to track

Once the face is located in the video, the next step is to identify a feature that will help you track the face. Here, skin tone is used as the feature to track. As it provides a good contrast between face and the background.

Track the face

With the skin tone selected as the feature to track, Histogram Based Tracker is used for tracking. It provides the capability to track an object using a histogram of pixel values.

B. Kanade-Lucas-Tomasi Tracker Algorithm

The point tracker object tracks a set of points using the Kanade-Lucas-Tomasi (KLT), feature-tracking algorithm. The KLT algorithm tracks a set of feature points across the video frames.

Once the detection locates the face, it then identifies feature points that can be reliably tracked. With the feature points identified, you can now use the Point Tracker object to track them.

For each point in the previous frame, the point tracker attempts to find the corresponding point in the current

frame.

Implementation Results

The table 1 contains the types of videos used with their description and characteristics. Also the next table 2 gives the implementation details of the experiments with the total number of videos used in the experiments and the number of times the face detected by the two algorithms.

Dataset	Characteristics	Description
Person facing the camera	video, 320 × 240, 25fps, 488 kbps bitrate	a person moving in front of the camera and facing the camera and talking.
Person talking on a news channel	video, 320 × 240, 25fps, 488 kbps bitrate	a person continuously talking on a news channel.
Person Driving a car	video, 320 × 240, 25fps, 853 kbps bitrate	a person driving a car, facing side.
Person giving speech to the audience	video, 320 × 240, 25fps, 700 kbps bitrate	person giving speech facing the audience at various angles.
Person singing song	video, 240 × 180, 25fps, 650 kbps bitrate	high illumination video with a person singing song on guitar.
Person singing song	video, 320 × 240, 25fps, 650 kbps bitrate	video of a person sining during night.
Two people on a news channel interacting with each other	video, 320 × 240, 25fps, 650 kbps bitrate	video on a news channel of two people communicating.
Interviewing two people	video, 320 × 240, 25fps, 650 kbps bitrate	interview of two people having a poster behind with two persons.

Criteria	Total no. of videos	CAMShift	KLT
Frontal face	250	230	240
Pose Variation	250	200	210
Multi face tracking	250	180	210
Illumination	250	160	180

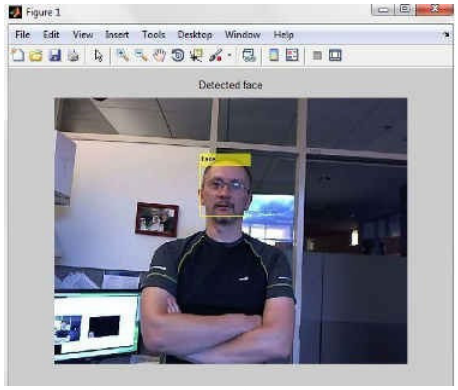

Figure 2: Frontal Face Detection CAMShift

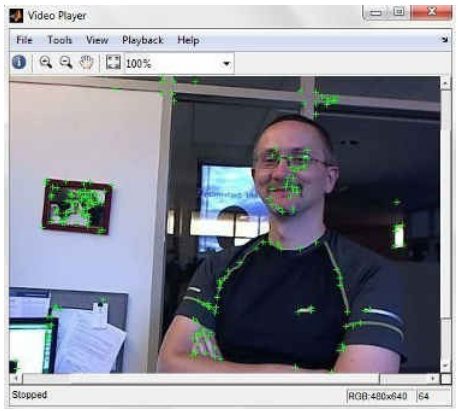

Figure 3: Frontal Face Detection KLT

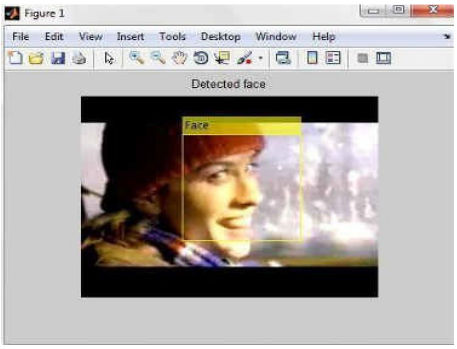

Figure 4: Pose Variation Face Detection CAMShift

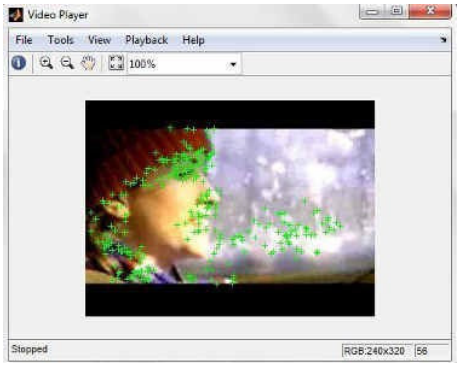

Figure 5: Pose Variation Face Detection KLT

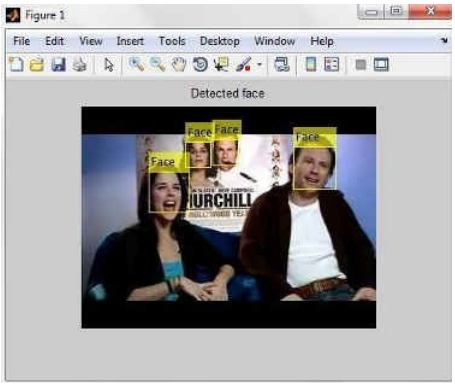

Figure 6: Multiple Face Detection CAMShift

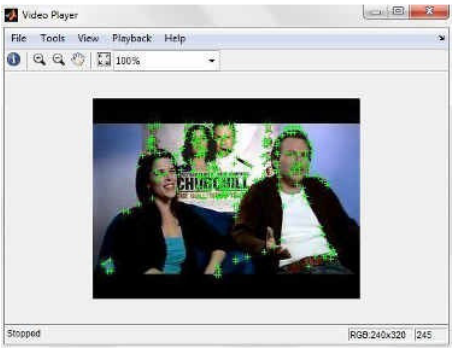

Figure 7: Multiple Face Detection KLT

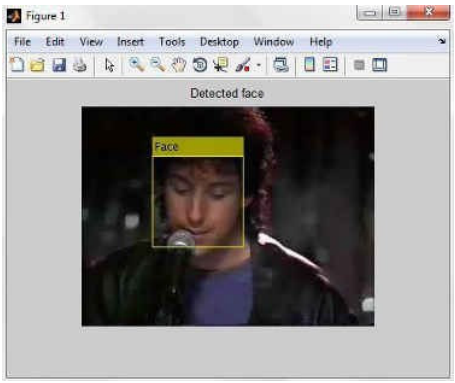

Figure 8: Illumination Face Detection CAMShift

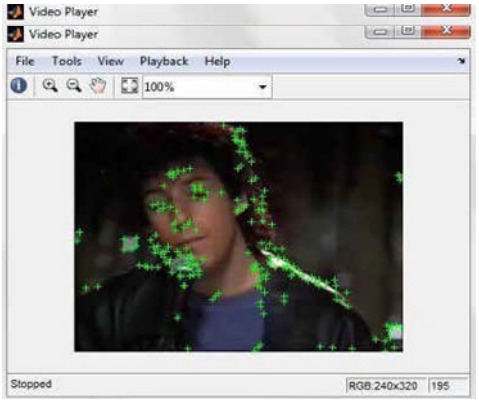

Figure 9: Illumination Face Detection KLT

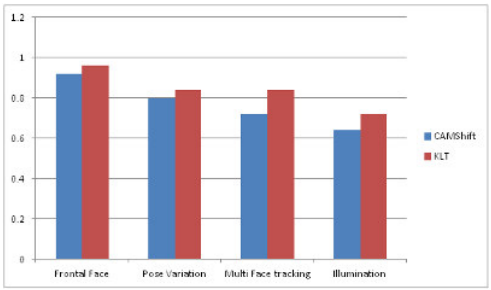

Figure 10: Accuracy Results

V. PROPOSED WORK

The figure below shows the proposed architecture for video based face detection and tracking.

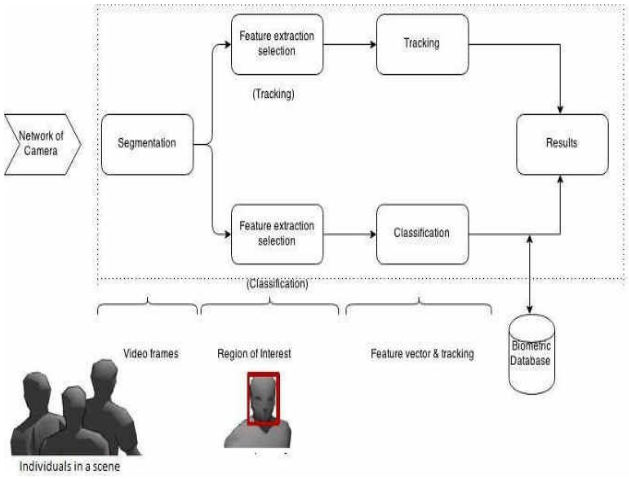

Figure 11: Proposed Architecture Here segmentation is done and then features are extracted using KLT.

Segmentation: Image segmentation is the division of an image into regions or categories, which correspond to different objects or parts of objects. Every pixel in an image is allocated to one of a number of these categories. A good segmentation is typically one in which: pixels in the same category have similar greyscale of multivariate values and form a connected region, neighbouring pixels which are in different categories have dissimilar values.
Segmentation is often the critical step in image analysis: the point at which we move from considering each pixel as a unit of observation to working with objects (or parts of objects) in the image, composed of many pixels. If segmentation is done well then all other stages in image analysis are made simpler. Here region-based segmentation is performed which operate iteratively by grouping together pixels which are neighbours and have similar values and splitting groups of pixels which are dissimilar in value.

Feature Extraction and Tracking: The point tracker object tracks a set of points using the Kanade-Lucas-Tomasi (KLT), feature-tracking algorithm. The point tracker object is used for video stabilization, camera motion estimation, and object tracking. It works particularly well for tracking objects that do not change shape and for those that exhibit visual texture. The point tracker is often used for short-term tracking as part of a larger tracking framework. As the point tracker algorithm progresses over time, points can be lost due to lighting variation, out of plane rotation, or articulated motion. To track an object over a long period of time, you may need to reacquire points periodically. For initializing the tracking process, the initialize method is used to specify the initial locations of the points and the initial video frame.

Implementation Results:

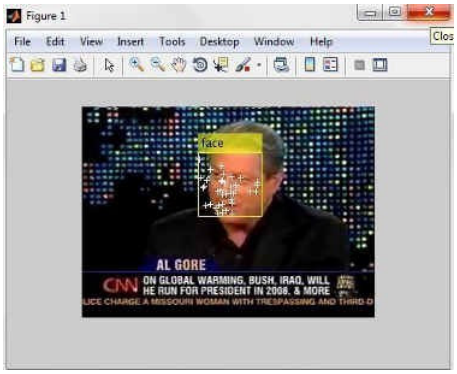

Figure 12: Frontal Face Detection

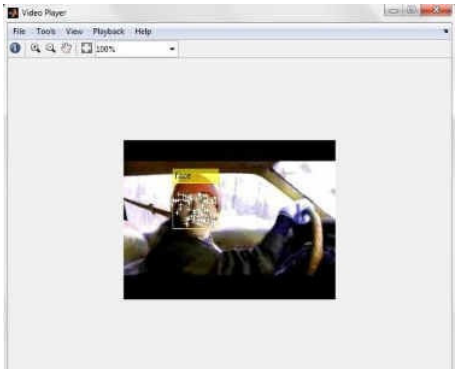

Figure 13: Pose variation Face Detection

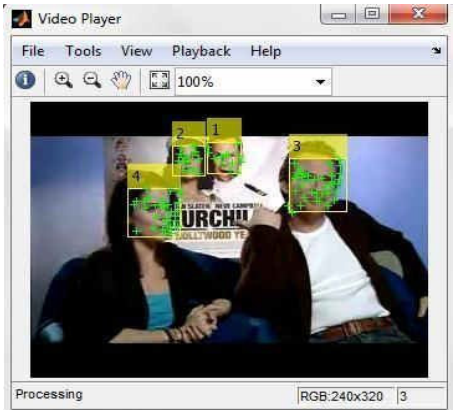

Figure 14: Multiple Face Detection

VI. CONCLUSION

The new approach presented, where object segmentation is performed, to identify the region of interests i.e face in the videos outperforms with the given dataset. Also Cascade object detector is incorporated into the face detection algorithm which allows the algorithm to update the expected position of the detected faces in the next frame. This continuity between the videos frames was not exploited by the CAMShift and KLT algorithms. Thus, in contrast to CAMShift algorithm and also to the Kanade-Lucas-Tomasi tracker, the proposed face tracker preserves information about the near positive and gives better results.

Forensic science is clearly a very important sector in the world. New advances in technology have placed forensics in an accelerating cycly of growth, as wider range of sectors are now using forensics for there own puposes. But nonetheless each technology brings with it, its own challenges. This paper has reviewed the trends in forensic science and the factors contributing towards it. It also consists of the challenges which the forensic science faces today. The last section reviews the practices and tools used for forensic science investigation. The new advancements, tools, and techniques leads to the wider future scope for forensic science investigation.

REFERENCES

[1] Dr.A.S.N.Chakravarthy, T.V.Sarath Kumar "Survey on Computer Crime Scene Investigation Forensic Tools" *International Journal of Computer Trends and Technology- volume3Issue2- 2012*

[2] Sriram Raghavan. "Digital forensic research: current state of the art" CSIT (March 2013) 1(1):91–114

[3] DFRWS Technical Committee (DFRWS) (2001) A road map for digital forensic research: DFRWS Technical Report. DTRT001-01 FINAL

[4] McKemmish R (1999) What is forensic computing? Trends and issues in crime and justice, vol 188. Australian Institute of Criminology, Canberra, pp 1–6. ISBN 0-642-24102-3

[5] Computer Security Institute (2010/11) Computer crime and security survey. In: 15th Annual Computer Crime survey (2010, GoCSI).https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf. Accessed 8 Oct 2012.

[6] Eugene Liscio, P. Eng,"Open Source Tools for 3D Forensic Reconstructions," AI2-3D Forensics https://www.ai2- 3d.com

[7] Simson L. Garfinkel, "Digital forensics research: The next 10 years" ScienceDirect.

[8] Pankaj Gupta, Jaspal Singh, Anterpreet Kaur Arora, Shashi Mahajan, "Digital Forensics- A Technological Revolution in Forensic" J Indian Acad Forensic Med. April-June 2011, Vol. 33, No. 2

[9] Seaskate. A Technical Report prepared for The National Committee on Criminal Justice Technology, National Institute of Justice, By Seaskate, Inc.July-1998.