ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

Criminal Detection in Cyber Forensic Using Face Recognition with Automatic Alert Sharing System

[1]S.Gopi BTech,ME., [2]Santhosh kumar .M., [3] Aswin.S, [4]Vignesh.R
[1] Assistant Professor Department of Information Technology, Muthayammal Engineering College (Autonomous), Rasipuram - 637 408, Tamil Nadu, India
[2] [3] [4] Student Department of Information Technology, Muthayammal Engineering College (Autonomous), Rasipuram - 637 408, Tamil Nadu, India

Abstract: ***Face recognition is an interesting and challenging problem and impacts important applications in authentication and personal identification among others. Extraction of these important elements from a picture, their useable representation, and classifications are the core concepts of automatic face recognition. Face recognition based on the geometric features of a face is probably the most instinctive approach for Human identification. The entire process may be broken down into three main parts, with the first step being the search for a reliable database of faces that includes numerous photographs for each person. The next phase is to find faces in the database photos so that the face recognizer can be trained on them. The last step is to test the face recognizer to see if it can still find the faces that it was trained on. Here implement an application for criminal detection, it helps forensic department for the accurate identification of criminal using his face image. The training face images are initially collected and stored on server. This system provides essential security to apartments and other control applications. During face capturing the face image will be match with registered images. An efficient classifier uses to classify the face images accurately. Criminal images are collected and stored by forensic department. During capturing process, face image will be classified with the criminal image database. If a match is made, we will be able to identify the offender and quickly make an arrest.***

I. INTRODUCTION

Network security contains policies and practices adopted to hinder and screen unauthorized entry, misuse, modification, or denial of a pc community and community-accessible assets. Network security involves the authorization of access to information in a network, which is managed with the aid of the community administrator. Customers decide upon or are assigned an identification and password or other authenticating information that allows for them access to expertise and packages within their authority. Community safety covers a type of pc networks, each public and personal, which can be used in day-to-day jobs; conducting transactions and communications amongst organizations, government organizations and participants. Networks can be personal, equivalent to inside a enterprise, and others which might be open to public access. Network security is concerned in corporations, organizations and other forms of associations. It does as its title explains: It secures the community, as good as defending and overseeing operations being achieved. Probably the most fashioned and easy means of defending a community resource is by means of assigning it a precise title and a corresponding password. Network security starts with authenticating, usually with a username and a password. Due to the fact that this requires just one element authenticating the person title—i.e., the password—this is generally termed one-element authentication. With two-factor authentication, anything the consumer 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile) and with three-component authentication, whatever the user 'is' can be used (e.g., a fingerprint or retinal scan). As soon as authenticated, a firewall enforces entry policies similar to what services are allowed to be accessed by way of the network customers. Newer methods combining unsupervised laptop finding out with full community traffic analysis can discover lively community attackers from malicious insiders or detailed 3 external attackers which have compromised a person desktop or account. Verbal exchange between two hosts making use of a community may be encrypted to maintain privateness. Honeypot, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, because the honeypot will not be most often accessed for respectable functions. Techniques utilized by the attackers that attempt to compromise these decoy resources are studied for the duration of and after an assault to preserve a watch on new exploitation strategies. Such analysis may be used to additional tighten protection of the genuine community being protected via the honeypot. A honeypot may also direct an attacker's concentration far from authentic servers. A honeypot encourages attackers to spend their time and vigor on the decoy server while distracting their concentration from the info on the actual server. Much like a honeypot, a honeynet is a community established with intentional vulnerabilities. Its intent can also be to ask assaults so that the attacker's approaches will also be studied and that know-how can be utilized to broaden community protection. A honeynet mostly includes a number of honeypot.

II. TYPES OF ATTACKS

Networks are field to attacks from malicious sources. Attacks will also be from two classes: "Passive" when a network intruder intercepts data travelling via the network, and "active" where an outsider initiates commands to disrupt the network's usual operation or to behavior reconnaissance and lateral action to seek out and achieve access to belongings available through the network.

The security threat to the network can be the attacker who attempts to grasp information to exploit the network vulnerability. This kind of attack is also known as passive attack. On the other hand, the attacker is attempting to disrupt the network communication and also affect the user productivity of a network. It is also known as an active attack. Here listed below are some of the most common types of the security threats.

DoS

The DOS- denial of service attack overwhelms the network host with the stream of bogus data which keep it to process the designed data. The DoS attacks will be launched against the computers and against the network devices. The DoS attack is the security threat which implies that the larger attacks are in progress. Then the DoS attack is a part of the attack that the hijacks communication from the user who already authenticated to the resource.

DDoS

The distributed denial of service is the attack occurs when the multiple system is used to flood the resources or bandwidth of a group of servers or one server. The main purpose of this attack is to saturate a resource so that it is not available longer for the legitimate use. It is used as the decoy to hide more malicious attack which attempts to steal sensitive information or other data. The specialized software called DDS can able to block the traffic that has a legitimate content but the bad intent.

Man in the middle

The man in the middle attack occurs when the person keep a logical connection or equipment between 2 communicating parties. These 2 communicating parties assume they are directly communicating with each other, but the information is being sent to a man in the middle who forwards it to the proposed recipient. This attack is very harmful to the organizations. Most of the organizations will adopt measures such as strong authentication as well as latest protocols, including IPSec/L2TP with the tunnel endpoint authentications.

Social Engineering

A social engineering attacks are not relying on technology or protocols to succeed, but instead it relies on the human nature. Users generally trust each other and where the this type of attacks start. It may comprise of false sites that ask for the information from the unsuspecting web surfers. And this type of attack is known as phishing. A social engineering attacks might be prevented by just training the users not to provide their credentials who asks for the information on the web page.

Virus

The computer virus is the program which can infect the computer and copy itself without user knowledge. These viruses started infecting the computers in 1980 itself and also continued to evolve till date. Some of the viruses are able to change after it infects the computers to try to hide from the antivirus software. As the viruses changed over the years and years, companies like McAfee and Symantec have specialized in the software, which can eradicate and detect viruses from the computer system. There are nearly more than 76,000 known viruses and users can eradicate it by updating the antivirus software up to date on all the clients and servers.

Worms

The worm is the something different from the viruses, it is just a program and just not an infestation. These worms will use a computer network to send worm copies to the other computers without the user's knowledge. They are proposed to cause network problem such as resource utilization and bandwidth issues. The most famous worms such as sobig and mydoom worms have affected more thousands of servers and computers in the past.

Buffer Overflow

The buffer overflow is the attack created anomaly by the rogue program when writing data to the buffer intentionally overwrite the buffer memories and the adjacent memory. It may result in memory errors and erratic behavior and a crash or breach of the system security. Make use of the products like ProPolice and Stackguard to prevent the buffer overflow attack from succeeding.

Packet Sniffing

The attacker can use the protocol analyzer to launch the attack by the packet sniffing. This is the process in which an attacker gathers the data sample with a software or hardware device which allows data inspection at a packet level. The attacker may see the IP addresses, unencrypted passwords, sensitive data and MAC addresses. After vulnerability is discovered, the attacker will begin an active attack.

VIDEO SURVEILLANCE SYSTEM

Video Surveillance is one of the active research topics in Image Processing. Video Surveillance started with analogue CCTV systems, to gather information and to monitor people, events and activities. Existing digital video surveillance systems provide the infrastructure only to capture, store and distribute video, while leaving the task of threat detection exclusively to human operators. Video surveillance cameras are used in shopping centres, public places, banking institutions, companies, and home security and ATM machines. Nowadays, researches experience continuous growth in network surveillance. Video surveillance systems have wide range of applications like traffic monitoring and human activity understanding. In video surveillance system we demonstrate a system which analyses activity in the monitored space in real time, and makes the events available for generating real time alerts and content based searching in real time. There are also works which handles pose variations implicitly without estimating the pose explicitly.

VIDEO PROCESSING

Video signal is basically any sequence of time varying images. A still image is a spatial distribution of intensities that remain constant with time, whereas a time varying image has a spatial intensity distribution that varies with time. Video signal is treated as a series of images called frames. The demand for digital video is increasing in areas such as video teleconferencing, multimedia authoring systems, education, and video-on-demand systems.

FRAME TYPES

Three types of video frames are I-frame, P-frame and B-frame. 'I' stands for Intra coded frame, 'P' stands for Predictive frame and 'B' stands for Bidirectional predictive frame. 'I' frames are encoded without any motion compensation and are used as a reference for future predicted 'P' and 'B' type frames. 'I' frames however require a relatively large number of bits for encoding.

III. PROPOSED SYSTEM

Face detection is the first stage of a face recognition system. A lot of research has been done in this area, most of which is efficient and effective for still images only & could not be applied to video sequences directly. Face recognition in videos is an active topic in the field of image processing, computer vision and biometrics over many years. Compared with still face recognition videos contain more abundant information than a single image so video contain spatio-temporal information. To improve the accuracy of face recognition in videos to get more robust and stable recognition can be achieved by fusing information of multi frames and temporal information and multi poses of faces in videos make it possible to explore shape information of face and combined into the framework of face recognition.

In proposed system develop a system that can be used by police or investigation department to recognize criminal from their faces. The face detection algorithm looks for specific Haar features. When one of these features is found, the algorithm allows the face candidate to pass to the next stage of detection. The features are classified with dataset using cascade features. It is further compared with the images stored in database to identify if the person is criminal/suspect. If he is criminal/suspect the time for which he was under the surveillance of the camera is noted and provide notification.

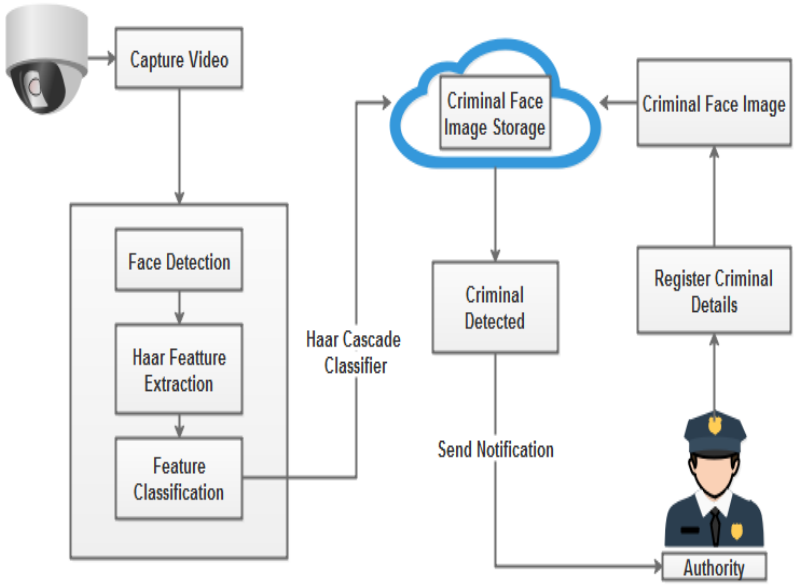
ADVANTAGES

- The method of face recognition used is fast, robust, reasonably simple and accurate with a relatively simple and easy to understand algorithms and technique.
- This method works very efficiently because face image of a person will not change.
- The proposed system can successfully recognize more than one face which is useful for quickly searching suspected persons as the computation time is very low.

SYSTEM ARCHITECTURE

Criminal detection using face recognition in a surveillance system involves employing a Haar Cascade Classifier-based approach for efficient and real-time identification of individuals.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024



System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes.

A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. System architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components.

MODULES

- Criminal Image Storage
- Face Image Acquisition
- Feature Extraction
- Criminal Detection
- Alert System

MODULES DESCRIPTION

CRIMINAL IMAGE STORAGE

Face registration is the process of transforming different sets of data into one coordinate system. Facial features are stored with labels. Image registration or image alignment algorithms can be classified into intensity-based and feature-based. Face recognition systems identify people by their face images. Feature-based methods establish a correspondence between a numbers of especially distinct points in images. Knowing the correspondence between a numbers of points in images, a geometrical Face image registration is the process of transforming different sets of data into one coordinate system.

FACE IMAGE ACQUISITION

A digital video surveillance system is a surveillance system capable of capturing images and videos that can be compressed, stored or sent over communication networks. Digital video surveillance systems can be used for nearly any environment. A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a face database In proposed work, the face image which is captured by web camera.

FEATURE EXTRACTION

Applying human visual property in the recognition of faces, people can identify face from very far distance, even the details are vague. That means the symmetry characteristic is enough to be recognized. Human face is made up of eyes, nose, mouth and chin etc. There are differences in shape, size and structure of those organs, so the faces are differ in thousands ways, and we can describe them with the shape and structure of the organs so as to recognize them.The face detection algorithm looks for specific Haar features and not pixels of a human face. A face candidate is a rectangular section of the original image which is called as a sub-window.

CRIMINAL DETECTION

Face classification is the process of predicting the fake users and criminals. During face verification user face image is capturing through real time camera. Then the facial features are extracted and matched with database. Face classification also used for predicting criminals. Criminals face images are already collected and stored on database. If captured image match with criminal database that will analyse and predict criminals easily. The cascade classifier contains a list of stages, where each stage consists of a list of weak learners. The system detects the required object by moving a window over the image.Each stage of the classifier labels the specific region defined by the current location of the window as either positive or negative where positive means that an object was found and negative means that the specified object was not found in the image.

ALERT SYSTEM

The automatic detection of abnormal activities can be used to alert the related authority of potential criminal or dangerous behaviors, such as automatic reporting of a person. In proposed system unknown event alert send to the predefined contact numbers regarding particular officers. Here also implement image sharing for easy identification of criminals.

CONCLUSION

Smart security surveillance for forensic department system has been successfully designed and implemented which is capable of recording the videos and capturing the images and the same has been uploading to server. At the same time SMS notifications and Gmail notifications with captured snapshots will send to user. Live video streaming also provided to monitor continuously. It is advantageous as it offers reliability and privacy on both sides. By using this system we can easily identify the unknown person easily.

FUTURE ENHANCEMENT

As the future scope of this system can be extended further by adding additional IoT features to detect the people face if they wore the mask on his/her face.And alsoimplement various algorithms to provide still to video face matching with improved accuracy rate.

REFERENCES

[1] Kwan-Loo, Kevin B., José C. Ortíz-Bayliss, Santiago E. Conant-Pablos, Hugo Terashima- Marín, and P. Rad. "Detection of violent behavior using neural networks and pose estimation." IEEE Access 10 (2022): 86339-86352.
[2] Adil, Muhammad, Saqib Mamoon, Ali Zakir, Muhammad Arslan Manzoor, and Zhichao Lian. "Multi scale-adaptive super-resolution person re-identification using GAN." Ieee Access 8 (2020): 177351-177362.
[3] Alansari, Mohamad, Oussama Abdul Hay, Sajid Javed, Abdulhaid Shoufan, Yahya Zweiri, and Naoufel Werghi. "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations." IEEE Access (2023).
[4] Deng, Jiankang, Jia Guo, Evangelos Ververas, Irene Kotsia, and Stefanos Zafeiriou. "Retinaface: Single-shot multi-level face localisation in the wild." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 5203-5212. 2020.
[5] Deng, Jiankang, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. "Arcface: Additive angular margin loss for deep face recognition." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 4690-4699. 2019.
[6] Zhu, Yanjia, Hongxiang Cai, Shuhan Zhang, Chenhao Wang, and Yichao Xiong. "Tinaface: Strong but simple baseline for face detection." arXiv preprint arXiv:2011.13183 (2020).
[7] Feng, Yao, Fan Wu, Xiaohu Shao, Yanfeng Wang, and Xi Zhou. "Joint 3d face reconstruction and dense alignment with position map regression network." In Proceedings of the European conference on computer vision (ECCV), pp. 534-551. 2018.
[8] Ferrari, Claudio, Stefano Berretti, and Alberrto Del Bimbo. "Extended youtube faces: a dataset for heterogeneous open-set face identification." In 2018 24th International Conference on Pattern Recognition (ICPR), pp. 3408-3413.IEEE, 2018.
[9] Lin, Yiming, Shiyang Cheng, Jie Shen, and Maja Pantic. "Mobiface: A novel dataset for mobile face tracking in the wild." In 2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019), pp. 1-8.IEEE, 2019.
[10] Wang, Hao, Yitong Wang, Zheng Zhou, Xing Ji, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu. "Cosface: Large margin cosine loss for deep face recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5265- 5274. 2018.