Implementation of Automated Criminal Face Detection System Using Facial Recognition Approach

V. Jebasheeli[1], R. Vadivel[2*]

[1]Department of Information Technology, Bharathiar University, Tamil Nadu India
[2]Department of Information Technology, Bharathiar University, India

Corresponding Author: vlr_vadivel@yahoo.co.in

Abstract— Criminal records usually contain personal information about a particular person and image. To identify any criminal, require an identity document in person, provided by eyewitnesses. In many cases the quality and resolution of parts of the recorded images is poor and difficult to detect. Identification can be done in many ways such as finger print, eyes, DNA etc. One of the programs is facial recognition. Although the ability to use intelligence or character in suspicious facial expressions, one's ability to recognize faces is amazing. Criminal records usually contain personal information about a particular person and image. The identification of any criminal requires specific identification in relation to a particular person or persons, provided by eyewitnesses. Based on the information provided by eyewitnesses, this investigation will be conducted. In many cases the quality and resolution of parts of the recorded images is poor and difficult to detect. In this paper, it is divided into the performance of graphical images in three stages; low, medium and high level to process and analyze a given face. This paper demonstrates better results than the conventional methods associated with the face recognition process used in crime detection.

Keywords— Biometrics, Face recognition, Digitization, Preprocessing, Restoration, Compression

I. INTRODUCTION

The motivation of this paper is to implement an automated criminal face detection system using facial recognition approach. The project, entitled "Criminal Face Detection System" is intended to identify criminals in any department investigating. Here is the process that it is already saved some of the images of the criminals in the database and its details and that the photos have been divided into many pieces namely eyes, hair, lips, nose, etc. These images are then stored in another data recorder so that any criminal eyewitness will see images or threads that appear on the screen by using them to enhance the face, which may or may not match the images [1]. When any image is compared up to 99% predict that person as criminal. Thus implementing this project provides a very user friendly environment for both operators and eyewitnesses of any face can easily identify criminals [2]. The project is aimed at identifying criminals with the help of eyewitnesses. There are four modules in the project. Adding, Removing, Updating, and Identifying Criminals There are three roles especially in the project. The administrator is responsible for providing user ids and passwords. Management provides authentication to users. Administration creates deletion and Updates user ids and passwords. The supplier, which is under the investigating department, is responsible for entering the criminal information and maintaining it. User adds, removes and updates criminal information. The agency has also created a criminal face with the help of

eyewitnesses. An eyewitness identifies criminals with the help of plant parts stored in a separate database by the employee. Eyewitnesses select the target segment from the database and that composite segment will be delivered by the operator in this way, the full face of the criminal is created and details of the criminal are available in the database. User can also create a new image for those plant parts that user consider as the face imagined by a criminal.

II. RELATED WORK

Biometric technology [3] has been introduced as a viable solution for performing safe and personalized detection. The need for more secure identification and personal authentication technologies is evident as the level of security breaches and transaction fraud increases [4]. The increasing use of biometric technologies in higher and higher security applications has created the need for more reliable face detection systems. The Face Recognition system is used to verify one's identity by comparing a given face to an objection to a known face information database [5]. User have evolved into another way to discover traditional art and authentication methods such as using keys, identity cards and passwords. Face recognition involves the computer visualization of user identity based on geometric or mathematical symbols taken from facial images [6]. Although people recognize and point faces at the scene with ease, building an automated system is a challenge. Surveillance technology can be used in a variety

of application environments including control of access to PCs, airport surveillance, private surveillance, criminal crime monitoring system moving into the next generation of environments where computers are designed to interact more with people. In recent years, significant progress has been made in the area of facial recognition with the development of many other useful techniques [7]. Advances in computer technology have facilitated the development of real-time visual communication modules in recent years. Examples are common, especially in biological models and human computer communication as the information contained on the surface needs to be analyzed in order for systems to respond appropriately [8]. For biometric systems that use the face as separate input modules, it is important to find faces in the scene before any algorithm is installed. A user's perspective based on a smart idea should be able to tell the user's focus (e.g. where the user is looking) in order to respond appropriately. To obtain facial features directly through applications such as digital cosmetics, face needs to be identified and pre-registered for further processing [9]. Face detection is tied to detecting whether or not the face of a given image (usually on a gray scale) and, if available, replace the image and content of each face. This is the first step of any automated system that analyzes information contained on the face (e.g. identity, gender, appearance, age, race and pose) [10]. This work focuses on how to make the same input by dividing the image into manageable and logical components to calculate the correct results [11].

A. Existing System
Criminal records usually contain personal information about a particular person and image. The identification of any criminal requires an identity document in relation to a person, provided by eyewitnesses [12]. Depending on the information provided by eyewitnesses, the criminal who committed the crime will be identified.

B. Problems with the existing system
- Often the quality and resolution of the recorded images is unhealthy and difficult to detect.
- If eyewitnesses see a criminal from one location, they may not be able to see him.
- An image, which is a hard copy, cannot separate or divide into different modules. So it's very difficult to find.
- Sometimes the eyewitness may not be able to draw the face of a criminal.
- Sometimes, when User keep criminal information on hand and in the body. After a while, photos and other details can usually be deleted..

III. METHODOLOGY

Knowing that User have a criminal database in the records, it would be an easy task to gather information about a person who has a criminal record and is a suspect in this particular case. Now seeing the situation will be an eye-witness to be able to trace the alleged image and make sure

that the paint made by him is the same as the face seen in this particular crime. Now, to compare faces with an existing database, first, User need to divide the face into six equal parts such as hair, head, eyes, nose, mouth and chin. Separating the data can be an easy task for facial recognition. In most cases it will be seen while looking at the classification of images. A particular image is divided into six sections such as hair, forehead, eye, nose, mouth and beard. Figure 1 explains the flow of data [13].

A. Algorithm for Proposed Classification
Step 1: Divide the image into six equal sections of hair, forehead, eye, nose, mouth and beard.
Step 2: Now the face is divided into individual parts, which is an easy way to create a new face and match the criminal with the database.
Step 3: Use each of these components to create a new face as an eyewitness.
Step 4: Compare all the face separators with the available database. It can generate a list of compatible responses from database i.e. they can be more than one.
Step 5: Implement a comparison process to match the complete image with images that have some similarities so that User can find the most relevant suspect from the database available among all suspects.
Step 6: So with the match comparisons made to all parts of the image against the background data images, User come to a specific image showing the complete game. So, comes the picture of a complete game of a suspected criminal.
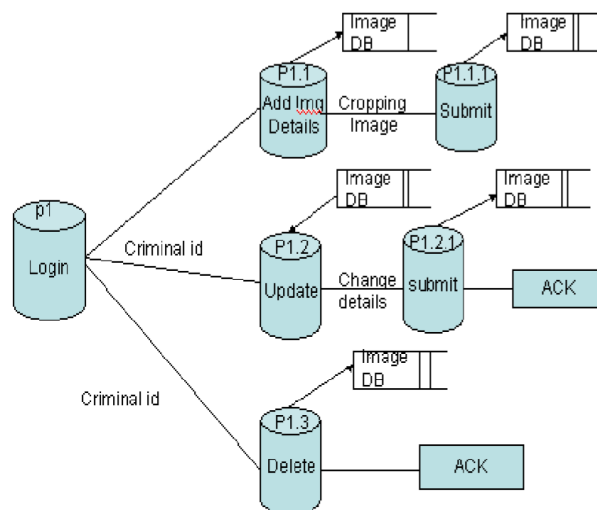

Figure 1. Diagrammatic Representation of Criminal Face Detection System

VI. SYSTEM ANALYSIS AND DESIGN

User-designed projects improve system maintenance. A formal system is one that is developed from the ground up and the scale that is, divided into functional objects. In this project User modelled the system so that the project had little effect on each other. This application is designed for five independent modules that take care of different functions.

A. Modules Description
- User Interface Module.
- Admin Module.
- Client Module.
- Database Operations Module.
- Splitting and Merging Module. ❑Identify Module.

a. User Interface Module
In fact every app has one user interface to access the entire app. In this app User also provide a single user mode for accessing this app. The user interface is completely built based on end users. Provides user-friendly access. This user interaction has an attractive and sensual look. Technically using the swap in core java to configure this user interface.

b. Admin Module.
This Module gives the user a new user id and password. An administrator can delete an unwanted user id and password. Firstly the user details will be available using the user id and password. After receiving the original information the updated information is sent.

c. Client Module.
This module helps employees access the homepage by entering their id and password. A criminal's personal information is stored on a database. Images are grown and stored in a database. Update details and photos of an existing criminal. Delete details and imagery of unwanted hijacker.

d. Database Operations Module.
This module helps to view all the clips and select the clip shown by eyewitnesses. Compare drag and photos of criminals. Create a criminal face by inserting all the burned fingers.

e. Splitting and Merging Module.
Add Module: Add-on module helps in adding criminal information and criminal image information. When User add criminal information, User cut out the criminal's picture and keep those parts planted in a different location.
*Delete Module***:** This module removes criminal information and imagery. The operator first invokes the id of the case first and seeks access to the id where it stores it. If that id is found in a database, then the operator can delete the record of that particular criminal.

Update Module: The operator first logs in with the criminal id and seeks access to that id .If that id is found in the database, the details of this criminal are available and the operator can update the details of the criminal and that the criminal information is stored in the database again for recovery.

f. Identify Module
User has personally seen the part planted by the criminal and frozen by the operator. After that the full face of the criminal is formed and details of the crime are obtained.

IV. PERFORMANCE EVALUATION

This section describes the analyzes needed to develop the proposed system for operational requirements and non-operational requirements. Function requirements specify what the system should do and support the user's tasks in performing and completing tasks. The program allows the user to log in using the default username and password as "admin".
- The system allows the user to enter a photo to be matched.
- The system allows the image to be compared.
- The system provides a compatible event when the input has more than 70% similarity to the image on the face.

Facial information is created through the acquisition of images of people. This image should be part of the body when the face is forward. In the process of image id validation, an image captured using a digital camera will be processed. The image will be retrieved and ready for the next stage. The next stage is pre-processing, in which the unnecessary material is removed. This is to reduce the effort for unnecessary work. In the feature extraction, images are collected from the database and represented as a vector, and then the algorithm will find the average face vest or expression and will remove the dynamic face from each sample face. These features will be used in the recognition phase when trying to match the image to the database. For comparison, image identification will be guaranteed, otherwise it will stop.

A. Hardware Requirements
- Processor   : Pentium III – 900 MHz
- Hard Disk   : 300GB
- RAM   : 2GB

B. Software Requirements
- ❑ Operating System   : Windows 8.1
- ❑ GUI   : Java Swing, AWT.
- ❑ Application Logic   : Java 7.
- ❑ Database   : Oracle 10g
- ❑ IDE/Workbench   : My Eclipse 6.0.

C. Results and Discussion
The performance of Criminal face detection system is analyzed and compared with existing face recognition approaches. The metrics used for comparison are accuracy in detection, time taken to detect, error rate and recognition rate. The tables and figures given in this paper establish the detailed description of the performance of proposed criminal face detection system and existing approaches.

a. Accuracy
Accuracy is defined as the correctness of the exact value predicted. In table 1, the accuracy obtained by proposed criminal face detection and existing approaches is shown.

On analysis accuracy is moderately increased in proposed method than existing method. Figure 2 shows the graph view of accuracy. It is clear that the proposed method works better than the existing methods and gives better accuracy of 91%.

Table 1. Analysis of Accuracy

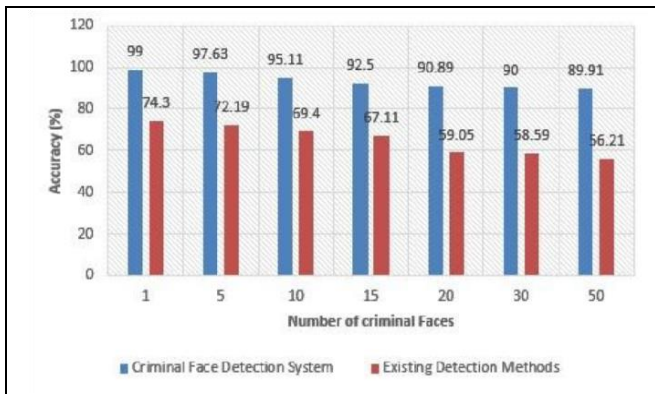| Number of Criminals	Accuracy (%)	
	Proposed Criminal Face Detection System (%)	*Existing Detection Methods*
1	99	74.3
5	97.63	72.19
10	95.11	69.4
15	92.5	67.11
20	90.89	59.05
30	90	58.59
50	89.91	56.21

Figure 2. Comparison graph of Accuracy

b. Time Speed in detecting

The time speed is the total time taken by the system to complete the prediction. Table 2 and shows the time speed for face detection and during the detection. Time taken to detect number of faces is reduced and quick response is accomplished in proposed method. Figure 3 shows the graph of time speed. The time speed for detecting the criminals is increased in the proposed method. It works better about 97% of speed.

Table 2. Time Speed in detecting

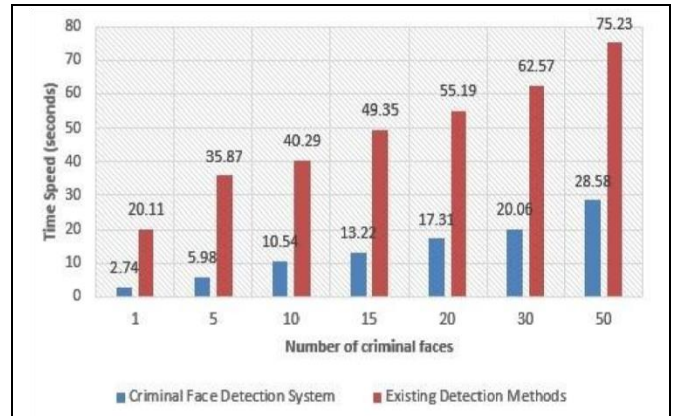| Number of Criminals	Time Speed (seconds)	
	Proposed Criminal Face Detection System	*Existing Detection Methods*
1	2.74	20.11
5	5.98	35.87
10	10.54	40.29
15	13.22	49.35
20	17.31	55.19
30	20.06	62.57
50	28.58	75.23

Figure 3. Comparison of Time Speed

c. Error Rate

Error rate is defined as the frequency of errors occurred and error rate should be gradually decreased. Table 3 shows the error rate occurred during the detection. Figure 4 sows the graph of error rate. In the proposed method the error rate it reduced about 99%.

Table 3. Error Rate

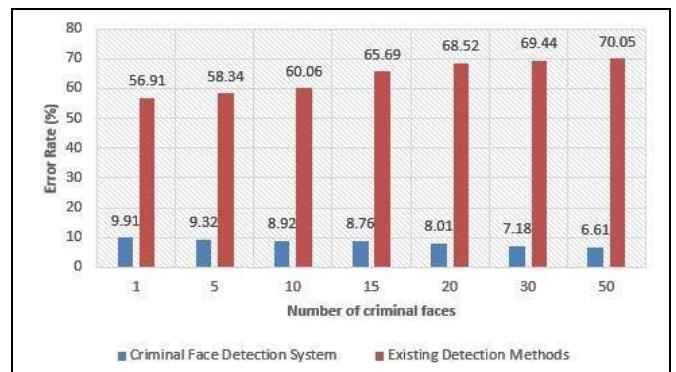| Number of Criminals	Error Rate (%)	
	Criminal Face Detection System	*Existing Detection Methods*
1	9.91	56.91
5	9.32	58.34
10	8.92	60.06
15	8.76	65.69
20	8.01	68.52
30	7.18	69.44
50	6.61	70.05

Figure 4. Comparison graph of Error Rate

d. Recognition Rate

Recognition Rate is defined as the number of positive decisions from total number of decisions. In table 4, the face recognition rate is been depicted. The proposed method gradually increases the recognition rate. Recognition rate is shown as graph view in figure 5. The proposed method increases the recognition rate of about 92%.

Table 4. Recognition Rate

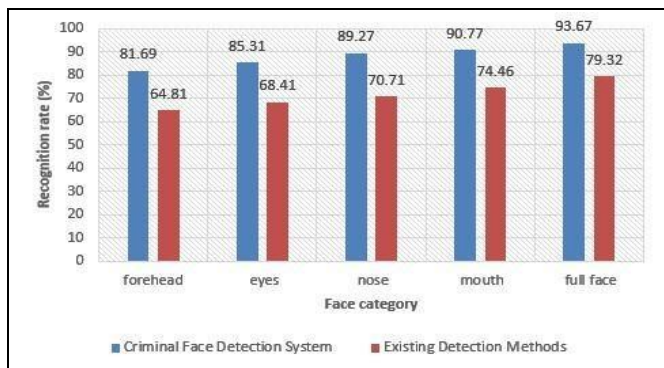| Face Category	Recognition Rate (%)	
	Criminal Face Detection System	*Existing Detection Methods*
Forehead	81.69	64.81
Eyes	85.31	68.41
Nose	89.27	70.71
Mouth	90.77	74.46
Full face	93.67	79.32

Figure 5. Comparison graph of Recognition Rate

V. CONCLUSION AND FUTURE SCOPE

Criminal Identification Program is a User based application to identify criminals. This software package has been successfully calculated and tested for "test cases". It is user-friendly and has the necessary, user-friendly options to perform the tasks user want. The criminal facial recognition system should be able to recognize faces in many different Images. It cases and will find the face User without searching the image completely. The criminal face identification system will have a broad application for distribution in intelligence areas. The software is developed using java as a front end and a back-end in windows environment. By analysing the results produced by the proposed method, it is well understood that it works better than the exiting works by 98% improvement. The future development of this work includes the following:

• Criminal images can be of any size.
• By selecting any part of the case piece, User can get a full picture of the criminals and details.
• New faces formed by decorative parts can be saved.

REFERENCES

[1] Murray I. Cole, "Algorithmic skeletons: structured management of parallel computations," in Research Monographs in Parallel and Distributed Computing. London:Pitman, MIT Press, 1989.
[2] Jain AK, Bolle R, Pankanti S, editors. "Biometrics: personal identification in networked society". Springer Science & Business Media; Apr 2006.
[3] D. Serot and J. Derutin, "Skipper: A skeleton-based programming environment for image processing applications," in Proceeding of the Fifth International Conference on Parallel Computing Technologies, 1999.
[4] C. Nicolescu and P. Jonker, "A data and task parallel image processing environment," Lecture Notes in Computer Science, vol. 2131, pp. 393–408, 2001.
[5] J. Haddadnia, K. Faez, and P. Moallem, "Human face recognition with moment invariants based on shape information," in Proceedings of the International Conference on Information Systems, Analysis and Synthesis, vol. 20, (Orlando, Florida USA), International Institute of Informatics and Systemics (ISAS), 2001.
[6] T. Ramesh and S.Sumithra, "OPKNOT – Schemata Method for Mutation Testing Experimented on Event Driven Web Applications", International Journal of Innovative Research in Computer and Communication Engineering, ISSN 2320-9798,Vol 5, Issue 1, PP 761-770, January 2017.
[7] Wagner A, Wright J, Ganesh A, Zhou Z, Mobahi H, Ma Y. "Toward a practical face recognition system: Robust alignment and illumination by sparse representation". IEEE transactions on pattern analysis and machine intelligence, Vol.34, Issue.2, pp. 372-386, Jun 2011.
[8] T. Ramesh and S.Sumithra, "A Review on Different Approaches of Mutation Cost Reduction Techniques", International Journal of Innovative Research in Computer and Communication Engineering, Vol.5, Issue.1, pp.771-775, January 2017.
[9] Cai, D., He, X., Han, J. and Zhang, H.J, "Orthogonal laplacianfaces for face recognition". IEEE transactions on image processing, Vol.15, Issue.11, pp.3608-3614. 2006.
[10] H. Fatemi, H. E. Malek, R. Kleihorst, H. Corporaal, and P. Jonker, "Real-time face recognition on a mixed SIMD VLIW architecture," 4th seminar on embedded systems, Proceedings, (NieuUsergein, The Netherlands), 22 October 2008.
[11] S.Anila&Dr.N.Devarajan, "Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions", Global Journal of Computer Science and Technology Graphics & Vision, pp.13-18, 2012.
[12] Boya Akhila1 , Burgubai Jyothi, "Face Identification through Learned Image High Feature Video Frame Works", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.4, pp.24-29, August 2018.
[13] Ratnesh Kumar Shukla1, Ajay Agarwal , Anil Kumar Malviya, "An Introduction of Face Recognition and Face Detection for Blurred and Noisy Images", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.3, pp.39-43 , June 2018.

AUTHORS PROFILE

M. Jebasheeli received Bachelors Degree in Information technology in the year 2018 from Nirmala Arts and Science College for Women, Coimbatore, Tamil Nadu, affiliated to Bharathiar University. She is currently pursuing a Masters Degree in Information Technology from 2018 to 2020, at Bharathiar University, Coimbatore, Tamil Nadu. Her area of interest is Data Sciences and Cloud computing.

R. Vadivel is an Assistant Professor in the Department of Information Technology, Bharathiar University, Tamil Nadu, India. He received his Ph.D degree in Computer Science from Manonmaniam Sundaranar University in the year 2013. He obtained his Diploma in Electronics and Communication Engineering from State Board of Technical Education in the year 1999, B.E., Degree in Computer Science and Engineering from Periyar University in the year 2002, M.E., degree in Computer Science and Engineering from Annamalai University in the year 2007. He had published over 40 journals papers and over 30 conferences papers both at National and International level. His areas of interest include Computer Networks, Network Security, Information Security, etc.