Research Paper on Security Systems using Viola Jones for Face Detection

Simra Kamil[1], Mohd Saif Wajid[2]
[1]M. Tech Scholar (CSE), [2]Assistant Professor
BBDU, Lucknow, UP

Abstract **-** Today's institutions are facing major security issues; consequently, they need several specially trained personnel to attain the desired security. These personnel, as human beings, make mistakes that might affect the level of security.

A proposed solution to the aforementioned matter is a Face Recognition Security System, which can detect intruders to restricted or high-security areas, and help in minimizing human error. This system is composed of two parts: hardware part and software part. The hardware part consists of a camera, while the software part consists of face-detection and face-recognition algorithms software.

"Seeing is believing", the old saying goes. Vision plays a very important role in our daily life. We should agree that the most important way to understand the world is through our eyes. Although the underlying mechanism of human vision is not clear, people can see objects and recognize them with very little effort. This ability makes us respond appropriately to our environment. The power of human vision led people to attempt the creation of a machine that could see. In particular, people believe that machines with vision capability might be able to respond to its environment, just as humans do. Such machines would be useful in minimizing human intervention in areas like surveillance and industrial flaw detection. Recognition of the human face is an important himian machine interface component. In this thesis, we present an approach for the development of a real time biometric system for detection, tracking and recognition of the human face.

Keywords **–** Digital Image Processing, Face Detection, Face Recognition, Biometrics

I. INTRODUCTION

A. Face Recognition - A Biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioural characteristic of the person [JBP99]. Biometrics represents the most secure way of identifying individuals because verification of identity is established using a physical and imique biometric characteristic. Passwords or PINs used alone are responsible for accessibility frauds on corporate computer networks and the Internet because they can be guessed or stolen. Plastic cards, smart cards or computer token cards by themselves are also not secure because they can be forged, stolen or lost, or can become corrupt or unreadable. Biometric methods for identification can be widely adapted to forensics, ATM banking, time and attendance recording, access control and many other applications. Biometric technologies include:

i). Face Recognition
ii). Finger Print Identification
iii). Hand Geometry Identification
iv). Iris Identification
v). Voice Recognition
vi). Signature Recognition
vii). Retina Identification
viii). DNA Sequence Matching

Among these methods, there are multiple benefits in face recognition over the others. While the others require some voluntary action, face recognition can be used passively. It has the advantages of being easy to use as well as adaptable for covert use as in surveillance applications. Face images also allow easy audit and verification performed by human operators when logging biometrics records. It is also easier to acquire good images than good fingerprints. It turns out that about 5% of all people cannot provide a fingerprint good enough for a reader for verification. The reasons may be numerous such as cut skin, bandaged finger, callused finger, dry skin, diseased skin, old skin, oriental skin, narrow finger, smudged sensor on reader, etc. Damage of epidermis tissue distorts identification through hand geometry. Use of fingerprint scanners or palm readers can transmit germs through contact areas. In contrast, a face recognition system is totally hygienic and requires no human intervention because the face is measured fi-om a distance non-intrusively. Iris scans can provide a very high accuracy for person identification. However, because the iris is so small, it takes two expensive camera motion drives with high resolution to find the iris. As the camera view has to be narrow to capture the resolution of the iris, the whole process is highly sensitive to body motion and as a consequence the subject has to be significantly co-operative for correct recognition. Retina readers sense the retinal vein patterns in the back of the eye. The subject is required to look into an eyepiece while some light is being reflected off the back of the eye to capture the vein patterns. Although retina scanning yields highly accurate identification, most people would still resist having intrusive measurement inside their eyes. Both iris and retina scanning fail to identify people who wear vanity contact lenses which cover

the iris and the retina or people blinking while being captured.

Glare from glasses can also prevent the scaimers from finding the iris or the retina. In contrast, an automated face recognition system requires an inexpensive camera which does not need to move because as it has a large enough field of vision to cover the subject irrespective of posture amidst a wide range of extraneous noise and distortions to the image such as glare reflected from the spectacles, closure of eyes etc. Voice recognition for surveillance is not reliable in noisy environments like public places or across phone lines with variable acoustic properties. Voice recognition systems are also sensitive to hoarse throat conditions when people are sick with cold. A tape recording of the person's voice can fool voice recognition systems that do not have a challenge-response process.

Signatures are used for legally binding documents, but it usually turns out that signatures greatly vary fi:om time to time and from mood to mood. Face recognition is convenient to be operated indoors and outdoors by detecting and cropping the area containing probable face pattern from complex background. Different biometric techniques can be combined with face recognition in order to build a reliable and accurate multi-modal person authentication system. Face recognition system find application in all surveillance and authentication requirements.

B. Problem specification - The goal of this research is to develop an on-line face recognition system based on a fast and efficient face segmentation approach to investigate the performance of the popular face recognition techniques in a real time scenario. As the subjects enter the scene the system should:

i). Capture images from the camera on-line,
ii). Detect the existence ofa face in each frame,
iii). Efficiently segment the face,
iv). Normalize the face and finally
v). Recognize and display human Photo.

Recognition is based on frontal face images with certain pose and scale variation in a cluttered background. The system developed should display the current frame, the segmented face and the name of person in the scene if he/she is belongs to trained set.

II. LITERATURE REVIEW

Raghavendra *et al.* have described the Reliable user identification which was a common requirement for almost every secure system. Biometric offer a natural and reliable solution to certain aspects of identity management by recognizing the individuals based on their inherent physical and behaviour characteristics. Multimodal biometric person verification was gaining much popularity in recent years as they outperform uni-modal person verification. Their paper presents a person verification system using speech and face data. The verification system comprises of two classifiers whose scores were fused using sum rule after normalization. The experiments were carried out on VidTIMIT database. The experimental results show that face expert designed using Two-Dimensional Linear Discriminate Analysis and speech expert using Linear Prediction Cepstral Coefficients as feature extractor and Gaussian Mixture Model as opinion generator with 16 mixtures will provide a Half Total Error Rate of 1.2%.

Uma Maheswari and Anbalagan have described an intelligent multimodal biometric verification system for physical access control, based on fusion of iris, face and fingerprint patterns. Feature vectors were created independently for query images and are then compared with the enrolled templates of each biometric trait to compute the matching score. The final decision was made by fusion at their matching score level. Their proposed system was designed to suit embedded solutions for high security access in pervasive environments using biometric features.

Mohamed Soltane *et al.* have proposed the use of finite Gaussian Mixture Modal (GMM) based Expectation Maximization (EM) estimated algorithm for score level data fusion. Automated biometric systems for human identification measure a "signature" of the human body, compare the resulting characteristic to a database, and render an application dependent decision. Those biometric systems for personal authentication and identification were based upon physiological or behavioral features which were typically distinctive, Multi-biometric systems, which consolidate information from multiple biometric sources, are gaining popularity because they were able to overcome limitations such as non-universality, noisy sensor data, large intra-user variations and susceptibility to spoof attacks that are commonly encountered in mono modal biometric systems. Simulation shows that Finite Mixture Modal (FMM) was quite effective in modelling the genuine and impostor score densities, fusion based the resulting density estimates achieves a significant performance on eNTERFACE 2005 multi-biometric database based on face and speech modalities.

Rufeng Chu *et al.* have presented a face and palmprint multimodal biometric identification method and system to improve the identification performance. Effective classifiers based on ordinal features were constructed for faces and palmprints, respectively. Then, the matching scores from the two classifiers were combined using several fusion strategies. Experimental results on a middle-scale data set have demonstrated the effectiveness of their proposed system.

Dakshina Ranjan Kisku *et al.* have presented a feature level fusion approach which uses the improved K-medoids clustering algorithm and isomorphic graph for face and palmprint biometrics. Partitioning Around Medoids (PAM) algorithm was used to partition the set of n invariant feature points of the face and palmprint images into k clusters. By partitioning the face and palmprint images with scale invariant features SIFT points; a number of clusters were formed on both the images. Then on each cluster, an isomorphic graph was drawn. In their next step, the most probable pair of graphs was searched using iterative

relaxation algorithm from all possible isomorphic graphs for a pair of corresponding face and palmprint images.

Finally, graphs were fused by pairing the isomorphic graphs into augmented groups in terms of addition of invariant SIFT points and in terms of combining pair of key point descriptors by concatenation rule. Experimental results obtained from the extensive evaluation show that the proposed feature level fusion with the improved K-medoids partitioning algorithm increases the performance of the system with utmost level of accuracy.

Most existing face and iris fusion schemes are concerned about improving performance on good quality images under controlled environments.

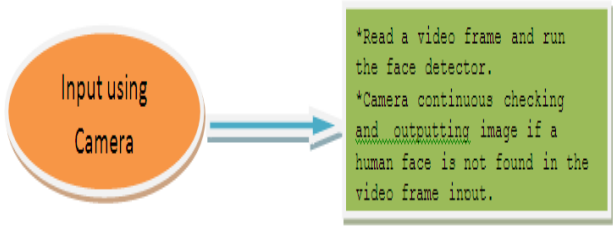
Xiaobo Zhang *et al*. have proposed a hierarchical fusion scheme for low quality images under uncontrolled situations. In the training stage, canonical correlation analysis (CCA) was adopted to construct a statistical mapping from face to iris in pixel level. In their testing stage, firstly the probe face image was used to obtain a subset of candidate gallery samples via regression between the probe face and gallery irises, then ordinal representation and sparse representation are performed on these candidate samples for iris recognition and face recognition respectively. Finally, score level fusion via minmax normalization was performed to make final decision. Experimental results on our low quality database show the outperforming performance of their proposed method.

Due to the increase in security requirements, biometric systems have been commonly utilized in many recognition applications. Multimodal has great demands to overcome the issue involved in single trait system and it has become one of the most important research areas of pattern recognition.

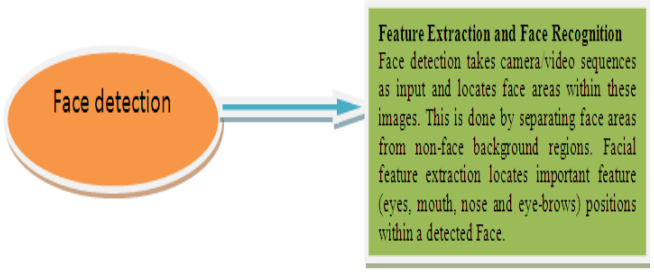
III. PROPOSED METHODOLOGY

A. FLOW STEP -

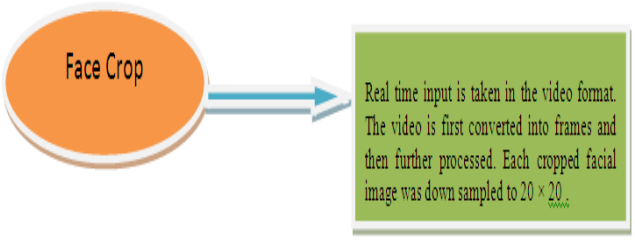
STEP -1



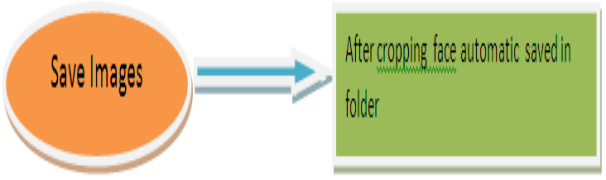
STEP -2



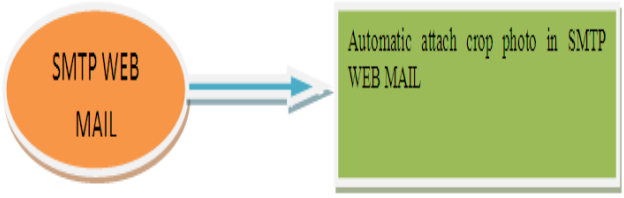
STEP -3



STEP -4



STEP -5



STEP-6

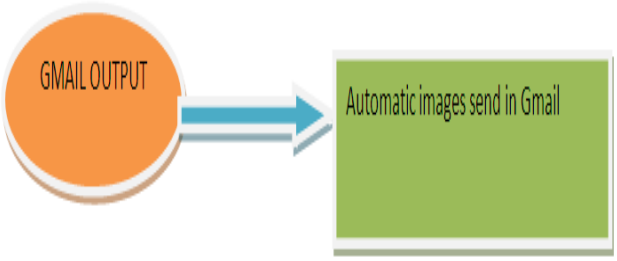


Figure 1: Flow Step

The Viola–Jones Face location system is the main Face recognition structure to offer focused thing discovery cites continuously proposed in 2001 by means of Paul Viola and Michael Jones. Notwithstanding the way that it could figure out how to go over an implication of thing classes, it transformed into supported in the primary through the issue of face location. The inconvenience to be tackled is identification of appearances in a photo. A human can attempt this without trouble; however a PC wants exact directions and imperatives. To make the end eavor additional conceivable, Viola–Jones calls for full view frontal upright appearances. In this manner for you to be recognized, the total face needs to indicate the computerized

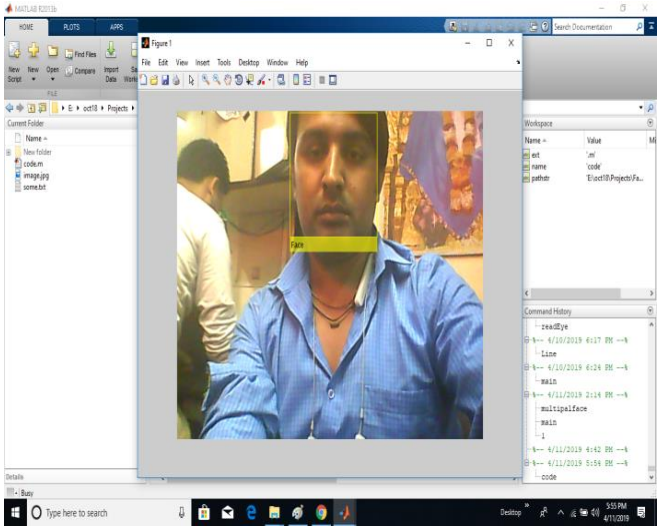
camera and need to not be tilted to both aspect. While it appears those requirements could decrease the arrangement of tenets programming especially, in light of the fact that the location step is most generally joined by an acknowledgment venture, in exercise these cut off points on posture are pretty suitable. The abilities looked for by means of the recognition system all around includes the wholes of photograph pixels inside square districts. In that capacity, they look somewhat like Haar premise highlights, which have been utilized in the past inside the domain of photo based thoroughly Face detection.[3] in any case, in light of the fact that the capacities utilized by Viola and Jones all rely on upon two or three square region, they might be typically additional confused. The figure at right outlines the four restrictive sorts of abilities utilized as a part of the system. The cost of any given element is always unquestionably the aggregate of the pixels inside clean rectangles subtracted from the whole of the pixels inside shaded rectangles. As is not out of the ordinary, square.

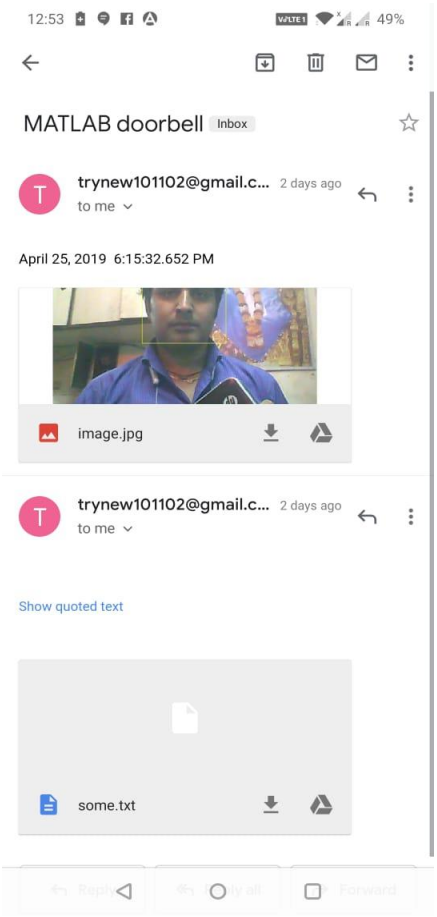
B. Viola jones face detection algorithm - By and large, viola jones confront identification calculation has three basic strides, including highlight extraction, boosting and multi-scale discovery.

C. Feature Extraction - Clearly highlight is extremely critical to any Face location calculation. Fundamentally, there are a ton of elements, for example, eyes, nose, the topology of eye and nose, can be utilized for face location. In viola jones confront location, an exceptionally basic and clear component has been utilized. Figure 1 indicates four diverse elements in viola jones calculation. Each element can be gotten by subtracting white regions from the dark regions.

Here, the region implies the summation of the considerable number of pixels' dim an incentive inside the rectangle. Going for figuring these elements, an exceptional portrayal named as necessary picture has been utilized.

IV. RESULTS





V. CONCLUSION

Face recognition systems are going to be used more and more in the future for security reasons because they provide better performance over other security systems.

An experimental study face recognition system is presented, which may be applied in identification systems and access control.

Real time face recognition is part of the field of biometrics. Biometrics is the ability for a computer to recognize a human through a unique physical trait. Face recognition provides the capability for the computer to recognize a human by facial characteristics. Today, biometrics is one of the fastest growing fields in advanced technology. Predictions indicate a biometrics explosion in the next century, to authenticate identities and avoid and unauthorized access to networks, database and facilities.

VI. REFERENCE

[1]. **X. Li and S. Areibi,** "A Hardware/Software Co-design Approach for Face Recognition," Proc. 16th International Conference on Microelectronics, Tunis, Tunisia, Dec 2004.

[2]. **Moritoshi Yasunaga, Taro Nakamura, and Ikuo Yoshihara**, "A Fault-tolerant Evolvable Face Identification Chip," Proc. Int. Conf. on Neural Information Processing, pp.125-130, Perth, November 1999.

[3]. **In Ja Jeon, Boung Mo Choi, Phill Kyu Rhee**. "Evolutionary Reconfigurable Architecture for Robust Face Recognition,"

ipdps, p. 192a, International Parallel and Distributed Processing Symposium (IPDPS'03), 2003.

[4]. **R. Chellappa, C.L. Wilson, and Sirohey**, "Human and Machine Recognition of Faces, A survey," *Proc. of the IEEE*, Vol. 83, pp. 705-740, 1995.

[5]. 3D model enhanced face recognition ***Wen Yi Zhao; Chellappa, R.;*** Image Processing, 2000. Proceedings. 2000 International Conference on , Volume: 3 , 2000.

[6]. SFS based view synthesis for robust face recognition ***Wen Yi Zhao; Chellappa, R.;*** Automatic Face and Gesture Recognition, 2000. Proceedings. Fourth IEEE International Conference on , 2000

[7]. **Rajamäki, J., Turunen, T., Harju, A., Heikkilä, M., Hilakivi, M. and Rusanen, S.,** "Facial Recognition System as a Maritime Security Tool", in *Proceedings of the 8th WSEAS International Conference on Signal Processing (SIP '09)*, Istanbul, Turkey, May 30 - June 1, 2009, pp. 115-121.

[8]. **Sertbay, H. and Toygar, Ö,** "Face Recognition in the Presence of Age Differences using Holistic and Subpattern-based Approache", in *Proceedings of the 8th WSEAS International Conference on Signal Processing (SIP '09)*, Istanbul, Turkey, May 30 - June 1, 2009, pp. 94-98.