Face Analysis for Improvised System Security using LASER Focus

Dhruvesh Chudasama[1], Vijay Prakash Tiwari[2], Vikas Tiwari[3], Prof. Parinita Chate[4]

[1]*Department of Computer Engineering, Bharati Vidyapeeth's COE, Lavale, Pune, MH, IN*
[2] *Department of Computer Engineering, Bharati Vidyapeeth's COE, Lavale, Pune, MH, IN*
[3]*Department of Computer Engineering, Bharati Vidyapeeth's COE, Lavale, Pune, MH, IN*
[4]*Professor, Department of Computer Engineering, Bharati Vidyapeeth's COE, Lavale, Pune, MH, IN*

---***---

Abstract – *Today, technological advancement is taking place at every corner of the world. The more advance its gets, the more security is required for the verification and identification of the end user. Therefore, the security systems are always the area of interest for the researchers. Many algorithms have been implemented for the same. Involving the Biometrics Methods to it took the security to next level. But it wasn't new that Biometrics methods is getting handy for the identification and verification purpose. Its foundation was already established back in 19th Century. Face Recognition and Face detection has always been the most recognized method of identification and verification. But it eventually failed to identify weather the image of the face in front of the camera is of a real person or any unauthorized person that is holding photograph of the authorized person. Solution to this problem is introduction of the LASER Focus Technology to it. In this paper, we will discuss and understand various Face Analysis Techniques like Facial recognition and Face Detection. Followed up by how can we integrate the LASER Focus Technology to it to have an Improvised System Security.*

Key Words: **Face Analysis, Facial Recognition, Face Detection, LASER Focus**

1.INTRODUCTION

Based on the individual's physiological and behavioral characteristics, Biometrics has various self-executable methods for individual's recognition. Earlier, in Biometrics method of recognition of an individual utilizes characteristics like the distinctive body characteristics that includes scars or collection of other physiological characteristics like color of eyes, skin complexion, height, etc. The present features are Facial Recognition, Finger Prints, Handwriting, Hand Geometry, Iris, Vein, Voice and Retinal Scan. Foundation of various highly secured identification and verification procedure are Biometric Techniques. Day by day the attacks on system is increasing, security is breached with exponential rate therefore the demand for an accurate, efficient and highly secured verification and identification system. Current world scenario of various security breaches has raised a lot of question over the existing systems for verification and identification. This increases the area of interest in the field involving biometrics and its techniques that can be used for the security purposes. Biometrics Techniques has evolved since decades therefore they can be broadly classified in two categories. First, Old Biometrics Techniques that involves Hand Prints, Anthropometrics, Finger Prints, Manual or Semi-Automated Facial Recognition, etc. Second, Modern Biometrics Techniques that involves Fully-Automated Facial Recognition, Iris Pattern Differential, Heartbeat Pattern Recognition, Brain Signal Pattern Recognition, etc. Among all techniques, the most widely recognized Biometric Method used for identification and verification is Facial Recognition Technique.

2. FR (FACIAL RECOGNITION)

By just looking at the face of an individual, one can differentiate that person from another. FR (Facial Recognition) is the Biometric Technique that performs recursive search in order to matching the physiological features of the face for recognizing the face on an individual. FR basically records all the spatial geometry of a particular face and use it a signature value for the verification and identification purposes. FR comes in handy when the Law and Enforcement need to identify the terrorists or the criminals. FR is a cheap and non-intrusive Technology. In 2D FR, various factors affect the accuracy of the system to identify the person. These factors include the Light, Age of Person, Colored Hair, Amount of Facial Hair, Wearing Eye Glasses or Contact Lenses, Low Resolution Image and the type of Camera used. Many Countries like, India, US, etc. utilizes this FR Technology to issue the Identifications to their Citizens. Due to various complexity factor involve in FR that affect the result, there the FR has been a very challenging area of research since ages. On one side, the applications of the FR are very useful for identification and verification system while on the other side, it is very difficult to implement a cent percent accurate system due to involvement of various factors that can alter the record or the result. FR (Facial Recognition) works as the Computer Vision that uses person's face to identify and verify their claimed identity. Following are the steps involve in FR implementation:

Step 1: ACQUIRING THE FACIAL IMAGE

There are two ways of acquiring the image of the individual's facial image.

1) Acquire a Live Image
2) Digitally Scan the Facial Image Photograph

Step 2: LOCATE FACE IN IMAGE

Various Software or Applications are used to locate the face in the image.

Step 3: ANALYSIS OF FACIAL PATTERN

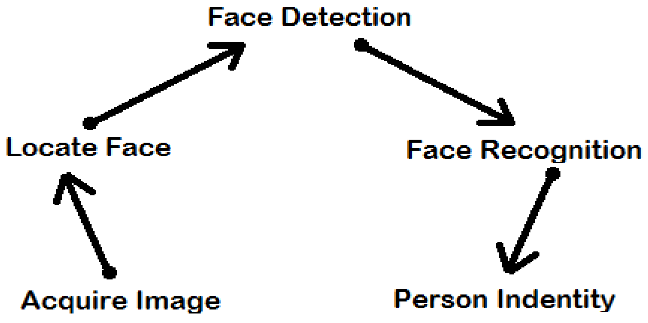
The Application or the Software used, measures face in the image based on its peaks and valleys. Software focuses on the inner area of the face identified as the "Golden Triangle". Peaks and Valleys are used to create a Face Print with their nodal points.

Step 4: COMPARE WITH EXISTING INFORMATION

The Face Print generated as an output given by the software used, is then compared to all face prints that the system has stored in its database.

Step 5: NO MATCH OR MATCH

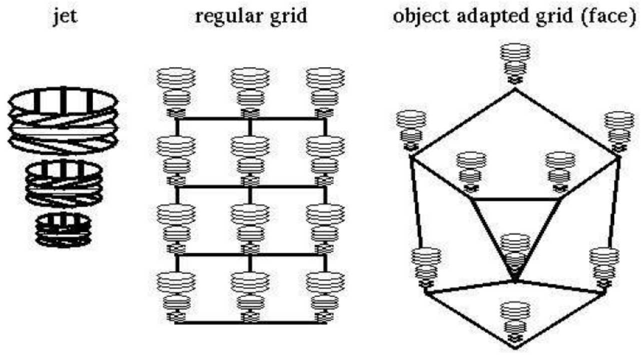
The Application or the Software used, decides whether or not any comparisons from Step 4 are close enough to declare a possible match.



2.1. FR (FACE RECOGNITION) ALGORITHMS

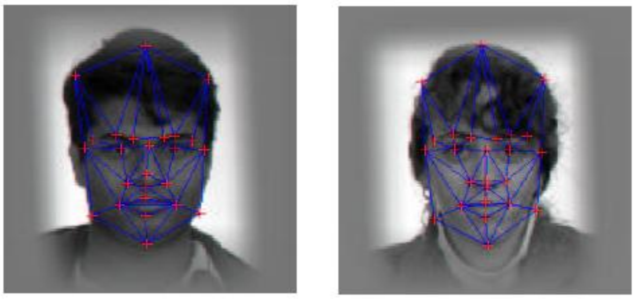
GWT (Gabor Wavelet Transform) is used to construct a labeled graph that would represent faces. A similar process will find image graphs of new faces automatically. Recognition is then done based on a simple similarity measure between the image graph and a database of model graphs known as galleries of model graphs. 3 major extensions were introduced to the previous system in order to handle larger variations and larger galleries in pose, and to increase the accuracy of match.

1. We use the phase of the complex GWT coefficient to achieve a more precise location of the nodes of the graph.
2. We employ objects adapted graphs, so that nodes refer to specific facial landmarks, called Fiducial Points. The correct correspondences between two faces can then be found across large viewpoint changes.
3. Bunch Graph, a new data structure was introduced, which serves as a generalized representation of faces by combining jets of a small set of individual faces. This allows the system to find the Fiducial Points in one match process, which eliminates the necessity for matching each model graph individually. This significantly reduces the computational effort.



2.1.1. PREPROCESSING WITH GABOR WAVELETS

Local features are represented on basis on a GWT. It is defined as a convolution of the grey value image with a family of Gabor kernels in the shape of plane waves with wave vector kj, restricted by a Gaussian envelope function. The aim of elastic Bunch Graph matching on a probe image is just to find the Fiducial Points and thus to extract from the image, a graph which maximizes the similarity with the FBG as defined in Equation (5). In practice, one has to apply a Heuristic algorithm to come close to the optimum within reasonable time. We use a coarse to fine approach in which we introduce the degrees of freedom of the FBG progressively: translation, scale, aspect ratio, and finally local distortions. Phase information is used only in the latter steps. The resulting graph is called the image graph and is stored as a representation for the individual face of the image.



3. FD (FACE DETECTION)

In recent years, FD (Face Detection) in an image sequence has always been an active area of research in the field of Computer Vision due to its potential applications as Monitoring and Surveillance Technology, Human-Computer Interfaces, Intelligent Robots and Biomedical Image Analysis. FD is based on identifying and locating a face in a given image, regardless of its position, size and condition. Simple physical characteristics such as Color, Motion, and Texture are used for the FD in early researches. Eventually with time, these characteristics based FD break down because of less accuracy and since the complexity of the real world. Real-Time Face Detection (RTFD) is achieved by using a High Performance Computer. RTFD System utilizes statistics based algorithm. Hence RTFD Technology, resulted in the development of RTFD Systems that employs an FPGA implemented system, that was designed by the Verilog HDL.

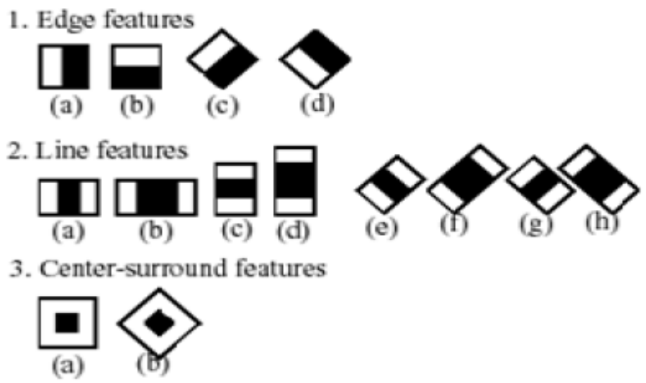
3.1. FD (FACE DETECTION) ALGORITHMS

Viola and Jones introduced a statistics based algorithm for Face Detection. The algorithm proposed always look for particular Haar features in a face. When algorithm find one of these features, then it allows the FC (Face Candidate) to pass to the next stage of detection. A Face Candidate is a sub-window of rectangular section of the original image. Mostly, these sub-windows have a fixed size of typically 24×24 pixels. These sub-windows are often scaled, in order to obtain a variety of different size faces. The algorithm scans the entire image using this window and denotes each respective section a FC (Face Candidate).

3.1.1. INTEGRAL IMAGE

Summation of the pixel values of the original image is defines as Integral Image. The value at any location (x, y) of the integral image is the sum of the images' pixels above and to the left of location (x, y).

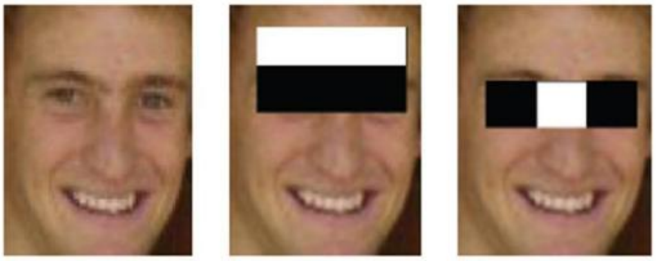
3.1.2. HAAR FEATURES



These are composed of either 2 or 3 rectangular sections. Face Candidates are scanned and searched for Haar features of the current stage. The weights are constants. Weights are generated by the learning algorithm.

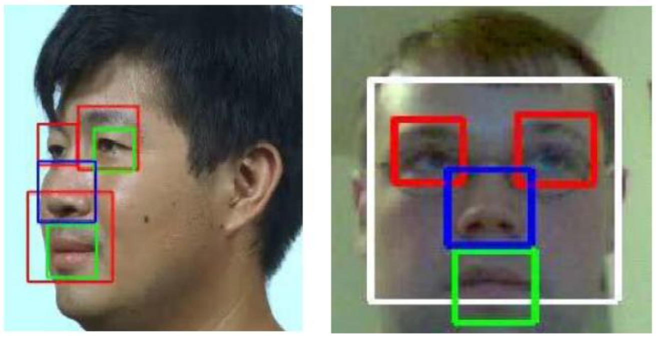
3.1.3. CASCADE

FC are quickly eliminated by the algorithm using a cascade of stages. Candidates are eliminated by making requirements stricter at every stage. Later stages become much more difficult for a candidate to pass. Candidates exit the cascade if they pass all stages or fails. A face is detected if a candidate passes all stages.



3.1.4. REGIONALIZED DETECTION

There is a method is required to reduce the false positive rate of the classifier and to increase accuracy, without modifying the classifier training attribute. The proposed method is to limit the region of the image that is analyzed for the facial features. By reducing the area to be analyzed, accuracy will increase gradually since less area exists to produce false positives. It increases efficiency as well since fewer features are needed to be computed and the area of the integral images is smaller.

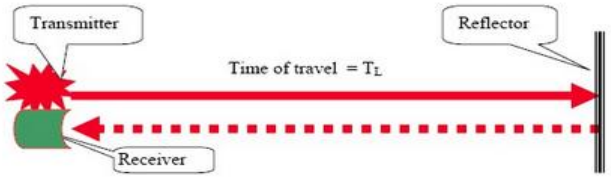


4. LASER FOCUS WITH FR AND FD

Acquiring an image for the analysis of face can be used as a security feature. There the software need to justify weather the user is authorized or not. If an image from the photograph is used for ID verification, then the system will grant the permission to the user without checking that the user is an intruder or not. The system will break down on this. Therefore, introduction of the LASER Focus technology for differentiating between the person's image from a photograph and the live image from the real person is an essential step towards securing the Facial Recognition.

4.1 WORKING

Using LASER Technologies for distance calculation is not new. The idea has been used in numerous industries and products since ages, including in some compact digital cameras. Using the same idea for verifying that the particular user is legitimate or not. There's a small LASER transmitter located on the device near the camera sensor, which is where most of the work takes place. The first step involves firing out a short laser light burst, which is then reflected back off whatever you happen to be pointing the camera at. This light then travels back towards the sensor, where the software calculates the time it takes for the light to leave and return, resulting in a very accurate measurement of how far away the target object is.



The beam that is emitted is extremely thin, which manes that there's a lower chance of multiple returns caused by reflections and refractions. However, such a technique doesn't always produce the desire accuracy and results, especially at longer distances and in more open environments. Since, the size of the receiving sensor is quite compact and therefore the angle for error is also relatively small. To solve this issue, the camera has to operate as more of a hybrid device, making use of either laser or contrast detection methods when required. Device compensates for poor laser returns, reflective surfaces and detection of transparent surfaces, which the laser would pass through, with contrast detection. Contrast detection uses the main image sensor, sweeping upwards through increasing levels of contrast to find the difference between adjacent pixels. In situations where contrast detection is used, device's laser system allows the auto focus algorithm to automatically skip the first two feet of distance, which helps to speed up the process. However, there's no actual depth calculations with the contrast method, which makes it more difficult to track moving objects.

By using this hybrid system, the device will be able to very quickly and accurately detect the focal distance of closer objects. The laser operates perfectly in low light conditions, whereas contrast detection would struggle to tell the difference between multiple dark pixels.

5. CONCLUSIONS

The paper gives the various information and techniques used to implement the face recognition and face detection system. It surveys the various algorithms used to implement the system. It suggests how the laser focus technology can be involved with this system to improve the current security system. The paper concludes that the security systems that are used in our day to day life are need to be improved.

ACKNOWLEDGEMENT

This paper is written by the group of 3 people named as Dhruvesh Chudasama, Vikas Tiwari and Saurabh Marne under the guidance of Prof. Parinita Chate. Without the guidance and support of our guide and every individual's personal effort, this paper won't be possible.

REFERENCES

[1] Z. Guo, H. Liu, Q. Wang and J. Yang, " A Fast Algorithm of Face Detection for Driver Monitoring, " In Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications, vol. 2, pp.267 - 271, 2006.

[2] M. Yang, N. Ahuja, "Face Detection and Gesture Recognition for Human-Computer Interaction," The International Series in Video Computing, vol.1, Springer, 2001.

[3] Z. Zhang, G. Potamianos, M. Liu, T. Huang, "Robust Multi- View Multi-Camera Face Detection inside Smart Rooms Using Spatio-Temporal Dynamic Programming," International Conference on Automatic Face and Gesture Recognition, pp.407-412, 2006.

[4] W. Yun; D. Kim; H. Yoon, "Fast Group Verification System for Intelligent Robot Service," IEEE Transactions on Consumer Electronics, vol.53, no.4, pp.1731-1735, Nov. 2007.

[5] Yongsheng Gao; Leung, M.K.H., "Face recognition using line edge map", Pattern Analysis and Machine Intelligence, IEEE Transactions on , Volume: 24 Issue: 6 , June 2002, Page(s): 764 -779.

[6] Renu Bhatia, Biometrics and Face Recognition Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[7] Ms. Jaya M. Jadhav, Ms. Deipali V. Gore, Introducing Celebrities in an Images Using HAAR Cascade Algorithm, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013

[8] Face Recognition by Elastic Bunch Graph Matching,Laurenz Wiskott,Jean-Marc Fellous,Norbert Kruger and Christoph von der Malsburg, Institute for Neural Computation,Ruhr-University Bochum,D-44780 Bochum, Germany

BIOGRAPHIES

Dhruvesh Bhen Chudasama
Pursuing Bachelor of Engineering (B. E.) in Computer Engineering from Bharati Vidyapeeth's College of Engineering, Lavale, Pune, Maharashtra, India.

Vijay Prakash Tiwari
Pursuing Bachelor of Engineering (B. E.) in Computer Engineering from Bharati Vidyapeeth's College of Engineering, Lavale, Pune, Maharashtra, India.

Vikas Tiwari
Pursuing Bachelor of Engineering (B. E.) in Computer Engineering from Bharati Vidyapeeth's College of Engineering, Lavale, Pune, Maharashtra, India.

Prof. Parinita Chate
Professor, Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering, Lavale, Pune, Maharashtra, India.