CREATING REAL TIME DATABASE IN MATLAB & DEVELOPING INFORMATION SECURITY SYSTEM USING BIOMETRICS AUTHENTICATION TECHNIQUE-FACE DETECTION

Deshant [1], Manvi Sharma[2]

[1]*ECE Department, GGSIPU, (India)*

[2]*ECE Department, ABESIT, (India)*

ABSTRACT

In today's information technology world, security for systems is becoming more and more important. Authentication plays a major role in the field of exchanging any data or information where secrecy & privacy of the data to be transferred is must and another factor is, it should be accessed by only authorized person. Authentication is the process of giving someone identity so that he or she can access that particular application or data. It is the act of confirming something what it claims to be something like we are showing our ID proof to get access in the particular area restricted to particular persons only. Objective of the authentication technique using Face detection is to provide and to ensure the full proof security of the information or the data we are sharing by the mean of processing & comparing the unique structure of the face of the person to authenticate him.

Keywords: Authentication, Matrix, Biometric, Authentication.

I INTRODUCTION

Authentication can be defined as of three types:

1) Authentication using something we can remember like Password, PIN or any code.
2) Authentication using something physical thing we can have like Swipe card, Token or any Key.
3) Authentication using something we possess within us that is our Biological characteristics which is called Biometrics.

- Passwords, PIN & codes can be forgotten or hacked.
- Swipe card, Token & Keys can be lost or theft.
- Our Biological characteristics are something that ensures Secure, Convenient & Unique method of authentication of information.

1.1 Biometric Authentication

Biometric identification utilizes physiological and behavioral characteristics to authenticate a person's identity. The term Biometrics is usually associated with the use of unique physiological characteristics to identify any individual. Biometric authentication refers to the identification of humans by their characteristic. The most common application of biometrics is security. Biometric authentication can be further categorized on the basis of physiological versus behavioral characteristics.

Biometric authentication requires to compare a registered biometric sample against a newly captured biometric sample (captured during a login). This is a three-step process followed by a process:

- CAPTURE
- PROCESS
- ENROLL

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. Next step is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed mathematical representation. In next phase, the processed sample (mathematical representation of the biometric) is stored / registered in a storage medium for future comparison during an authentication.

Some of the common physical characteristics that may be used for identification

Includes:

- Fingerprints,
- Palm prints/Hand geometry,
- Retinal scan
- Face recognition
- Iris recognition, etc.

Some of the behavioral characteristics includes:

- Signature,
- Voice recognition
- Keystroke pattern, etc.

A biometric system works by capturing and storing the information and then comparing the recorder/stored information with what is stored in the memory of the device.

Out of all the various physical characteristics available, faces are one of the more accurate physiological characteristics that can be used. Face detection technology does provide a good method of authentication to replace the current methods of passwords, token cards or PINs and if used in conjunction with something the user knows in a two-factor authentication system then the authentication becomes even stronger.

II LITERATURE REVIEW

During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces. He was proud of this work, but because the funding was provided by an unnamed intelligence agency that did not allow much publicity, little of the work was published. Given a large database of images and a photograph, the problem was to select from the database a small set of records such that one of the image records matched the photograph. The success of the method could be measured in terms of the ratio of the answer list to the number of records in the database.

By about 1997, the system developed by Christoph von der Malsburg and graduate students of the University of Bochum in Germany and the University of Southern California in the United States outperformed most systems with those of Massachusetts Institute of Technology and the University of Maryland rated next. The Bochum system was developed through funding by the United States Army Research Laboratory. The software was sold as ZN-Face and used by customers such as Deutsche Bank and operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hair styles and glasses—even sunglasses".

In about January 2007, image searches were "based on the text surrounding a photo," for example, if text nearby mentions the image content. Polar Rose technology can guess from a photograph, in about 1.5 seconds, what any individual may look like in three dimensions, and claimed they "will ask users to input the names of people they recognize in photos online" to help build a database. Identix, a company out of Minnesota, has developed the software, Face It. Face It can pick out someone's face in a crowd and compare it to databases worldwide to recognize and put a name to a face. The software is written to detect multiple features on the human face. I can detect the distance between the eyes, width of the nose, shape of cheekbones, length of jaw lines and many more facial features. The software does this by putting the image of the face on a face print, a numerical code that re In 2006, the performance of the latest face recognition algorithms were evaluated in the presents the human face.

Facial recognition software used to have to rely on a 2D image with the person almost directly facing the camera. Now, with Face It, a 3D image can be compared to a 2D image by choosing 3 specific points off of the 3D image and converting it into a 2D image using a special algorithm that can be scanned through almost all databases. Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.

U.S. Government-sponsored evaluations and challenge problems have helped spur over two orders-of-magnitude in face-recognition system performance.

Since 1993, the error rate of automatic face-recognition systems has decreased by a factor of 272. The reduction applies to systems that match people with face images captured in studio or mugshot environments. In Moore's law terms, the error rate decreased by one-half every two years.

Low-resolution images of faces can be enhanced using face hallucination. Further improvements in high resolution, megapixel cameras in the last few years have helped to resolve the issue of insufficient resolution.

III FACE RECOGNITION TECHNOLOGY

Face recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the faces. A facial recognition system is a computer application for automatically 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 facial database.It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.Face recognition uses camera technology to acquire images of the detailed structures of the face. Digital templates encoded from these patterns, by mathematical algorithms. These algorithms allow the identification of an individual. Databases of existing templates are searched & matched by the matcher engines at speeds measured in the millions of templates per second per CPU

3.1 Face Detection Process

The process of capturing an face into a biometric template consists of below steps:

1. Capturing the image
2. Defining and optimising the image
3. Storing and comparing the image.

1. Capturing the Image:

The image of the face can be captured using a standard camera using both visible and infrared light and may be either a manual or automated procedure. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the face in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face and face automatically thus making this process much more user friendly

2. Defining and Optimising the Image

The face detection system identifies the image that has the best focus and clarity of the face. The image is then analyzed to identify the outer boundary of the face.

The face detection system then identifies the areas of the face image that are suitable for feature extraction and analysis. This involves removing areas that are covered, any deep shadows and reflective areas.

3. Storing and Comparing the Image

Once the image has been captured, an algorithm is used to map segments of the face into hundreds of vectors. These algorithms also take into account the changes that can occur with an face, for example the pupil's expansion and contraction in response to light will stretch and skew the face. This information is used to produce a code which is called as the Face Code, which is a 512-byte record. This record is then stored in a database for future comparison.

When a comparison is required the same process is followed but instead of storing the record it is compared to all the Face Codes which are already stored in the database. The comparison also doesn't actually compare the image of the face but compares the hexadecimal value produced after the algorithms have been applied.

In order to compare the stored Face Code record with an image just scanned, a calculation of the Hamming Distance is required. The Hamming Distance is a measure of the variation between the Face Code record for the current face and the Face Code which is stored in the database. Each of the bits is compared against each other, i.e. bit 1 from the current Face Code and bit 1 from the stored Face Code record are compared, then bit 2 and so on. Any bits that don't match are assigned a value of one and bits that do match a value of zero. Once all the bits have been compared, the number of non-matching bits is divided by the total number of bits, to produce a two-digit figure by which the two Face Codes differ. For example a Hamming Distance of 0.40 means that the two Face Codes differ by 40%.

In All biometric systems there are two type of error rates:

3.2 False Reject Rate (FRR)

FRR occurs when the biometric measurement taken from the live subject fails to match the template stored in the biometric system.

3.3 False Accept Rate (FAR)

FAR occurs when the measurement taken from the live subject is so close to another template that a correct match will be declared by mistake. The point at which the FRR and the FAR are equal is known as the Crossover Error Rate (CER). The lower the CER, the more reliable and accurate the system is. In face detection technology, during detection mode, the comparison has to occur between the Face Code from the live subject and every Face Code stored in the database, before the live subject is rejected.

IV TECHNIQUES

Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances.

.

4.1 3-Dimensional Recognition

A newly emerging trend, claimed to achieve improved accuracies, is three-dimensional face recognition. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. Three-dimensional data points from a face vastly improve the precision of facial recognition. 3D research is enhanced by the development of sophisticated sensors that do a better job of capturing 3D face imagery. The sensors work by projecting structured light onto the face. Up to a dozen or more of these image sensors can be placed on the same CMOS chip—each sensor captures a different part of the spectrum. Even a perfect 3D matching technique could be sensitive to expressions.

4.2 Skin Texture Analysis

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.Tests have shown that with the addition of skin texture analysis, performance in recognizing faces can increase 20 to 25 percent.

V WORKING

The input is 230V AC which is step down using the transformer (12-0-12) .The 12V ac input is fed to the bridge diode to gives 12V pulsating DC. This DC voltage is filtered through the capacitor to remove the ripples. The filtered DC is fed to 7805 regulator to fetch +5v regulated output. This regulated voltage is given to all the components to function properly.

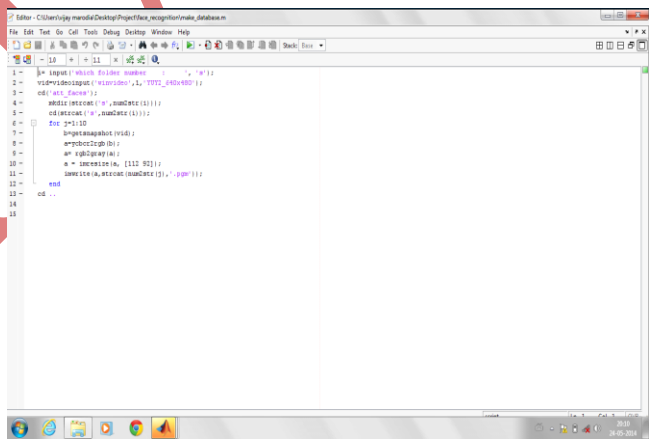


Fig 1: Making the Database.

There are two parts of the projects. One is software and other is hardware. In the software section we are using MATLAB to design the interface between the user and the computer. As shown in fig 1. First a folder is made and 10 random images is taken to be stored in data base.

In fig 2, all the images stored in the database are converted into matrix as the processing of images in form of matrix is easier.

Now in real world a picture as shown in fig 3, is taken from the webcam and will be converted in to matrix form.

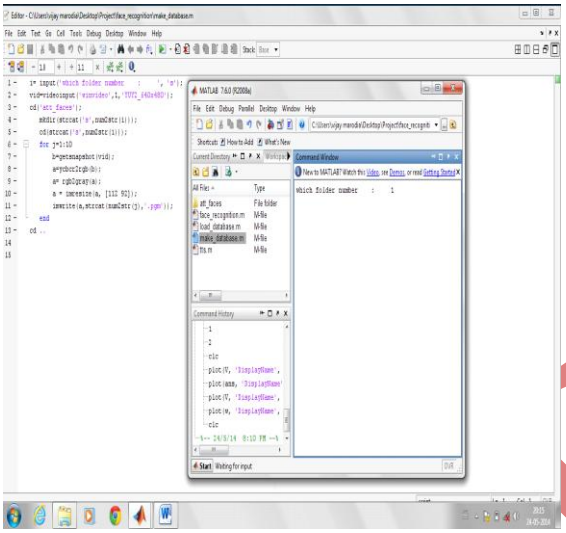


Fig.2: Storing the Database

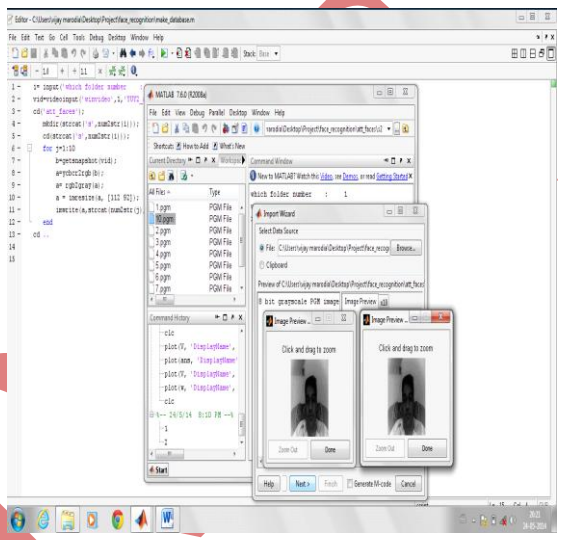
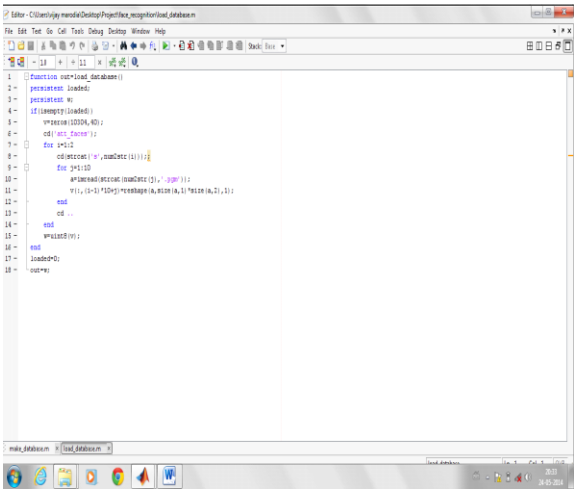


Fig.3: Capturing a Real Time Image

As shown in fig 4, the eigen values and eigen vectors of the image are calculated and for that some predefined maximum values of an image are taken care of.

As shown in fig 5, after eigen value calculation, mean of the matrix is calculated to remove useless information or errors. This is actually done for the removal of noise. In the program, eigen values are restricted to upto 10 which is called as Dominant Eigen values composed of highly detailed information of the face. Now, a correlation technique is applied to compare the real time image with that stored in the database. Correlation converts 2D image values into 1D image values so that comparison becomes bit easier. If the values match with the values stored in the database then the access to that person is given.

In the Hardware part, from computer we send the data at the COM port of the computer. The serial data of computer is USB based. The UART MODULE converts this standard into the TTL standard of the microcontroller. The microcontroller reads the data from the computer turns on door accordingly. To open the door and close it, we are using MATLAB for face recognition (0-1) and generate the serial event on matching of face.



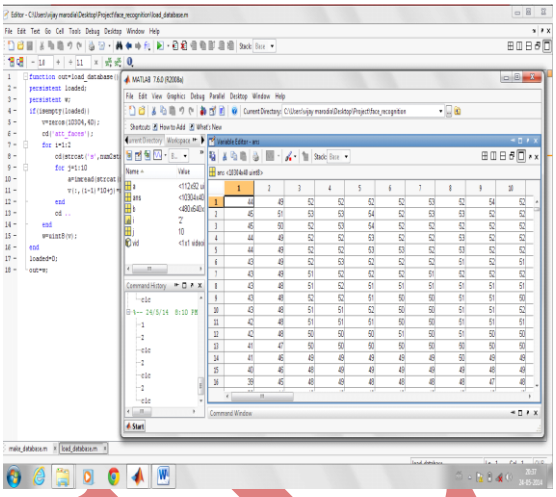


Fig. 4 Calculation of Eigen Values and Eigen Vectors Fig.5 Making Matrix Of The Image.

5.1 Advantages of Face Detection Technology

1. The physiological properties of faces are major advantages to use them as a method of authentication.
2. Uniqueness of the face patterns.
3. One key advantage is that it does not require the cooperation of the test subject to work.
4. It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless the user actually engages it.
5. The accurateness of the scanning technology is a major benefit with low error rates, hence resulting in a highly reliable system for authentication.
6. Scalability and speed of the technology are a major advantage.
7. The technology is designed to be used with large-scale applications such as with ATMs.
8. Ability of the system to scan and compare the face within a matter of minutes is a major benefit.

5.2 Disadvantages of Face Detection Technology

As with any technology there are challenges with face detection as well.

1. Face recognition is not perfect and struggles to perform under certain conditions.
2. Conditions where face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low resolution images.
3. The camera used in the process needs to have the correct amount of illumination. Without this, it is very difficult to capture an accurate image of the face.
4. Along with illumination, problem with reflective surfaces, within the range of the camera & unusual lighting may occur.
5. Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective.

6. Normal day-to-day problems such as system failures, power failures, network problems, and software problems can contribute to rendering a biometric system unusable.

VI CONCLUSİON

Biometric technology is increasingly being used in various applications specially for the smooth flow of cross-border traffic, for authentication of criminal identities and controlled access to military facilities. In addition, more and more consumer market players are using biometrics for effective identification. This includes airlines, gyms and self-service convenience stores aiming to increase their efficiency, as well as pharmacies using it to secure their medicine stocks.

Face detection came into existence due to uniqueness of the face structure as even genetically identical individuals have completely independent face textures.

- High speed of matching with existing templates.
- Extreme resistance to False Matches
- Increased security.
- Eliminate problems caused by lost IDs or forgotten passwords
- Replace hard-to-remember passwords which may be shared/disclosed.

REFERENCES

[1] Poulami Das, Debnath Bhattacharya, Samir Kumar Bandyopadhyay, Tai-hoon Kim “Person identification through Face detection”, International Journal of security & its applications (vol. 3, No. 1), January 2009, pg. 129-147.

[2] Michael Negin, Thomas A.Chmielewski, Jr. Marcos Salganicoff, Theodore A. Camus, Ulf M. Cahn von Seelen, Peter L. Venetianer, Guanghua G. Zhang “ An Face Biometric System for Public and Personal Use”, 2000 IEEE, pg. 70-75.

[3] Harley Geiger, "Facial Recognition and Privacy". Center for Democracy & Technology. Retrieved 2012-01-10.

[4] Jon Krueger, Marshall Robinson, Doug Kochelek, Mathew Escarra, “Obtaining The Eigenface Basis” version 1.3: Dec 17, 2004.

[5] Jonathon Shlens, “A Tutorial on Principal Component Analysis”, Syaytems Neurobiology Laboratory, version 2, 2005.

Books

[6] Cryptography and Network Security by Behrouz A. Forouzan, Debdeep Mukhopadhyay

[7] Data Communication and Networking by Behrouz A. Forouzan