International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 3, March-2014, pp: (80-85), Impact Factor: 1.252, Available online at: www.erpublications.com

A Review Paper on Facial Recognition

Himanshu Garg, Sukhwinder Singh
Student[1], Mentor[2]
[1,2]ECE Department, Assistant Professor, PEC University of Technology, Chandigarh, India

Abstract: This project is to evolve a face detection scheme. The face detection scheme notices a person's face which encompasses eye brows, eyes, nose and mouth. A facial acknowledgement scheme is a computer submission for mechanically identifying or verifying a person from a digital likeness or a video border from a video source. One of the way is to do this is by comparing selected facial characteristics from the likeness and a facial database. It is normally utilized in security systems and can be compared to other biometrics such as fingerprint or eye iris acknowledgement schemes. Lately face acknowledgement is attracting much vigilance in the humanity of network multimedia data access. Localities such as mesh security, content indexing and retrieval, and video compression benefits from face acknowledgement expertise because "people" are the center of attention in an allotment of video. Network get access to control via face acknowledgement not only makes hackers virtually unrealistic to rob one's "password", but also increases the User friendliness in human-computer interaction. Indexing and/or retrieving video facts and figures based on the appearances of particular individuals will be helpful for users such as report reporters, political researchers, and moviegoers. In this paper we focus on 3-D facial acknowledgement scheme and biometric facial recognition system.

Keywords: Introduction, facial recognition at a glance, Scope in India, Criticism, Future Enhancements, Conclusion.

I. Introduction

In today's networked world, the need to maintain the security of information or physical property is becoming both increasingly important and increasingly difficult. From time to time we hear about the crimes of credit card fraud, computer break-in by hackers, or security breaches in a company or government building. In most of these crimes, the criminals were taking advantage of a fundamental flaw in the conventional access control systems: the systems do not grant access by "who we are", but by "what we have", such as ID cards, keys, passwords, PIN numbers, or

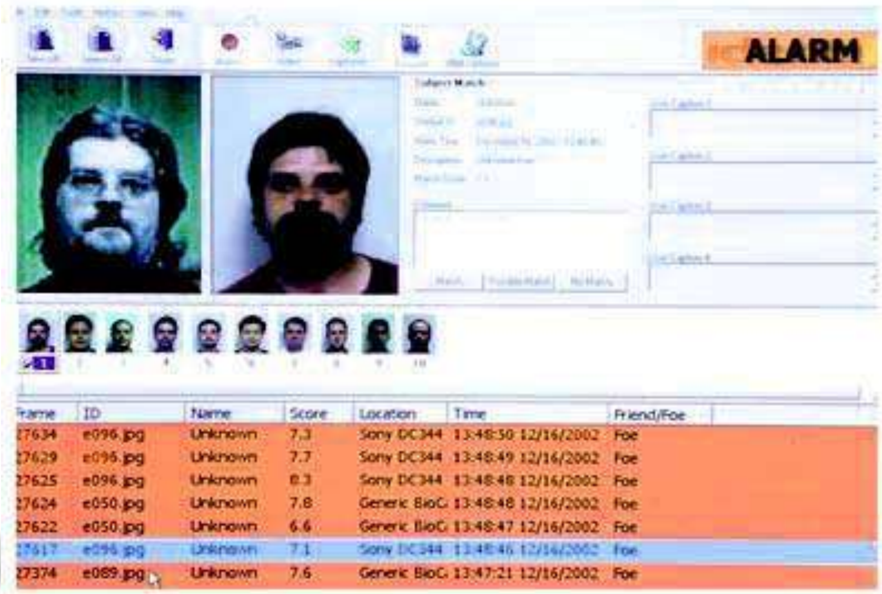
Mother's maiden name. None of these means are really defining us. Rather, they merely are means to authenticate us. It goes without saying that if someone steals, duplicates, or acquires these identity means, he or she will be able to access our data or our personal property any time they want. Recently, technology became available to allow verification of "true" individual identity. This technology is based in a field called "biometrics". Biometric access control are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as fingerprints or facial features, or some aspects of the person's behavior, like his/her handwriting style or keystroke patterns. Since biometric systems identify a person by biological characteristics, they are difficult to forge.

Among the various biometric ID methods, the physiological methods (fingerprint, face, DNA) are more stable than methods in behavioral category (keystroke, voice print). The reason is that physiological features are often non-alterable except by severe injury. The behavioral patterns, on the other hand, may fluctuate due to stress, fatigue, or illness. However, behavioral IDs have the advantage of being no intrusiveness. People are more comfortable signing their names or speaking to a microphone than placing their eyes before a scanner or giving a drop of blood for DNA sequencing.

Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. It has the accuracy of a physiological approach without being intrusive. For this reason, since the early 70's (Kelly, 1970), face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision. Numerous algorithms have been proposed for face recognition; for detailed survey please see Chellappa (1995) and Zhang (1997).
While network security and access control are it most widely discussed applications, face recognition has also proven useful in other multimedia information processing areas. Chan et al. (1998) use faces recognition techniques to browse video database to find out shots of particular people.
The system is to be automatic, robust and able to operate with minimal necessary interaction from the user.

II. Facial Technology At A Glance

Identix®, a company based in Minnesota, is one of many developers of facial recognition technology. Its software, FaceIt®, can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images. In order for this software to work, it has to know how to differentiate between a basic face and the rest of the background. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face.



Frame	ID	Name	Score	Location	Time	Friend/Foe
27634	e096.jpg	Unknown	7.3	Sony DC344	13:48:50 12/16/2002	Foe
27629	e096.jpg	Unknown	7.7	Sony DC344	13:48:49 12/16/2002	Foe
27625	e096.jpg	Unknown	8.3	Sony DC344	13:48:48 12/16/2002	Foe
27624	e050.jpg	Unknown	7.8	Generic BioC	13:48:48 12/16/2002	Foe
27622	e050.jpg	Unknown	6.6	Generic BioC	13:48:47 12/16/2002	Foe
27617	e096.jpg	Unknown	7.1	Sony DC344	13:48:46 12/16/2002	Foe
27374	e089.jpg	Unknown	7.6	Generic BioC	13:47:21 12/16/2002	Foe

Fig.1. Face IT software compares the face print with other images in the database. (Photo Identix Inc.)

Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Face It defines these landmarks as nodal points. Each human face has approximately 80 nodal points. Some of these measured by the software are:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw

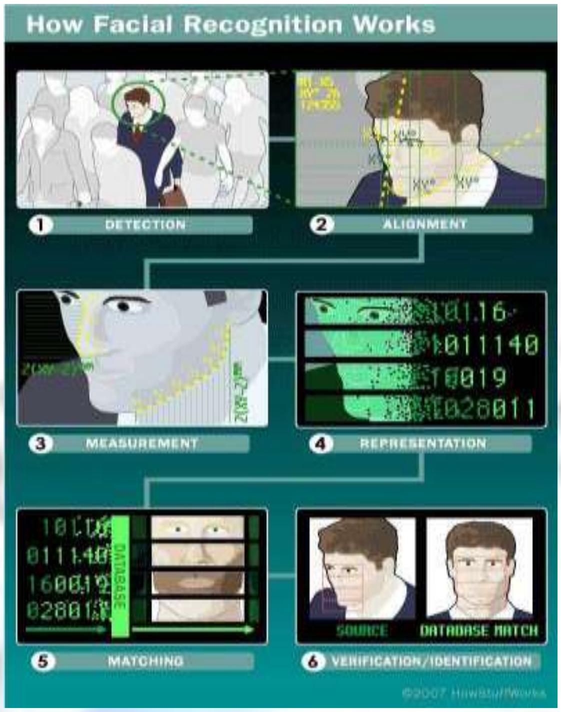
These nodal points are measured creating a numerical code, called a face print, representing the face in the database.
In the past, facial recognition software has relied on a 2D image to compare or identify another 2D Image from the database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. This created quite a problem.
In most instances the images were not taken in a controlled environment. Even the smallest changes in light or orientation could reduce the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure. In the next section, we will look at ways to correct the problem.

Facial Recognition

A newly-emerging trend in facial recognition software uses a
3D Model, which claims to provide more accuracy. Capturing a real-time 3-D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the

eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time. Using depth and an axis of measurement that is not affected by lighting, 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile).

Using the 3D software, the system goes through a series of steps to verify the identity of an individual.



a) Detection:-Acquiring an image can be accomplished by digitally scanning an existing photograph (2D) or by using a video image to acquire a live picture of a subject (3D).

b) Alignment: Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees. While with 2-D the head must be turned at least 35 degrees toward the camera.

c) Measurement:-The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.

d) Representation:-The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.

e) Matching: If the image is 3D and the database contains 3D images, then matching will take place.

f) Challenge currently facing databases that are still in 2D images. 3D provides a live, moving variable subject being compared to a flat, stable image. New technology is addressing this challenge. When a 3D image is taken, different points (usually three) are identified. For example, the outside of the eye, the inside of the eye and the tip of the nose will be pulled out and measured.

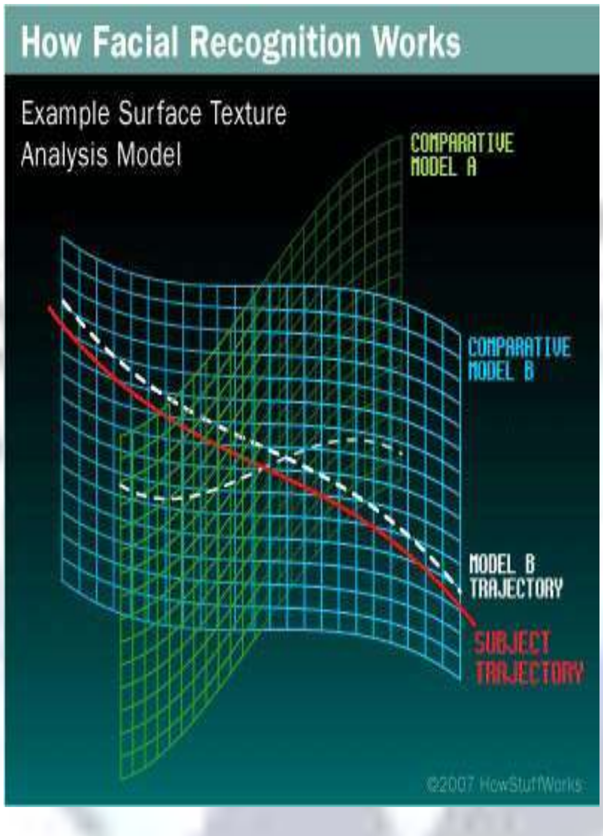
g) Verification or Identification: In verification, an image is matched to only one image in the database (1:1). For example, an image taken of a subject may be matched to an image in the Department of Motor Vehicles database to verify the subject is who he says he is. If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match. In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is. Next, we'll look at how skin biometrics can help verify matches.

III. Biometric Facial

The image may not always be verified or identified in facial Recognition alone. Identix® has the development of FaceIt®Argus uses skin biometrics, the uniqueness of skin texture, to yield even more accurate results.

The process, called Surface Texture Analysis, works much the same way facial recognition does. A picture is taken of a patch of skin, called a skin print. That patch is then broken up into smaller blocks. Using algorithms to turn the patch into a mathematical, measurable space, the system will then distinguish any lines and the skin texture. It can identify differences between twins, which is not yet possible using facial recognition alone.

Working of facial recognition
(Surface texture analysis model)



IV. Scope In India

I. In order to prevent the frauds of ATM in India, it is recommended to prepare the database of all ATM customers with the banks in India & deployment of high resolution camera and face recognition software at all ATMs. So, whenever user will enter in ATM his photograph will be taken to permit the access after it is being matched with stored photo from the database.

II. Duplicate voter are being reported in India. To prevent this, a database of all voters, of course, of all constituencies, is recommended to be prepared. Then at the time of voting the resolution camera and face recognition equipped of voting site will accept a subject face 100% and generates the recognition for voting if match is found.

III. Passport and visa verification can also be done using face recognition technology as explained above.

IV. Driving license verification can also be exercised face recognition technology as mentioned earlier.

V. To identify and verify terrorists at airports, railway stations and malls the face recognition technology will be the best choice in India as compared with other biometric technologies since other technologies cannot be helpful in crowdie places.

VI. In defense ministry and all other important places the face technology can be deployed for better security.

VII. This technology can also be used effectively in various important examinations such as SSC, HSC, Medical, Engineering, MCA, MBA, B- Pharmacy, Nursing courses etc. The examinee can be identified and verified using Face Recognition Technique.

VIII. In all government and private offices this system can be deployed for identification, verification and attendance.

IX. It can also be deployed in police station to identify and verify the criminals.

X. It can also be deployed vaults and lockers in banks for access control verification and identification of authentic users [1].

V. Criticism

Weaknesses

Face recognition is not perfect and struggles to perform under certain conditions. Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems." Other 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.

Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render in the system less effective. For instance: Canada now allows only neutral facial expressions in passport photos.

Effectiveness

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system having been Running for several years. "Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target." This information seems to conflict with claims that the system was credited with a 34% reduction in crime – which better explains why the system was then rolled out to Birmingham also.

An experiment by the local police department in Tampa, Florida, had similarly disappointing results. "Camera technology designed to spot potential terrorists by their facial characteristics at airports failed its first major test at Boston's Logan Airport".

Safe house International Limited, an Australian company, patented software including iMotion and iCount systems. The company claimed this system were able to track moving people and calculate the number of people in a crowd. After 9/11, the software was considered “commercially attractive” by the US administration. It was later revealed by David Mapley, a US shareholder of Safehouse International Limited) that the software actually never worked.

VI. Future Enhancements

A likely future application for facial acknowledgement schemes lies in retailing. A retail shop (for example, a food store shop) may have money lists equipped with cameras; the cameras would be aimed at the faces of customers, so images of customers could be obtained. The camera would be the primary means of recognizing the clientele, and if visual identification failed, the clientele could complete the buy by utilizing a PIN (personal identification number). After the money list had calculated the total sale, the face acknowledgement scheme would verify the identity of the clientele and the total amount of the sale would be deducted from the customer's bank account.

Hence, face-based retailing would supply convenience for retail customers, since they could go buying easily by displaying their faces, and there would be no need to convey debit cards, or other economic media. Wide-reaching submissions of face based retailing are likely encompassing retail stores, bistros, video theaters, car rental businesses, hotels.

VII. Conclusions

Face recognition technologies have been affiliated usually with very costly peak protected applications. Today the centre technologies have developed and the cost of equipment is going down spectacularly due to the integration and the increasing processing power. Certain applications of face acknowledgement expertise are now cost productive, dependable and highly accurate. As a outcome there are no technological or financial Obstacles for pacing from the navigate project to widespread deployment.

Though there are some flaws of facial acknowledgement system, there is a marvelous scope in India. This scheme can be effectively utilized in ATM's ,identifying duplicate voters, passport and visa verification, driving permit verification, in defense, comparable and other written tests, in authorities and personal sectors. Government and NGOs should focus and promote submissions of facial acknowledgement system in India in various fields by giving economical support and appreciation.

Face acknowledgement is a both challenging and important recognition technique. Amidst all the biometric techniques, face acknowledgement approach possesses one large benefit, which is its user-friendliness (or non-intrusiveness). In this paper, we have given an introductory survey for the face recognition expertise. We wish this paper can supply the readers a better comprehending about face acknowledgement.

References

[1]. MohanadHalaweh, Christine Fidler" Security Perception in Ecommerce:Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE.

[2]. Shazia Yasin, Khalid Haseeb. "Cryptography Based E-CommerceSecurity: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012

[3]. Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8No.5, May 2008.

[4]. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011).

[5]. Randy C. Marchany, Tom Wilson. A Keystroke Recorder Attack on a Client/Server Infrastructure. Proceedings of the Network Security '96 Conference, SANS Institute.

[6]. M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces," in Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 586–591. 1991.

[7]. A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces," in Proc. IEEE Conference on Computer Vision and Pattern Recognition, vol. 59, pp 748 – 760, May 1971.

[8]. M. A. Fischler and R. A. Elschlager, "The Representation and Matching of Pictorial Structures," IEEE Transaction on Computer, vol. C-22, pp. 67-92, 1973.

[9]. S. S. R. Abibi, "Simulating evolution: connectionist metaphors for studying human cognitive behaviour," in Proceedings TENCON 2000, vol. 1 pp 167-173, 2000.

[10]. Y. Cui, J. S. Jin, S. Luo, M. Park, and S. S. L. Au, "Automated Pattern Recognition and Defect Inspection System," in proc. 5th International Conference on Computer Vision and Graphical Image, vol. 59, pp. 768 – 773, May 1992.