International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 3, March-2014, pp: (482-486), Impact Factor: 1.252, Available online at: www.erpublications.com

Facial Recognition (A Review)

Yash Kaushik[1], Sukhwinder Singh[2]
Student[1], Assistant Professor[2]
[12]E & EC Dept., PEC University of Technology, Sector-12, Chandigarh, INDIA

Abstract: A facial recognition system is an application which is used for identifying or verifying a person from a digital image or a video frame. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is generally used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Areas such as network security, content indexing and retrieval, and video compression benefit from face recognition technology since people themselves are the main source of interest. Network access control via face recognition not only makes hackers virtually impossible to steal one's "password", but also increases the user friendliness in human-computer interaction. Although humans have always had the innate ability to recognize and distinguish between faces, yet computers only recently have shown the same ability. In the mid 1960s, scientists began work on using the computer to recognize human faces. Since then, facial recognition software has come a long way. In this article, I have explored the reasons behind using facial recognition, the products developed to implement this biometrics technique and also the criticisms and advantages that are bounded with it.

Keywords:- Biometrics, Facial, Scope, Privacy, Texture Analysis.

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. Crimes involving credit card frauds, security breaches of government organizations have become commonplace. In most of such crimes, the criminals take 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 and PIN numbers . These objects merely authenticate us and if stolen, can lead to theft of our personal data. Biometrics is a step forward to tackle this problem. 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 behaviour, 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 non intrusive. 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, face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision.

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. But this technology works on the principle that it should be able to differentiate a face from the background of the image.

Each face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. FaceIt 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 a hindrance since most images clicked were not suitable. Hence even the smallest changes in light or orientation reduced the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure.

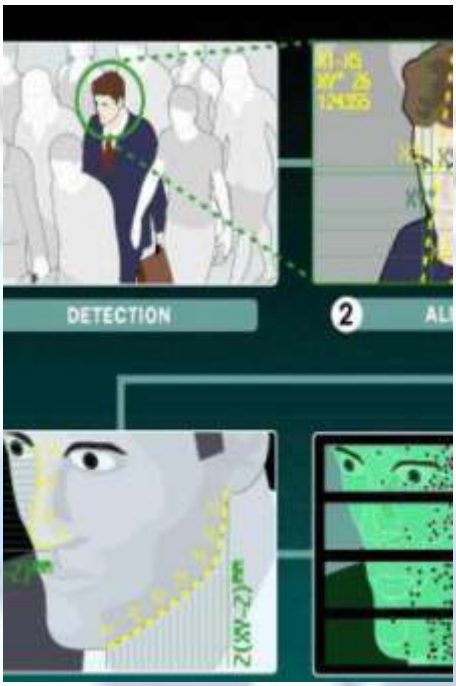

Fig. 1: 3D Facial Recognition

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.

(1)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).

(2)Alignment: Once it detects a face, the system determines the head's position, size and pose. 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.

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

(4)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.

(5) Matching: If the image is 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a 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.
Once those measurements are in place, an algorithm (a step-by step procedure) will be applied to the image to convert it to a2D image. After conversion, the software will then compare the image with the 2D images in the database to find a potential match.

(6) Verification or Identification: In verification, an image is matched to only one image in the database. 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 (1:1). If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match (1: N). In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is.

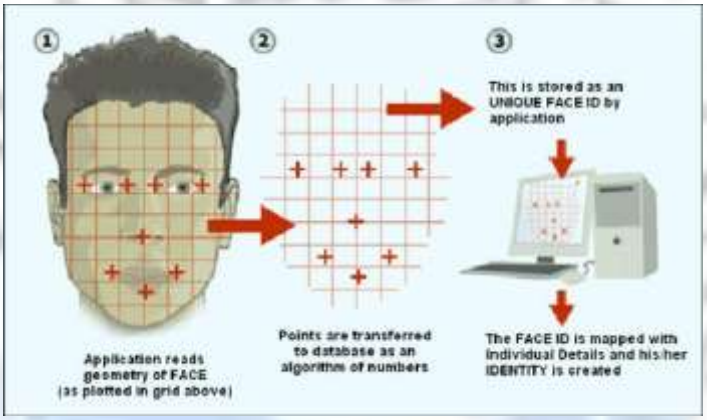

Fig.2

BIOMETRIC FACIAL RECOGNITION

The image may not always be verified or identified in facial recognition alone. Identix has created a new product to help with precision. 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, pores and the actual skin texture. It can identify differences between identical twins, which is not yet possible using facial recognition software alone.

According to Identix, by combining facial recognition with surface texture analysis, accurate identification can increase by 20 to 25 percent FaceIt currently uses three different templates to confirm or identify the subject: vector, local feature analysis and surface texture analysis.

• The vector template is very small and is used for rapid searching over the entire database primarily for one to- many searching.
• The Local Feature Analysis (LFA) template performs a secondary search of ordered matches following the vector template.
• The Surface Texture Analysis (STA) is the largest of the three. It performs a final pass after the LFA template searches, relying on the skin features in the image, which contains the most detailed information.

By combining all three templates, FaceIt has an advantage over other systems. It is relatively insensitive to changes in expression, including blinking, frowning or smiling and has the ability to compensate for moustache or beard growth and the appearance of eyeglasses. The system is also uniform with respect to race and gender. Among the different biometric techniques facial recognition may not be the most reliable and efficient but its great advantage is that it does not require aid from the test subject. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd. Other biometrics like fingerprints, iris, and speech recognition cannot perform this kind of mass scanning. However, questions have been raised on the effectiveness of facial recognition software in cases of railway and airport security.

III. SCOPE IN INDIA

1. 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.

2. Duplicate voters are being reported in India. At the time of voting the resolution camera and face recognition equipped of voting site will accept a subject face and generate the recognition for voting if match is found.

3. Passport and visa verification can also be done using face recognition technology.

4. Driving license verification can also be exercised by face recognition technology.

5. In defence ministry and other important places the face technology can be deployed for better security.

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

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

IV. CRITICISM

A. 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.

B. EFFECTIVENESS

(a) 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."

(b) 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".

(c) Safehouse 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.

C. PRIVACY ISSUES

Many citizens express concern that their privacy is being compromised by the use of surveillance technologies by corporations and the state. Some fear that it could lead to a "total surveillance society," with the government and other authorities having the ability to know the whereabouts and activities of all citizens around the clock. This knowledge has, is and could continue to be deployed to prevent the lawful exercise of rights of citizens to criticize those in office, specific government policies or corporate practices. Many centralized power structures with such surveillance capabilities have abused their privileged access to maintain control of the political and economic apparatus and curtail populist reforms. Facial recognition can be used not just to identify an individual, but also to unearth other personal data associated with an individual – such as other photos featuring the individual, blog posts, social networking profiles, Internet behavior, travel patterns, etc. – all through facial features alone. Moreover, individuals have limited ability to avoid or thwart facial recognition tracking unless they hide their faces. This fundamentally changes the dynamic of day-to-day privacy by enabling any marketer, government agency, or random stranger to secretly collect the identities and associated personal information of any individual captured by the facial recognition system.

V. FUTURE ENHANCEMENTS

A possible future application for facial recognition systems lies in retailing. A retail store (for example, a grocery store) may have cash registers equipped with cameras; the cameras would be aimed at the faces of customers, so pictures of customers could be obtained. The camera would be the primary means of identifying the customer, and if visual identification failed, the customer could complete the purchase by using a PIN (personal identification number). After the cash register had calculated the total sale, the face recognition system would verify the identity of the customer and the total amount of the sale would be deducted from the customer's bank account. Hence, face-based retailing would provide convenience for retail customers, since they could go shopping simply by showing their faces, and there would be no need to bring debit cards, or other financial media.

VI. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologies have evolved and the cost of equipment is going down dramatically due to the integration and the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment.
Though there are some weaknesses of facial recognition system, there is a tremendous scope in India. This system can be effectively used in ATM's ,identifying duplicate voters, passport and visa verification, driving license verification, in defence, competitive and other exams, in governments and private sectors.
Government and NGOs should concentrate and promote applications of facial recognition system in India in various fields by giving economical support and appreciation. Face recognition is a both challenging and important recognition technique. Among all the biometric techniques, face recognition approach possesses one great advantage, which is its user-friendliness (or non-intrusiveness). In this paper, we have given an introductory survey for the face recognition technology. We hope this paper can provide the readers a better understanding about face recognition.

VII. ACKNOWLEDGEMENT

I would like to thank our respected professor who gave me the opportunity to work on a review paper and under his guidance. I was able to achieve this. I would like to thank him for his help and guidance at every point. I would also like to thank my friends who helped me in choosing the topic.

REFERENCES

[1]. http://arxiv.org/abs/1005.4263.
[2]. http://www.inform.nu/Articles/Vol3/v3n1p01-07.pdf
[3]. http://www.technologyreview.com/Infotech/18796/?a=f.
[4]. http://www.cs.technion.ac.il/~ron/PAPERS/BroBroKimIJCV05.pdf.
[5]. Face Recognition: a Summary of 1995 – 1997 by Thomas Fromherz