# ATM SECURITY USING FACE RECOGNITION

# <sup>1</sup>RAHUL. K, <sup>2</sup>ARVIND.S, <sup>3</sup>B.PRASHANTH, <sup>4</sup>N.BALAJI ABHISHEK

<sup>1,3,4</sup>4<sup>th</sup> Year, R.M.K Engineering College, Electrical and Electronics Engineering <sup>2</sup>4<sup>th</sup> Year, R.M.D Engineering College, Electrical and Electronics Engineering

**Abstract-** Government agencies are investing a considerable amount of resources into improving security systems as result of recent terrorist events that dangerously exposed flaws and weaknesses in today's safety mechanisms. Badge or password based authentication procedures are too easy to hack. Biometrics represents a valid alternative but they suffer of drawbacks as well.

# I. INTRODUCTION



• Iris scanning, for example, is very reliable but too intrusive; fingerprints are socially accepted, but not applicable to non-consentient people.On the otherhand, face recognition represents a good compromise between what's socially acceptable and what's reliable, even when operating under controlled conditions.

• In last decade, many algorithms based on linear/non-linear methods, neural networks, wavelets, etc. have been proposed. Nevertheless, face recognition vendor test 2002 shown that most of these approaches encountered problems in outdoor conditions. This lowered their reliability compared to state of the art biometrics.

## **II. WHAT IS FACE RECOGNITION?**

• Face recognition technology is the least intrusive and fastest biometric technology. It works

with the most obvious individual identifier – the human faces.

• Instead of requiring people to place their hand on a reader or precisely position their eye in front of a scanner, face recognition systems unobtrusively take pictures of people's faces as they enter a defined area.

It's 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 photo. FaceIt software compares the face print with other images in the database. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face. Every face has numerous, distinguishable landmarks, the different peaks and valleys that makeup 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 line
- These nodal points are measured creating a numerical code, called a face print, representing the face in the database.

#### **III. TECHNOLOGY**

• Our technology is based on neural computing and combines the advantages of elastic and neural networks. Neural computing provides technical information processing methods that are similar to the biological systems, such as human brain. Elastic networks can compare facial landmarks even if images are not identical, as is practically always the case in real world situations.

#### **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.

## **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 3D 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 – identify the subject. These areas are all unique and don't change overtime.
Using 3D software the system goes through a series of steps to verify the identity of an individual.

## **Detection:**

• Acquiring an image can be accomplished by digitally scanning existing photographs (2D) or by using a video image to acquire a live picture of a subject.



#### IV. MATCHING

• If the image 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a challenged currently facing database that is 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 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 will be applied to the image to convert it to a 2D image. After conversion, the software will then

compare the image with the 2D images in the database to find a potential match.



# V. 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.

#### VI. SURFACE TEXTURE ANALYSIS

• The image may not always be verified or identified in facial recognition alone. Identic 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.

• The vector template is very small and is used for rapid searching over the entire database primarily for 1 to many searching.

• The local feature analysis(LFA) template performs a secondary search of ordered matches following the vector template.

• The STA is the largest of the three. It performs a final pass after the LFA search relying on the skin features in the image, which contains the most detailed information.

- There are some factors that could get in the way of recognition, including:
- Significant glare on eyeglasses or wearing sunglasses.
- Long hair obscuring the central part of the face.
- Poor lighting that would cause the face to the over or under exposed.
- Lack of resolution(image was taken too far away)
- Future uses of facial recognition systems:
- The ideal solution

- All of this makes face recognition ideal for high traffic areas open to the general public, such as:
  - Airports and railway stations
  - Casinos
  - Cash points
  - Stadiums
  - Public transportation
  - Financial institutions
  - Government offices
  - Business of all kinds

In the past the primary users of facial recognition software have been law enforcement agencies, who used the system to capture random faces in crowds. The US Government has recently began a program called US - VISIT(United States Visited and Immigrant Status Indicator Technology), aimed at foreign travellers gaining entry to the united states. When a foreign traveller receives his visa, he will submit fingerprints and have his photograph taken. The fingerprints and photographs are checked against a database of known criminals and suspected terrorists. When the traveller arrives in the united states at the port of entry, those same fingerprints photographs will beused to verify that the person who received the visa is the same person attempting to gain entry.

#### VIII. HARD TO FOOL

• Face recognition is also very difficult to fool. It works by comparing facial landmarks – specific proportions and angles of defined facial features which cannot easily be concealed by beards, eye glasses or makeup.

• There are now many more situations where the software is becoming popular.

• As a systems become less expensive, making their use more widespread.

• They are now compatible with cameras and computers that are already in use by banks and airports. Registered Traveller program will provide speedy security screening form passengers who volunteer information. At the airport there will be specific lines for the registered traveller to go through that will move more quickly, verifying the traveller by their facial features.

• Other potential applications include ATM and check- cashing kiosk captures a digital image of him.

• By using the facial recognition software, there's no need for a picture ID, bank card or personal identification number (PIN) to verify a customer's identity. This way Business can prevent fraud from occurring.

#### CONCLUSION

As with many developing technologies, the incredible potential of facial recognition comes with some drawbacks, but manufacturers are striving to enhance the usability and accuracy of the systems. Face recognition promises latest security invents in the upcoming trends based on biometrics and pattern matching techniques and algorithms.

#### REFERENCES

- [1]. "Using Your body as key legal aspects of biometrics". http://cwis.kub.nl/~frw/people/kraling/content /biomet.htm
- [2]. Y.Adini, Y.Moses and S.Ullman, "Face recognition:theproblem of compensating for changes in illumination direction,"IEEETrans.PatternAnal.Machine Intel., vol.19,pp.721 – 732, july 1997.

\*\*\*