Journal of Advances in Science and Technology

Vol. VIII, Issue No. XVI, February-2015, ISSN 2230-9659

A REVIEW ON APPLICATIONS AND CHALLENGES OF FACE RECOGNITION SYSTEM: A BIOMETRIC TECHNOLOGY

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

Journal of Advances in Science and Technology
Vol. VIII, Issue No. XVI, February-2015, ISSN 2230-9659

A Review on Applications and Challenges of Face Recognition System: A Biometric Technology

Narayan T. Deshpande[1] Dr. S. Ravishankar[2]

[1]Associate Professor, Department of E & C, BMS College Of Engineering, Bangalore

[2]Professor, Department of E & C, R V College of Engineering, Bangalore

Abstract – Face recognition has long been a goal of computer vision, but only in recent years reliable automated face recognition has become a realistic target of biometrics research. New algorithms, and developments spurred by falling costs of cameras and by the increasing availability processing power have led to practical face recognition systems. These systems are increasingly being deployed in a wide range of practical applications, and future improvements promise to spread the use of face recognition further still.

Face recognition presents a challenging problem in the field of image analysis and computer vision, and as such has received a great deal of attention over the last few years because of its many applications in various domains.

This paper focuses on the meaning of face recognition system, human face features that use to identify the face, face recognition types including two- dimensional system (2D) and three-dimensional system(3D)& the explanation of three-dimensional recognition procedures We also explained our new idea for recognizing the human face.

Face recognition has been employed in various security related applications such as surveillance, mug shot identification, e-passport, and access control. Despite its recent advancements, privacy concern is one of several issues preventing its wider deployment. In this paper, we address the privacy concern for a self-exclusion scenario of face recognition, through combining face recognition with a simple biometric encryption scheme called helper data system. The combined system is described in detail with focus on the key binding procedure. Experiments are carried out on the CMU PIE face database. The experimental results demonstrate that in the proposed system, the biometric encryption module tends to significantly reduce the false acceptance rate while increasing the false rejection rate.

----------♦----------

INTRODUCTION

Recognizing faces is something that people usually do effortlessly and without much conscious thought, yet it has remained a difficult problem in the area of computer vision, where some 20 years of research is just beginning to yield useful technological solutions. As a biometric technology, automated face recognition has a number of desirable properties that are driving research into practical techniques.

The problem of face recognition can be stated as 'identifying an individual from images of the face' and encompasses a number of variations other than the most familiar application of mug shot identification. One notable aspect of face recognition is the broad interdisciplinary nature of the interest in it: within computer recognition and pattern recognition; biometrics and security; multimedia processing; psychology and neuroscience. It is a field of research notable for the necessity and the richness of interaction between computer scientists and psychologists.

The automatic recognition of human faces spans a variety of different technologies. At a highest level, the technologies are best distinguished by the input medium that is used, whether visible light, infra-red or 3-dimensional data from stereo or other range-finding technologies. Thus far, the field has concentrated on still, visible-light, photographic images, often black and white, though much interest is now beginning to

be shown in the recognition of faces in colour video. Each input medium that is used for face recognition brings robustness to certain conditions, *e.g.* infra-red face imaging is practically invariant to lighting conditions while 3-dimensional data in theory is invariant to head pose. Imaging in the visible light spectrum, however, will remain the preeminent domain for research and application of face recognition because of the vast quantity of legacy data and the ubiquity and cheapness of photographic capture equipment.

Now a days with the network world, the way for crime is become easier than before. Because of this reason, network security has become one of the biggest concerns facing today's IT departments. We heard a lot about hackers and crackers ways to steal any password or pin code, crimes of ID cards or credit cards fraud or security breaches in any important building and then reach any information or important data from any organization or company. These problems allow us to know the need of strong technology to secure our important data.

This technology is based on a technique called “biometrics". Biometric is a form of bioinformatics that uses biological properties to identify people. Since biometric systems identify a person by biological characteristics, they are difficult to fake. Examples of biometrics are iris scanning, signature authentication, voice recognition and hand geometry.

Face recognition is one example of biometric and it is use the character of the face to identify a person. Face recognition has drawn attention in computer vision at 1970 and the rest time the system of face recognition used was at 2001 for the purpose of reducing the crimes but this system fails to recognize the clear picture of any thief because the thieves were wearing a mask.

Face recognition techniques can be broadly divided into three categories based on the face data acquisition methodology: methods that operate on intensity images; those that deal with video sequences; and those that require other sensory data such as 3D information or infrared imagery.

Face recognition has a wide range of applications, such as surveillance, access control, e-passport, and human-computer interaction. In particular, face recognition is one of the three identification methods used in e-passports. Furthermore, facial features scored the highest compatibility among the six biometric attributes in a machine readable travel documents (MRTD) system based on several evaluation factors including enrollment, renewal, machine requirements, and public perception. This is largely due to the fact that compared to other popular biometric technologies: face recognition is non-intrusive and easy to use.

The work presented in this paper has been partially supported by the

Ontario Lottery and Gaming Corporation (OLG). The views, opinions, and findings contained in this paper are those of the authors and should not be construed as official positions, policies, or decisions of the OLG, unless so designated by other official documentation.

The authors would like to thank Mr. Klaus Peltsch from the Ontario Lottery and Gaming Corporation, and Dr. Ann Cavoukian and Dr. Alex Stoianov from the Information and Privacy Commissioner of Ontario for many useful discussions.

Although face recognition has made tremendous progress in the past two decades, there have been several concerns preventing its wider deployment, such as the effectiveness in field test, the performance under uncontrolled conditions, and privacy concern. Privacy concern arises when there are large centralized databases of biometric passwords and there are risks of identity theft and privacy leaks. Consequently, biometric encryption has emerged to address this concern.

The objective is to deploy biometrics in a privacy-enhancing way that minimizes the possibility of abuse, maximizes individual control, and ensures full functionality of the systems in which biometrics are used. For face recognition with biometric encryption, rather than storing one’s facial image in a database, the facial image is used to encrypt (code) some other information such as a cryptographic key and only the biometrically-encrypted data is stored. This removes the need to collect and store actual biometric data in database and most privacy concerns associated with centralized databases are eliminated.

FACIAL TECHNOLOGY AT A GLANCE

Every 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 line

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.

A. 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.

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 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-bystep procedure) 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.

f) *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 (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. Next, we'll look at how skin biometrics can help verify matches.

B. 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 Face It ® 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 oneto-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 search, 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 mustache 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.

APPLICATIONS

Face recognition is used for two primary tasks:

1. Verification (one-to-one matching): When presented with a face image of an unknown individual along with a claim of identity, ascertaining whether the individual is who he/she claims to be.

2. Identification (one-to-many matching): Given an image of an unknown individual, determining that person's identity by comparing (possibly after encoding) that image with a database of (possibly encoded) images of known individuals.

There are numerous application areas in which face recognition can be exploited for these two purposes, a few of which are outlined below:

- Security (access control to buildings, airports/seaports, ATM machines and border checkpoints; computer/ network security; email authentication on multimedia workstations).

- Surveillance (a large number of CCTVs can be monitored to look for known criminals, drug offenders, etc. and authorities can be notified when one is located; for example, this procedure was used at the Super Bowl 2001 game at Tampa, Florida; in another instance, according to a CNN report

- General identity verification (electoral registration, banking, electronic commerce, identifying newborns, national IDs, passports, drivers' licenses, employee IDs).

- Criminal justice systems (mug-shot/booking systems, post-event analysis, forensics).

- Image database investigations (searching image databases of licensed drivers, benefit recipients, missing children, immigrants and police bookings).

- "Smart Card" applications (in lieu of maintaining a database of facial images, the face-print can be stored in a smart card, bar code or magnetic stripe, authentication of which is performed by matching the live image and the stored template) .

- Multi-media environments with adaptive human computer interfaces (part of ubiquitous or context- aware systems, behavior monitoring at childcare or old people's centers, recognizing a customer and assessing his needs).

- Video indexing (labeling faces in video).

- Witness face reconstruction.

FACE AS A BIOMETRIC

Face recognition for recent surveys) has a number of strengths to recommend it over other biometric modalities in certain circumstances, and corresponding weaknesses that make it an inappropriate choice of biometric for other applications. Face recognition as a biometric derives a number of advantages from being the primary biometric that humans use to recognize one another. Some of the earliest identification tokens, *i.e.* portraits, use this biometric as an authentication pattern. Furthermore it is well-accepted and easily understood by people, and it is easy for a human operator to arbitrate machine decisions — in fact face images are often used as a human-verifiable backup to automated fingerprint recognition systems.

Because of its prevalence as an institutionalized and accepted guarantor of identity since the advent of photography, there are large legacy systems based on face images—such as police records, passports and driving licenses—that are currently being automated. Video indexing is another example of legacy data for which face recognition, in conjunction with speaker identification, is a valuable tool.

Face recognition has the advantage of ubiquity and of being universal over other major biometrics, in that everyone has a face and everyone readily displays the face. (Whereas, for instance, fingerprints are

captured with much more difficulty and a significant proportion of the population has fingerprints that cannot be captured with quality sufficient for recognition.) Uniqueness, another desirable characteristic for a biometric, is hard to claim at current levels of accuracy. Since face shape, especially when young, is heavily influenced by genotype, identical twins are very hard to tell apart with this technology.

With some configuration and co-ordination of one or more cameras, it is be more or less possible to acquire face images without active participation of the subject. Such passive identification might be desirable for customization of user services and consumer devices, whether that be opening a house door as the owner walks up to it, or adjusting mirrors and car seats to the driver's presets when sitting down in their car.

Surveillance systems rely on passive acquisition by capturing the face image without the cooperation or knowledge of the person being imaged. Face recognition also has the advantage that the acquisition devices are cheap and are becoming a commodity (though this is not true for non-visible wavelength devices and some of the more sophisticated face recognition technologies based on 3-dimensional data).

The main drawbacks to face recognition are its current relatively low accuracy (compared to the proven performance of fingerprint and iris recognition) and the relative ease with which many systems can be defeated (Section 4.2.1). Finally, there are many attributes leading to the variability of images of a single face that add to the complexity of the recognition problem if they cannot be avoided by careful design of the capture situation. Inadequate constraint or handling of such variability inevitably leads to failures in recognition.

These include:

Physical changes: facial expression change; aging; personal appearance (make-up, glasses, facial hair, hairstyle, disguise).

Acquisition geometry changes: change in scale, location and in-plane rotation of the face (facing the camera) as well as rotation in depth (facing the camera obliquely, or presentation of a profile, not full-frontal face).

Imaging changes: lighting variation; camera variations; channel characteristics (especially in broadcast, or compressed images).

The main challenges of face recognition today are handling rotation in depth and broad lighting changes, together with personal appearance changes. Even under good conditions, however, accuracy needs to be improved.

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. 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.

2. 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.

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

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

5. 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 crowdy places.

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

7. 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.

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

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

10. It can also be deployed vaults and lockers in banks for access control verification and identification of authentic users.

11. Present bar code system could be completely replaced with the face recognition technology as it is a better choice for access & security since the barcode could be stolen by anybody else.

CONCLUSION

Face recognition is a technology just reaching sufficient maturity for it to experience a rapid growth in its practical applications. Much research effort around the world is being applied to expanding the accuracy and capabilities of this biometric domain, with a consequent broadening of its application in the near future. Verification systems for physical and electronic access security are available today, but the future holds the promise and the threat of passive customization and automated surveillance systems enabled by face recognition.

As you can see, face recognition system is very important in our daily life. It is possesses a really great advantage. Among the whole types of biometric, face recognition system is the most accurate. Research has been conducted vigorously in this area for the past four decades or so, and though huge progress has been made, encouraging results have been obtained and current face recognition systems have reached a certain degree of maturity when operating under constrained conditions; however, they are far from achieving the ideal of being able to perform adequately in all the various situations that are commonly encountered by applications utilizing these techniques in practical life.

In conclusion, biometrics technology is a new technology for most of us because it has only been implemented in public for short period of time. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

REFERENCES

- K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Security," A. K. Jain, R. Bolle, and S. Pankanti, Eds.: Kluwer Academic Publishers, 1999.

- Chin-Seng Chua, Feng Han, and Yeong-Khing Ho. 3D Human Face Recognition using Point Signature. In International Conference on Face and Gesture Recognition, pages 233–238, 2000.

- Duane M. Blackburn, Mike Bone, and P. Jonathon Phillips. Facial Recognition Vendor Test 2000 Evaluation Report. Technical Report, Department of Defence Counterdrug Technology Development Program Office, February 2001.

- H. Moon, "Biometrics Person Authentication Using Projection- Based Face Recognition System in Verification Scenario," in International Conference on Bioinformatics and its Applications. Hong Kong, China, 2004, pp.207-213.

- H. Veronica.(2001) \Biometrics: Face Recognition Technology".GIAC, SANS Institute. pp.2-3. Accessed at March 7th, 2011.

- Roberto Brunelli and Tomaso Poggio. Face Recognition: Features versus Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(10):1042–1052, October 1993.

- Stan Z. Li and Anil K. Jain, “Introduction,” in Handbook of Face Recognition, Stan Z. Li and Anil K. Jain, Eds. 2004, pp. 1–11, Springer-Verlag.

- Xiaoguang Lu & Anil K. Jain.\Multimodal Facial Feature Extraction for Automatic 3D Face Recognition" Accessed at April 12th, 2011.