World Journal of Engineering Research and Technology
WJERT
www.wjert.org

A REVIEW ON BIOMETRIC SECURITY SYSTEMS

Dr. Samir Kumar Bandyopadhyay[1], Sanjay Nag[2] and Nabanita Basu[2]

[1]Professor, Department of Computer Science & Engineering, University of Calcutta.

[2]Research Scholar, Department of Computer Science & Engg., University of Calcutta.

Article Received on 15/12/2015 **Article Revised on 08/01/2016** **Article Accepted on 30/01/2016**

***Correspondence for Author**
Prof. (Dr.) Samir Kumar Bandyopadhyay
Professor, Department of Computer Science & Engineering, University of Calcutta, India.
skb1@vsnl.com

ABSTRACT

Two of the most popular biometric security systems work on the model of either fingerprint recognition or palm vein technology. The first type of biometric security device uses the fingerprint recognition technique where a highly sensitive camera captures the thumb prints of the individuals. The person has to place his thumb over the scanner, which then captures the fingerprint and matches it with existing records. The biometric device is mostly used for fingerprint recognition, fingerprint verification, fingerprint authentication, fingerprint scanning and fingerprint matching applications. The device is so designed that it is able to capture dry, wet and blurred images as well.

The other kind of biometric security device with palm vein technology uses an infrared sensor that identifies an individual's vein pattern. This method works on a very sensitive model of authentication technique. This type of biometric security system does not require being touched; the user has to place the hand over a few inches on the scanner. Palm veins are unique to every individual and with the help of infrared sensor; the scanner captures this never-changing pattern. The biometric device is also an option because of its hygiene mode. In traditional biometric security systems, the device was required to be touched, making way for sanitary issues that are now dealt with, Both these fingerprint access control devices incorporate those features of the humans that do not change or are not prone to any manipulation. Factors like age, wounds, cuts, change in skin colour do not make up for any difference unlike the earlier counterparts of these biometric devices. This paper discusses general biometric security systems. This paper reviews different biometric security systems.

KEYWORDS: Biometrics, Feature Extraction, and Biometrics Recognition System.

INTRODUCTION

Biometrics generally refers to the study of measurable biological characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

There are several types of biometric identification schemes:

- **face**: the analysis of facial characteristics
- **fingerprint**: the analysis of an individual's unique fingerprints
- **hand geometry**: the analysis of the shape of the hand and the length of the fingers
- **retina**: the analysis of the capillary vessels located at the back of the eye
- **iris**: the analysis of the coloured ring that surrounds the eye's pupil
- **signature**: the analysis of the way a person signs his name.
- **vein**: the analysis of pattern of veins in the back if the hand and the wrist
- **voice**: the analysis of the tone, pitch, cadence and frequency of a person's voice.

The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enrol) followed by a Verification or Identification process.

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrolment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.

Review Works

A key advantage of biometric authentication is that biometric data is based on physical characteristics that stay constant throughout one's lifetime and are difficult (some more than others) to fake or change. Biometric identification can provide extremely accurate, secured access to information; fingerprints, palm vein and iris scans produce absolutely unique data sets (when done properly). Automated biometric identification can be done rapidly and uniformly, without resorting to documents that may be stolen, lost or altered. It is not easy to determine which method of biometric data gathering and reading does the "best" job of ensuring secure authentication. Each of the different methods has inherent advantages and disadvantages. Some are less invasive than others; some can be done without the knowledge of the subject; others are very difficult to fake.[1]

Yuhang Ding, Dayan Zhuang and Kejun Wang, July 2005,[2] have shown the theoretical foundation and difficulties of hand vein recognition, at first. Then, the threshold segmentation method and thinning method of hand vein image are deeply studied and a new threshold segmentation method and an improved conditional thinning method are proposed. The

method of hand vein image feature extraction based on end points and crossing points is studied initially, and the matching method based on distances is used to match vein images.

Shi Zhao, Yiding Wang and Yunhong Wang, proposed [3] a biometric technique using hand-dorsa, extracting vein structures. For conventional algorithm, it is necessary to use high-quality images, which demand high-priced collection devices. The proposed method makes using low-cost devices possible. The results shown that they could extract the vein networks as successfully as using high-quality images.

Masaki Watanabe, Toshio Endoh, Morito Shiohara, and Shigeru [4] have shown a biometric authentication using contactless palm vein authentication device that uses blood vessel patterns as a personal identifying factor. Implementation of these contactless identification systems enables applications in public places or in environments where hygiene standards are required, such as in medical applications. In addition, sufficient consideration was given to individuals who are reluctant to come into direct contact with publicly used devices.

Zhenan Sun, Yunhong Wang, Tieniu Tan, and Jiali Cui, in 2005, proposed [5] to overcome the limitations of local feature based classifiers (LFC). In addition, in order to recognize various iris images efficiently a novel cascading scheme is proposed to combine the LFC and an iris blob matcher. When the LFC is uncertain of its decision, poor quality iris images are usually involved in intra-class comparison. Then the iris blob matcher is resorted to determine the input iris identity because it is capable of recognizing noisy images. Extensive experimental results demonstrate that the cascaded classifiers significantly improve the system's accuracy with negligible extra computational cost.

Different Methods

We will now discuss different biometric security devices in the subsequent paragraphs.

Face Detection

Human face detection has drawn considerable attention in the past decades as it is one of the fundamental problems in computer vision. Given a single image, the ideal face detection should identify and locate all faces regardless of its three-dimensional position, orientation, and lighting conditions. The existing face detection techniques can be classified into four categories, namely, knowledge-based methods, feature invariant approaches, template matching methods, appearance based methods.[7]

Human face detection and segmentation is an active research area until recently. This field of research plays an important role in many applications such as face identification system, face tracking, video surveillance and security control system, and human computer interface.

Those applications often require segmented human face which is ready to be processed. There are many factors that influence the success of human face detection and segmentation. Those factors include complex colour background, condition of illumination, change of position and expression, rotation of head, and distance between camera and subject.

Face detection is a sub branch of object detection. The human face is a dynamic object and has a high degree of variability in its appearance, which makes face detection a difficult problem in computer vision.

Images containing faces are essential to intelligent vision-based human computer interaction, and research efforts in face processing include face recognition, face tracking, pose estimation, and expression recognition. However, many reported methods assume that the faces in an image or an image sequence have been identified and localized. To build fully automated systems that analyse the information contained in face images, robust and efficient face detection algorithms are required.

Given a single image, the goal of face detection is to identify all image regions which contain a face regardless of its three-dimensional position, orientation, and lighting conditions. Such a problem is challenging because faces are non- rigid and have a high degree of variability in size, shape, colour, and texture. Numerous techniques have been developed to detect faces in a single image.

Face detection and localization is the task of checking whether the given input image contains any human face, and if so, returning the location of the human face in the image. The wide variety of applications and the difficulty of face detection have made it an interesting problem for the researchers in recent years.

Face detection is difficult mainly due to a large component of non-rigidity and textural differences among faces. The great challenge for the face detection problem is the large number of factors that govern the problem space. The long list of these factors include the pose, orientation, facial expressions, facial sizes found in the image, luminance conditions,

occlusion, structural components, gender, ethnicity of the subject, the scene and complexity of image's background. Whenever we are detecting a face, we have to concern about its scale, rotation, pose, expression, presence or absence of some structural component, occlusion, illumination variation and image condition. We explain them briefly below.

Scale: An image can have multiple numbers of faces with different scale, which means the size (height and width) of a face may differ with other faces in the image.
Rotation: Image can have face images with different angle.
Pose: Face images dramatically change according to pose direction of camera, and some features can partially or wholly disappear.
Expression: A face image can have various expressions, which may affect the spatial characteristic of various facial features.
Presence or absence of some structural components: Presence of some structural components like mustaches, beards and glasses can make the face detection process very difficult.
Occlusion: Sometimes, faces can be partially occluded by other object.
Illumination variation: An image consists of various objects with different lighting effect.
Image noise: Presence of noise in the image due to some factors like the environment, characteristic of camera may affect the face detection process.

Finger Print Authentication

Automatic fingerprint recognition has been widely applied as a personal identification tool and biometrics applications due to their reliability and uniqueness features. One of the important tasks for any large scale fingerprint recognition system is fingerprint classification. Classifying a fingerprint images is a very difficult pattern recognition problem, due to the small interclass variability, the large intra-class variability, the presence of noise and the ambiguous properties of fingerprints. An accurate classification algorithm can greatly reduce the number of comparisons during fingerprint retrieval and consequently speeded up the identification process. Over the past few decades, a significant amount of researches and techniques has been proposed for distinguishing fingerprint classes.

Fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including

things like moiréfringe patterns and ultrasonics. Some verification approaches can detect when a live finger is presented; some cannot.[8]

A greater variety of fingerprint devices is available than for any other biometric. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance — despite the common — criminal stigma.

Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices

Hand geometry

Hand Geometry involves analyzing and measuring the shape of the hand. This biometric offers a good balance of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system.

Despite the fact that the use of hands as biometric evidence is not very new, and that one can witness an increasing number of commercial products being deployed, the documentation in the literature is scarcer as compared to other modalities like face or voice. However, processing of hands requires less complexity in terms of imaging conditions, for example a relatively simple sensor such as a flatbed scanner would suffice.[6]

Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Ease of integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric projects.

As the contact of present computer systems on everyday life increases, human computer Communications has become more and more significant in our everyday lives. Hand area based recognitions systems exploit features on the human hand to perform identity verification.

In fact, as the computing, communication and display technologies progress, the existing human computer interaction policies, such as keyboards, mousses limit the boundary of the speed and openness of our communication and may be converted into a restricted access in the successful usage of computers. Figure bellows illustrates the basic process of the recognition.

Figure1: Input Image

Figure2: Grayscale Image

Figure3: HPF Image

Figure4: Enhanced Image

Figure5: Hand with edge detection

Figure6: Contour of hand

Figure7: A view of pixel calculations

Retina

Retina based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.[9]

Iris

Iris based biometric, on the other hand, involves analyzing features found in the coloured ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact

between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.[10]

The human iris recently has attracted the attention of biometrics-based identification and verification research and development community. The iris is so unique that no two irises are alike, even among identical twins, in the entire human population.

Automated biometrics-based personal identification systems can be classified into two main categories: identification and verification. In a process of verification (1-to-1 comparison), the biometrics information of an individual, who claims certain identity, is compared with the biometrics on the record that represent the identity that this individual claims. The comparison result determines whether the identity claims shall be accepted or rejected. On the other hand, it is often desirable to be able to discover the origin of certain biometrics information to prove or disprove the association of that information with a certain individual. This process is commonly known as identification (1-to-many comparison).

Actual iris identification can be broken down into four fundamental steps. First, a person stands in front of the iris identification system, generally between one and three feet away, while a wide angle camera calculates the position of their eye. A second camera zooms in on the eye and takes a black and white image. After the iris system has one's iris in focus, it overlays a circular grid (zone's of analysis) on the image of the iris and identifies where areas of light and dark fall. The purpose of overlaying the grid is so that the iris system can recognize a pattern within the iris and to generate 'points' within the pattern into an 'eyeprint'. Finally, the captured image or 'eyeprint' is checked against a previously stored 'reference template' in the database.

Signature

Signature verification analyzes the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not.[11] People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices

are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Surprisingly, relatively few significant signature applications have emerged compared with other biometric methodologies. But if your application fits, it is a technology worth considering.

Vein

Palm vein authentication has a high level of authentication accuracy due to the uniqueness and complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this is a difficult method to forge. Also, the system is contactless and hygienic for use in public areas. It is more powerful than other biometric authentication such as face, iris, and retinal.[12]

Palm vein authentication uses an infrared beam to penetrate the users hand as it is held over the sensor; the veins within the palm of the user are returned as black lines. Palm vein authentication has a high level of authentication accuracy due to the uniqueness and complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this is a difficult method to forge. Also, the system is contactless and hygienic for use in public areas.

Voice

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware — most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrolment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.[13-14]

CONCLUSIONS

Biometric authentication of a person is highly challenging and complex problem. A significant research effort has gone into this areas and a number of research works were published, Biometrics is a growing technology, which has been widely used in forensics,

secured access, prison security, medical, and robotics areas financial services, ecommerce, telecommunication, government, traffic, health care the security issues are more important.

REFERENCES

1. Lye Wi Liam, Ali Chekima, Liau Chung Fan and Jamal Ahmad Dargham, "Iris Recognition using Self-Organizing Neural Network", IEEE 2002 Student Conference on Research and Development Proceedings, Shah Alam, Malaysia, pp. 169-172.
2. Eric Sung, Xilin Chen, Jie Zhu and Jie Yang, "Towards non-cooperative iris recognition systems", Seventh international Conference on Control, Automation, Robotics and Vision (ICARCV'02), Singapore, Dec. 2002. pp. 990-995.
3. Jiali Cui, Yunhong Wang, JunZhou Huang, Tieniu Tan and Zhenan Sun, "An Iris Image Synthesis Method Based on PCA and Super-resolution", IEEE CS Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), Cambridge, UK, 23-26 August 2004; 4: 471-474.
4. Hyung Gu Lee, Seungin Noh, Kwanghyuk Bae, Kang-Ryoung Park and Jaihie Kim, "Invariant biometric code extraction", IEEE Intelligent Signal Processing and Communication Systems (ISPACS 2004), Seoul, Korea, 18-19 November, 2004; pp. 181-184.
5. Zhenan Sun, Yunhong Wang, Tieniu Tan and Jiali Cui, "Improving Iris Recognition Accuracy via Cascaded Classifiers", IEEE Transactions on Systems, MAN, and CYBERNETICS - Part C: Applications and Reviews, August 2005; 35(3): 435-441.
6. R. Sanches-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Biometric Identification through Hand Geometry Measurements," IEEE Transactions of Pattern Analysis and Machine Intelligence, October 2000; 22(10.
7. Ajeet Singh, BK Singh and Manish Verma), - Comparison of Different Algorithms of Face Recognition, VSRD-IJEECE, 2012; 2(5): 272- 278.
8. Samir K Bandyopadhyay, Debnath Bhattacharyya and Anindya Jyoti Pal, "Secure Delivery of Handwritten Signature", ACM Ubiquity, October 16, 2006; 7(40).
9. Weiki Yuan, Zhonghua Lin and Lu Xu, "A Rapid Iris Location Method Based on the Structure of Human Eyes", Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference Shanghai, China, 1-4 September, 2005; pp. 3020-3023.
10. Christopher Boyce, Arun Ross, Matthew Monaco, Lawrence Hornak and Xin Li, "Multispectral Iris Analysis: A Preliminary Study", Proceedings of the 2006 Conference

on Computer Vision and Pattern Recognition Workshop (CVPRW'06), June 2006, New York, USA.

11. R. Dhamija and Perrig, "Deja Vu: a user study images for authentication", 9th *USENIX* Secwity Symposium, 2000.
12. Martin de La Gorce*, Nikos Paragios "A variational approach to monocular hand-pose estimation" Computer Vision and Image Understanding, 2010; 114: 363–372.
13. Kaushik Subramanian "Pointing Based Object Localization" Robotics and Computer Vision, ECE 472 April 16th, 2009.
14. CenkerÖden, AytülErçil, VedatTaylanYıldız, Hikmet Kırmızıta, and Burak Büke "Hand Recognition Using Implicit Polynomials and Geometric Features" Bo aziçi University, Alper Atalay BUPAM Laboratory 80815, Istanbul Turkey.