International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 18, 2017 ISSN: 2348-6600
Reference ID: IJCS-242 PAGE NO: 1524-1528
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

Security BM Techiniqueusing in Digital Image Processing

S.Thiraviya Regina Rajam[1], Dr. S.Britto Ramesh Kumar[2], G.Karthiga[3]

[1]Research Scholar, Department of Computer Science, St. Antony's College of Arts and Science for Women, Dindigul.
[2]Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirapalli.
[3]M.phil Research Scholar, Department of Computer Science,Mother Teresa women's university,Kodaikanal.
srajicic10@gmail.com [1], Karthisarathi1991@gmail.com[2]

Abstract - In today world advanced used in technology have made easier by providing to high levels of knowledge to different devices.one major function is how to secure in personal data and information. Biometrics means measurement statistical analysis of peoples physical and behavioral characters..The term "Biometrics"is derived from the Greek words Bio (life) and Metric(life).The Bio-Metric(BM) security system increasing in cyber security system. The biometrics recover the technologies for measuring and analyzing a person physiological characteristics. These characteristics are unique to verify and identify person. The main research areas and it application to develop the security system for high security areas.

Keyword: Cyber security, Iris and security.

1. INTRODUCTION

In this bio security system describe the various application is how can you used in digital image processing at physical access control refers to the process that requires the physical characteristics. On the other hand, logical access control is the schemes, procedures and techniques which are used in the system. The difference between logical and physical access control is really small and it can be confused easily because physical access control is controlled by logical access control.eyes, nose, mouths, ears, jaw, size of eyes, mouth and others expressions. Facial expression is also counted as one of the factors to change during a user's facial recognition process.we are all define the secure personal data and any application not occur any errors.if we can occur error how can solve the errors and describe various using application.

2. RELEVANT WORK

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 18, 2017 ISSN: 2348-6600
Reference ID: IJCS-242 PAGE NO: 1524-1528
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

The chien le talk about in this paper various application and the physical access control application is the access the devices in which are applied at computers. This application is important and is entrusted with a high level of security.

It also covers the aspect of data loss in the system and Logical access control refers to a process of a scheme control over data files.Logical access control is used by militaries and governments to protect their important data with high security systems using biometric technology. The only difference between logical access control and physical access control is that the logical access control is used for computer network.The human face is one of the easiest characteristic which can be used in biometric security system to identify a user. Face recognition technology, is very popular . Furthermore, it is easy to install and does not require any expensive hardware. Facial recognition technology is used widely in a variety of security systems such as physical access control . However, it is still not as unique as its counterparts such as retinal, iris or DNA. And another techniques are 2-D barcode biometrics technology is a 2-dimesional method of presenting digital security information which is provided by the biometrics technologies system. 2-D barcode is normally applied during the identification of items rather than users.

Biometric face recognition systems will collect data from the users' face and store them in a database for future use. Facial expression is also counted as one of the factors to change during a user's facial recognition process[1].

The joseph n.pato and lynettle define the Authentication technologies are typically based on one of three things: something the individual knows, such as a password; something the individual has, such as a physical key or secure token; and something the individual is or does. Biometric technologies employ the last of these. Unlike password- or token-based systems, biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place.

Although traditional biometrics testing tends to focus on the match performance for a test data set, experience from many domains suggests that process and quality control should be analyzed for the complete system life cycle. Methods used successfully for the study and improvement of systems in other fields such as manufacturing and medicine (for example, controlled observation and experimentation on operatThe author Edmund spinella has been influenced by such pseudo-sciences as Phrenology, the study of human skull characteristics and Anthropometry, the study of human body . The past development of two disciplines, Phrenology and Anthropometry, helped to pave the way for biometrics. Phrenology, the study of the structure of the skull to determine a person's character and mental capacity, was founded by Franz Joseph in early nineteenth century Germany.The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. Image quality is measured in dots per inch (DPI) – more dots per inch means a higher resolution image.Image acquisition can be a major challenge for finger-scan developers, since the quality of print differs from person to person

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 18, 2017 ISSN: 2348-6600
Reference ID: IJCS-242 PAGE NO: 1524-1528
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear or tear or physiological traits.11 Taking an image in the cold weather can have an affect also. Oils in the finger help produce a better print[2].

The author prabhakarpankantijaint talk about A threshold tregulates the system decision. The system infers that pairs of biometric samples generating scores higher than or equal to t are mate pairs (that is, they belong to the same person). Consequently, pairs of biometric samples generating scores lower . The distribution of scores generated from pairs of samples from different persons is called an impostor distribution;the score distribution generated from pairs of samples from the same person is called a genuine distribution

A biometric verification system can make two types of errors:

- Mistaking biometric measurements from two different persons to be from the same person (called false match or false accept)
- Mistaking two biometric measurements from the same person to be from two different persons (called false nonmatchor false reject
- An operational biometric system makes a trade-off between false match rate (FMR) and false nonmatch rate (FNMR). In fact, both FMR and FNMR are functions of the system threshold t: If the system's designers decrease t to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise tto make the system more secure, then FNMR increases accordingly. We can depict system performance at all operating points (thresholds t) in the form of a receiver operating characteristic (ROC) curve. An ROC curve plots FMR against (1 – FNMR) or FNMR for various values of threshold t.

Minutiae matching will compare the details of the extract mineutae to identify the difference between one users fingerprint as compared to othersThere are several benefits of using finger print recognition systems.If the surface of the finger system is used gets damaged.

This will be a limitation factor for the security algorithm. Finger print security system is widely in different applications such as cell phones,laptops,usb and other devices.It is also used in judicial systems in order to record users information and verify one personavavis identify[3].

The author Marious savvis is describe about there are two main factors which makes a persons voice unique.secondly it is a behavioral component which is known as the voice accent,Biometrics technology created voice recognition systems in order to verify each persons identification using only their voice,this equipment include microphones,telephone.So that the system can analyze the users voice more accurately.on the other hand,un auters can record authorized users voices and run it through the verification in order to get user access control to system.To prevent the risk of un authorized access via recording devices,voice recognition system during verification state.This is one of the common used algorithm for extracting features that characterizes a finger print images[4].

Salil prabhakar talk about biometric recognition security and privacy concerns,each biometric has its strengths and weakness and the choice typically

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 18, 2017 ISSN: 2348-6600
Reference ID: IJCS-242 PAGE NO: 1524-1528
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

depends on the application.Use match a specific biometric to an application operatioe basednal mode and the biometric characteristics propertiesAs mentioned traditional technology available for achieving a positive recognition include knowledgeBased methods and token based methods[5].

Iris recognition systems will scan the iris in different ways. It will analyze over 200 points of the iris including: rings, furrows, freckles, the corona and others characteristics. After recording data from each individual, it will save the information in a database for future use in comparing it every time a user want to access to the system

Iris recognition security systems are considered as one of the most accurate security system nowadays. It is unique and easy to identify a user. Even though the system requires installation equipment and expensive fees, it is still the easiest and fastest method to identify a user. There should be no physical contact between the user and the system during the verification process. During the verification process, if the users are wearing accessories such as glasses and contact lenses, the system will work as normal because it does not change any characteristics of the user's iris. Theoretically, even if users have eye surgery, it will have no effect on the iris characteristics of that individual[6].

3. BASIC CONCEPTS

In this paper, the committee outlines some of the concepts underlying the typical operation of biometric systems in order to provide a framework for understanding the analysis and discussion in the rest of the report. Two concepts are discussed: sources of (1) variability and(2) uncertainty in biometric systems and modalities, including multibiometric approaches.

Sample Operational Process

The operational process typical for a biometric system. The main components of the system for the purposes of this discussion are the capture (whereby the sensor collects biometric data from the subject to be recognized), the reference database (where previously enrolled subjects' biometric data are held), the matcher (which compares presented data to reference data in order to make a recognition decision),.

This diagram presents a very simplified view of the overall system. The operational efficacy of a biometric system depends not only on its technical components—the biometric sample capture devices (sensors) and the mathematical algorithms that create and compare references—but also on the end-to-end application design, the environment in which the biometric sensor operates, and any conditions that impact the behavior of the data subjects, that is, persons with the potential to be sensed.

For example, the configuration of the database used to store references against which presented data will be compared affects system performance. At a coarse level, whether the database is networked or local is a primary factor in performance. Networked databases need secure communication, availability, and remote access

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 18, 2017 ISSN: 2348-6600
Reference ID: IJCS-242 PAGE NO: 1524-1528
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

privileges, and they also raise more privacy challenges than do local databases. Local databases, by contrast, may mean replicating the reference database multiple times, raising security, consistency, and scalability challenges.9 In both cases, the accuracy and currency of any identification data associated with reference
WDW tested various hand geometry and finger scanning technologies at several theme park locations to evaluate alternative technologies to the then-existing finger geometry used in its turnstile application. WDW also tested technologies for other applications to increase guest service and improve operating efficiency. Testing there is done in four stages: laboratory testing, technology testing, scenario testing, and operational evaluation. Since WDW has had existing biometric technology in place since 1996 and a substantial amount of experience with the biometric industry, its mind-set is that a threshold has been set for performance in both error rates and throughput and prospective vendors must exceed this level of performance to be considered for future enhancement projects

4. CONCLUSION

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 users can new technology will change our lives for the better.so biometric using many various application in digital image processing.

REFERENCES

1.Julian Ashbourn, Biometrics: Advanced Identity Verification, London: Springer-Verlag, pp. 5-11,2015.
2.A.K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in a Networked Society, KluwerAcademic Publishers.
3.Best Practices in Testing and Reporting Biometric Device Performance,version 2.0, tech. report, United Kingdom Biometric Working Group, 2002; www.cesg.gov.uk/ technology/biometrics.
4. Maltoni et al., Handbook of Fingerprint Recognition, Springer, 2013.
5.Password Clues, The CentralNic Password Survey Report, CentralNic, 13 July 2015; www.centralnic.com/page. php?pid=73.
6. Maio et al., "FVC2002: Second Fingerprint Verification Competition," Proc. Int'l Conf. Pattern Recognition, vol. 3, IEEE CS Press, 2013, pp. 811–814.