A Survey of Biometrics Security System

Mohammed Nasir Uddin[1], Selina Sharmin[2], Abu Hasnat Shohel Ahmed[3] and Emrul Hasan[4], Shahadot Hossain[5] and Muniruzzaman[6]

Shanto Mariam University of Creative Technology[1, 3] ,Uttara University[4,5,6]

Summary
Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices. Although many technologies fit in the biometric space, each works a bit differently. Relatively new on the biometric scene, face recognition devices use PC-attached cameras to record facial geometry. Once the biometric data is collected, it is encrypted and stored--locally, in the case of the desktop-only products; in a central database for the network solutions. When a user tries to log on, the software compares the incoming biometric data against the stored data.

Key words:
Finger Prints, Hand Geometry, Biometrics, Pattern Matching

1. Introduction

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of-identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems are being used for real-time identification, the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan, speech, facial thermo grams, and hand geometry.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system. The current security model for verification of identity, protection of information and authentication to access data or services is based on using a token or password, tied to and thereby representing an individual to either authenticate identity or allow access to information [Ann et al, 2007]. This token may be password or shared secret (something you know), an identity card (something you have) or biometric (something you are). In all this cases, the details of the token are held by a third party whose functions is to authorizes and at times allow the transaction to proceed if the details of an individual's token match those stored in a database. Kaufman et al [2002] identified authentication systems such as password-based, address-based and cryptographic authentication all of which have some weaknesses. Many researchers have proposed the use of biometric-based authentication as the most secure and privacy way to access data on the network. [Haag et al 2004, William 2003, Bishop 2003, Ann et at 2007, Umit 2006].

2. Biometrics

The physical characteristics of a person like finger prints, hand geometry, face, voice and iris are known as biometrics. Each biometric trait has its strengths and weaknesses. The suitable biometric can be selected depending upon the application in various computer based security systems. The important features of the various biometrics are discussed briefly in this section.

Manuscript received October 5, 2011
Manuscript revised October 20, 2011

2.1 Finger Prints

The finger prints of a person have been used as person identification from long time. A finger print is the pattern of rids and valley on the surface of a finger tip. The finger prints of the identical twins are different. It is affordable to scan the finger prints of a person and can be used in computer for number of applications. This method is traditional and it gives accuracy for currently available Fingerprint Recognition Systems for authentication [6]. This fingerprint recognition system is becoming affordable in a large number of applications like banking, Passport etc. Figure 1(a) shows a sample finger print image of a person.

2.2 Hand Geometry

The hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, length and width of the fingers. This method is very simple and easy to use. As there is no effect of environment factors such as dry weather or dry skin, this does not appear to have dry negative effects on the authentification accuracy. Also hand geometry information may not be invariant during the growth period of the children [9]. The hand geometry is scanned as shown in figure 1(b) and used for identification and recognition of a person.

2.3 Face

The face is the commonly used biometric characteristics for person recognition. The most popular approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. All these attributes of the face image are shown in figure 1 ©.As this technique involves many facial elements; these systems have difficulty in matching face images [11]. The face recognition systems which are used currently impose a number of restrictions on how facial images are obtained. This face recognition system automatically detects the correct face image and is able to recognize the person.

2.4 Voice

The voice recognition systems have been currently used in various applications. Voice is a combination of physical and behavioral biometrics. The figure 1 (d) shows a sample speech signal. The features of person voice are based on the vocal tracts, mouth, nasal activities and lips movement that are used synthesis of sound. These physical characteristics of human speech are invariant for individuals. The behavioral part of the speech of person changes over time due to age, medical conditions, and emotional state. The speaker dependent voice recognition systems are text dependent; and the speaker independent systems are what he or she speaks [13]. The speaker dependent voice recognition system is more difficult to design but provides more protection.

2.5 Iris

The iris is biological feature of a human. It is a unique structure of human which remains stable over a person lifetime. The iris is the annular region of the eye. The left and right irises of an individual can be treated as separate unique identifier. A sample human eye image is given in figure 1 (e).The iris information can be collected by iris image. The accuracy of iris based recognition system is promising. Each iris is believed to be distinctive and even the irises of identical twins are also different [15]. The iris recognition system has become more users friendly and cost effective. The iris have a very low false accept rate as compared to other biometrics like finger print, face, hand geometry and voice

3. Biometric Recognition System

The Biometric Recognition Systems are used to identify the person based on the feature vectors of any one of the biometric that the person possesses [16]. These systems are person authorized systems hence offer more secure and convenient process of identification compared to alternative methods of identification. The computer based security systems are used in various commercial, civilian and forensic applications. Each person has to establish the identity ranging from drivers' license to gaining entry into a country to the passport. The biometric system uses the individual's physical characteristics like fingerprint, hand geometry, face, voice or iris. They are more reliable and secure as they provides the access to authorized users in their physical presence [24]. A simple biometric system consists of four modules: Image/Voice acquisition, Preprocessing, Feature extraction and Recognition. The proposed system should be able to collect the biometric image or voice, to perform preprocessing on original input, to encode the input to get feature vector, to match the features to recognized the person

3.1 Image/Voice Acquisition Module

This is the first module to acquire the biometric input. The input can be image or voice according to the selection of biometrics. The sensors like high resolution CCD camera or recorder can be used to capture the biometric image / voice. The distance between the sensor and human should be constant, the lighting system as well as physical capture

system should be constant to acquire standard biometric input.

3.2 Preprocessing Module

Once the input is captured, the original input image or voice signal is processed to remove the noise and blurring effect. The image is localized to extract the region of interest. The voice signal is framed to extract the desired signal. Then this processed input is given to feature extraction module.

3.3 Feature Extraction Module

In the feature extraction module, the preprocessed image /voice is used to extract the features. The feature extraction algorithms are applied to get feature vector of the biometric image / voice. There are various feature extraction techniques like Independent Component Analysis, Linear discriminate component, principal component analysis, wavelet transform, LPC, MFCC, etc [10][11][14][15]. According to the biometrics selected and its application the feature extraction technique can be applied.

3.4 Recognition Module

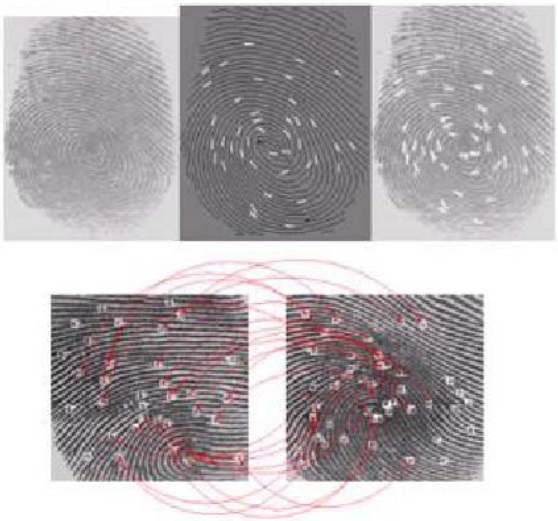
The feature vectors, generated in the Feature Extraction Module are used in this module to classify the biometric data. There are the classifiers like hamming distance, Euclidian distance, and Support vector machine classifier. The rules are defined for recognition of a person with his / her biometrics [27]. According to the biometric applications, the suitable classifiers can be used to get better performance of the system. The feature vectors are used to write the decision making rules. In this module user's identity is established or a claimed identity is accepted or rejected .

4. Applications of the Biometric Recognition Systems

The biometric is an emerging field of technology which uses the physical biological or behavioral characteristics that can be processed to perform automatic recognition of a person. Hence this requires achieving low cost, reliable human identification system by using feature set of individual characteristics. The biometric concentrates on physical aspects like finger print, hand geometry, face, voice and iris of a person [19].

4.1 Finger Print

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.



Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures cannot be completely characterized by minutiae. Efforts are being on to try an alternate representation of fingerprints, which will capture more local information and yield a fixed length code for the fingerprint. The matching will then hopefully become a relatively simple task of calculating the Euclidean distance will between the two codes.

Scientists are developing algorithms which are more robust to noise in fingerprint images and deliver increased

accuracy in real-time. A commercial fingerprint-based authentication system requires a very low False Reject Rate (FAR) for a given False
Accept Rate (FAR). This is very difficult to achieve with any one technique. Scientists are investigating methods to pool evidence
from various matching techniques to increase the overall accuracy of the system. In a real application, the sensor, the acquisition system and the variation in performance of the system over time is very critical. Scientists are also field testing this system on a limited number of users to evaluate the system performance over a period of time.

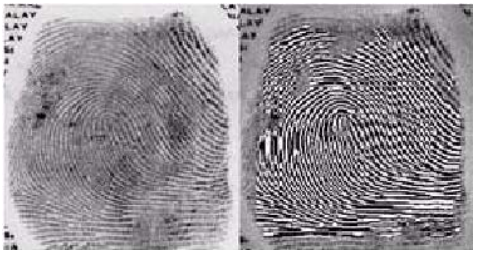
4.1.1 Finger Print Classification:

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database

To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.
Fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature, which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. Different algorithms are developed to classify fingerprints into five classes, namely, *whorl, right loop, left loop, arch, and tented arch*. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a Finger Code which is used for classification. This classification is based on a two-stage classifier which uses a K-nearest neighbor classifier in the first stage and a set of neural networks in the second stage.

4.1.2 Finger Print Image Enhancement:

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images.



In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. Scientists have developed a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and furrow structures of input fingerprint images based on the estimated local ridge orientation and frequency. Scientists have evaluated the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification system. Experimental results show that incorporating the enhancement algorithms improves both the goodness index and the verification accuracy.

4.2 Hand Geometry

Hand Geometry Biometric Recognition System uses the geometric shape of the hand to identify the person. This system also uses finger length, thickness, and curvature for the purpose of verification [21]. The hand geometry is not distinctive but it is the ideal choice. The hand geometry data collection is easier and hand geometry can be combined with other biometrics like finger print [20]. The recent applications of the hand geometry biometric systems include San Francisco International Airport uses hand geometry to restrict access to critical areas, child day care centers use to verify the identity parents, payroll accuracy and access control, the fast gate pilot program to track border crossings for frequent travelers, United States military using for access control and majority of nuclear power plants in US use hand geometry for access control [8]. The hand geometry is used in biometric

systems as it behaves the following features: • Very small template size, easy to maintain and store large database
• High reliability and accuracy
• Robust, user friendly and easy to integrate into existing and third party systems
• Ideal for rough outdoor environments like construction industry and can handle high throughput of people
• Relatively inexpensive offers excellent return on investment.

4.3 Face

Face recognition biometric systems uses facial characteristics of a person. It measures the overall facial structure, distance between eyes, nose, mouth, and jaw edges. These features are extracted and used for identification of a person [11]. Face recognition systems are using successfully in verification systems like Document control of passport, drivers licenses, transactional authentication, credit cards, ATMs, physical access control, smart doors, voter registration, election accuracy, time and attendance, entry and exit verification. Face recognition biometric systems are strongly recommended as it behaves following features:
• Facial photograph do not disclose information
• The facial image is already socially and culturally accepted internationally.
• It is already collected and verified to produce passport
• The public are already aware of its capture and use for identity as well as verification purpose.
• It is non-intrusive
• Many states have legacy database of facial images
• Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities

4.4 Voice

The speech recognition is most important research area in the today's world. There are various speech recognition approaches; among those are the acoustics phonetic pattern comparisons and automatic speech recognition approach [22]. The performance of speech recognition system depends on various factors some of them are speaker variation, ambient noise, and variation in the tone of the same speaker, sensitivity of phonetic input systems, distance and regular variations. The speaker recognition is most appropriate in phone based applications, the entertainment TV channels [13]. The voice recognition biometric systems are used for access control, banking, government offices and entertainment applications, smart cards, PIN and other security purposes.

4.4.1 Speaker Modeling:

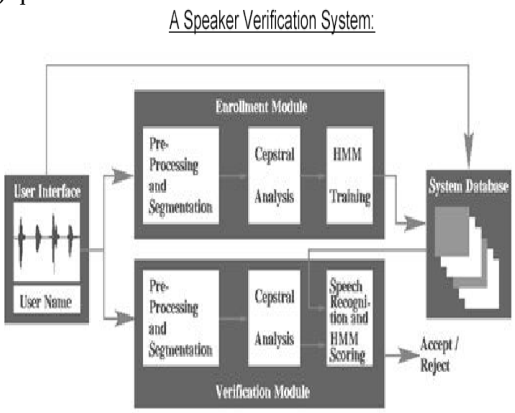
Utterances spoken by the same person but at different times result in similar yet a different sequence of feature vectors. The purpose of voice modeling is to build a model that captures these variations in the extracted set of features. There are two types of models that have been used extensively in speaker verification and speech recognition systems: stochastic models and template models. The stochastic model treats the speech production process as a parametric random process and assumes that the parameters of the underlying stochastic process can be estimated in a precise, well-defined manner. The template model attempts to model the speech production process in a non-parametric manner by retaining a number of sequences of feature vectors derived from multiple utterances of the same word by the same person. Template models dominated early work in speaker verification and speech recognition because the template model is intuitively more reasonable. However, recent work in stochastic models has demonstrated that these models are more flexible and hence allow for better modeling of the speech production process. A very popular stochastic model for modeling the speech production process is the Hidden Markov Model (HMM). HMMs are extensions to the conventional Markov models, wherein the observations are a probabilistic function of the state, i.e., the model is a doubly embedded stochastic process where the underlying stochastic process is not directly observable (it is hidden). The HMM can only be viewed through another set of stochastic processes that produce the sequence of observations. Thus, the HMM is a finite-state machine, where a probability density function p(x | s_i) is associated with each state s_i. The states are connected by a transition network, where the state transition probabilities are a_{ij} = p(s_i | s_j). For speech signals, another type of HMM, called a left-right model or a Bakis model, is found to be more useful. A left-right model has the property that as time increases, the state index increases (or stays the same) that is the system states proceed from left to right. Since the properties of a speech signal change over time in a successive manner, this model is very well suited for modeling the speech production process.

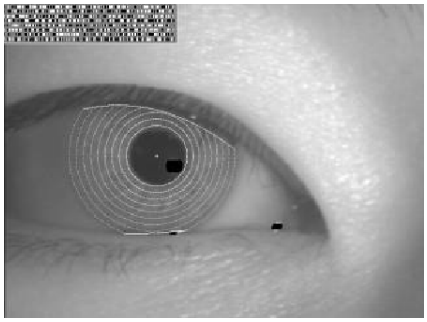
4.4.2 Pattern Matching:

The pattern matching process involves the comparison of a given set of input feature vectors against the speaker model for the claimed identity and computing a matching score. For the Hidden Markov models discussed above, the matching score is the probability that a given set of feature vectors was generated by the model. A Speaker Verification System:

4.5 Iris

Iris recognition is a new field of Pattern recognition. Iris recognition is based on visible (via regular and/or infrared light) qualities of the iris.





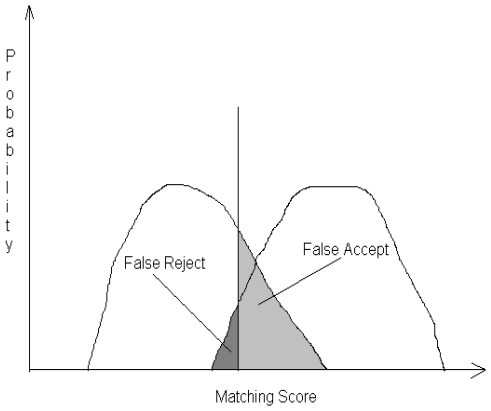
A primary visible characteristic is the trabecular meshwork (permanently formed by the 8th month of gestation), a tissue which gives the appearance of dividing the iris in a radial fashion. Other visible characteristics include rings, furrows, freckles, and the corona, to cite only the more familiar. Expressed simply, iris recognition technology converts these visible characteristics into a 512 byte Iris Code(tm), a template stored for future verification attempts. 512 bytes is a fairly compact size for a biometric template, but the quantity of information derived from the iris is massive. The density of information is such that each iris can be said to have 266 unique "spots", as opposed to 13-60 for traditional biometric technologies. This '266' measurement is cited in all iris recognition literature.; after allowing for the algorithm's correlative functions and for characteristics inherent to most human eyes., It has been concluded that 173 "independent binary degrees-of-freedom" can be extracted from his algorithm - an exceptionally large number for a biometric

The iris image consists of the colored tissue surrounding the pupil .The iris recognition systems are known as real time, high confidence recognition of person identification [25]. These systems are used in many applications like passports, activation security, and controlling access to restricted areas at airports, database access and computer login, access to building and homes, border crossings and other government program. The iris recognition systems behave following features:

• Perform 1: n identification with no limitation on numbers.
• The most robust biometric technology available in the market today never had a false acceptance.
• Biometric templates once captured do not need to be enrolled again, iris stable throughout a human life

5 Biometric System Performances

The recognition accuracy is depending on the image acquisition, the position of acquiring sensor, intensity of light focusing, environmental changes, noise, and bad user's interaction with the sensor. Therefore the two images acquired by the sensor may not be having same characteristics [26]. The biometric matching systems are used to find the matching score between the two images. The threshold t is assumed and the matching score is less than t then the image is considered as the different person [25]. Then two errors are measured in terms of false reject (FAR) and false accept rate (FRR). FAR: The biometric measurement between two persons is same. FRR: The biometric measurement between two persons is different.
If the system decreases t to make the system more tolerant to input variation and noise, FAR increases. On the other hand if the system increases t to make the system more secure, FRR increases accordingly [16]. Figure 3 shows the performance of the system which is depending on the matching score between two images and is measured by the errors; false accept rate and false reject rate



6. Biometrics-based Web Access

Authentication and encryption are crucial to network security. Public key cryptography provides a secure way

to exchange information but designing a high security authentication system still remains an open problem. Complex passwords are easy to forget while simple passwords are easily guessed by unauthorized persons. Several of the biometric characteristics of an individual are unique and do not change over time. These properties make biometrics well suited for authentication. Authentication systems based on fingerprints, voice, iris, and hand geometry exist for applications such as passport control, forensics, automatic teller machines, driver license, and border control. With the increasing growth of the Internet, there is a need to restrict access to sensitive data on the Web to authorized users. We have developed a prototype system which uses hand geometry to authenticate users to restrict access to web pages. Initial evaluation of the prototype system is encouraging. Similar techniques can be used to authenticate people for e-commerce applications

Conclusion

The Biometric security Systems are the systems which uses the physical characteristics of a person like finger print, hand geometry, face , voice and iris. These systems overcomes the drawbacks of the traditional computer based security systems which are used at the places like ATM, passport, payroll, drivers' licenses, credit cards, access control, smart cards, PIN, government offices and network security. The biometric security systems have been proved to be accurate and very effective in various applications. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer based security systems.

References

[1] Joseph Lewis, University of Maryland, Bowie State University, "Biometrics for secure Identity Verification: Trends and Developments" January 2002.

[2] Lia Ma, Yunhong Wang, Tieniu Tan, "Iris Recognition Based on Multichannel GaborFiltering", ACCV2002: The 5th Asian Conference on Computer Vision, 23-25 January 2002, Melbounce, Australia.

[3] Muhammad Khurram Khan, Jiashu Zhang and Shi-Jinn Horng, "An Effective Iris Recognition System for Identification of Humans", IEEE 2004.

[4] Libor Masek, the University of Western Australia, "Recognition of Human Iris Patterns for Biometric Identification", 2003.

[5] Mathew Kabatoff John Dougman, BioSocieties, "Pattern Recognition: Biometrics, Identity and State – An Interview with John Dougman", (2008), 3, 81, 86, © London School of Economics and Political Science, London UK.

[6] A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification" , IEEE Trans. Pattern Anal. Mach. Intel. 1997.

[7] K. Karu, A.K. Jain, "Fingerprint classification, Pattern Recognition", 1996.

[8] Pathak,Ajay Kumar Zhang, David D., "Hand geometry recognition using entropy-based discretization", IEEE Transactions on information forensics and security, June 2007, v. 2, no. 2, p. 181- 187, Jun-2007.

[9] Michael Goh Kah Ong,Tee Connie, Andrew Teoh Beng Jin, David Ngo Chek Ling, "A single-sensor hand geometry and palm print verification system", Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, Berkley, California , 2003 .

[10] Peng Wang; Qiang Ji; Wayman, J.L., "Modeling and Predicting Face Recognition System Performance Based on Analysis of Similarity Scores", Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume 29, Issue 4, April 2007.

[11] Steve Lawrence C. Lee Giles Ah Chung Tsoi, Andrew D. Back, "Face Recognition: A Convolutional Neural Network Approach", IEEE Transactions on Neural Networks, Special Issue on Neural Networks and Pattern Recognition.

[12] V. Amudha, B.Venkataramani, R. Vinoth kumar and S. Ravishankar, "Software/Hardware Co- Design of HMM Based Isolated Digit Recognition System " , JOURNAL OF COMPUTERS, VOL. 4, NO. 2, FEBRUARY 2009.

[13] Bill Swartz, Neeraj Magotra, "Feature Extraction for Automatic Speech Recognition ", 1997 IEEE Transaction.

[14] Wei Han, Cheong- Fat Chan, Chiu Sing Choy and Kong Pang Pun, "An Efficient MFCC Extraction Method in Speech Recognition", IEEE 2006.

[15] John Daugman, "How Iris Recognition Works", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004

[16] Kresimir Delac, Mislav Gregic, "A Survey of Biometric Recognition Methods", 46th International Symposium Electronic in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia.

[17] Natalia A. Schmid, Joseph A.O'Sullivan, "Performance Prediction Methodology for Biometric Systems using a Large Deviations Approch", IEEE Transaction of Signal Processing, October 2004.

[18] Li Ma , Tieniu Tan , Yunhong Wang , Dexin Zhang , " Personal Identification Based on Iris Texture Analysis" , IEEE Transactions on Pattern Analysis and Machine Intelligence , Vol. 25 No. 12, December 2003.

[19] John Carter, Mark Nixon, "An Integrated Biometric Database" Department of Electronics and Computer Science, University of Southampton, Highfield, Southanpton, SO95NH.

[20] Arun Rose, Anil Jain and Sharat Pankanti, "A Hand Geometry Based Verification System".

[21] Boreki, Guilherm, Zimmer, Alessandro, "Hand Geometry Feature Extraction through Curvature Profile Analysis", UNICENP, Computer Engineering Department, 2004.

[22] L. Rabiner, B. H. Juang, "Fundamentals of Speech Recognition", Pearson Education.

[23] Raul Sancher, Reillo, "Smart Card Information and Journal of Theoretical and Applied Information Technology © 2005 - 2010 JATIT. All rights reserved. www.jatit.org operation

Using Biometrics", IEEE AESS Systems Magazine, April 2001.
[24] Anil K. Jain, Arun Ross, Sharath Pankanti "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol 1, No. 2, June 2006.
[25] Sulochana Sonkamble, Dr. R.C. Thool, Balwant Sonkamble, "An Effective Machine-Vision System for Information Security and Privacy using Iris Biometrics", in The 12th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2008 at Orlando, Florida, USA during June 29th - July 2nd , 2008.
[26] John Daugman, Cathryn Downing, "Effect of Severe Image Compression on Iris Recognition Performance", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 1, March 2008.
[27] John Daugman, "Biometric Decision Landscapes", University of Cambridge the Computer Laboratory, England.

Mohammed Nasir Uddin received PhD in Computer Science from Moscow Power Engineering Institute (Technical University),Moscow. Russia. Masters of Science in Computer Engineering, and Bachelor of Engineering in Computer Engineering from State University of Lvivska Polytechnica, Lvov, Ukraine. Presently Working as an Assistant Professor,Department of Computer Science and Engineering, Shanto Mariam University of Creative Technology, Dhaka, Bangladesh. His areas of interest include Information & Computer security, Microprocessor system, Pattern Recognition and Digital Systems.

Selina Sharmin is a Lecturer of CSE & CSIT at Shanto-Mariam University of Creative Technology. She completed M.S and B.Sc with concentration in Computer Science & Enginnering, from University of Dhaka, Dhaka, Bangladesh. She has interest in the field of Bio-Informatics, Programming in Critical field, Computer security and Data Mining.

Shahadot Hossain is a Lecturer of CSE at Uttara University. He completed M.Sc and B.Sc(Engg.) in Computer Science and Engineering from Uttara University,Dhaka, Bangladesh. He has interest in the field of Digital System, Virtual Networking and computer and Network security.

Abu Hasnat Shohel Ahmed is a Lecturer of CSE & CSIT at Shanto-Mariam University of Creative Technology. He completed M.S and B.Sc with concentration in Applied Physics, Electronics and Communication Engineering from University of Chittagong, Chittagong, Bangladesh. He is the Associate Member of Bangladesh Computer Society. He has interest in the field of Wireless & Microwave communication, Networking, Computer security and Bio-Informatics

Emrul Hasan is a Lecturer of CSE at Uttara University. He completed M.Sc and B.Sc(Engg.) in Computer Science and Engineering from Uttara University,Dhaka, Bangladesh. He has interest in the field of Digital System, Algorithm in critical field of Programming, Virtual Networking and computer data security.

Muniruzzaman is a Lecturer of CSE at Uttara University. He completed M.Sc and B.Sc(Engg.) in Computer Science and Engineering from Uttara University,Dhaka, Bangladesh. He has interest in the field of Digital System, of Bio-Informatics, Programming in Critical field, Computer security and Data Mining.