Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Biometrics: Overview and potential use for E- Governance Services

Mrs Sharmila Jaywant Shinde
Assistant Professor
SCOEM, Satara
India

Mr Jaywant G.Shinde
Government Servant
Satara
India

Ms Mohini M Kharade
Student
Trinty College ,Pune
India

Ms Dhanashree H. Kadam
Assistant Professor
SCOEM, Satara
Inda

Abstrsct:- The definition of E-Governance is the use of Information and communication technology to provide the improvement in government services , transactions, interaction with citizens, land revenue, business and other parts of government. This paper investigates the applicability and potential use of biometrics for E-Government services. In this paper we also identify the requirements of biometrics in e-governance, recognition techniques and what are the possible attacks on biometric systems. We also provide some solutions to reduce the vulnerabilities in the system. A number of biometric traits have been developed and are used to authenticate the person's identity. A biometric system can be either an 'identification' system or a 'verification' (authentication) system. Biometrics technology continues to stride forward with its wider acceptance and its real need in various new security facets of modern society. Here we identify the requirements of biometrics in e-governance and also define how it is applicable and what are the possible attacks on biometric systems

Keywords :E-government , DNA, ISFET , ICT , G2B, Keystokes

I. INTRODUCTION

Biometrics

Biometrics or biometric authentication is the identification of humans by their characteristics . Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups . Following block diagrams shows enrollment, verification and identification tasks which are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database.

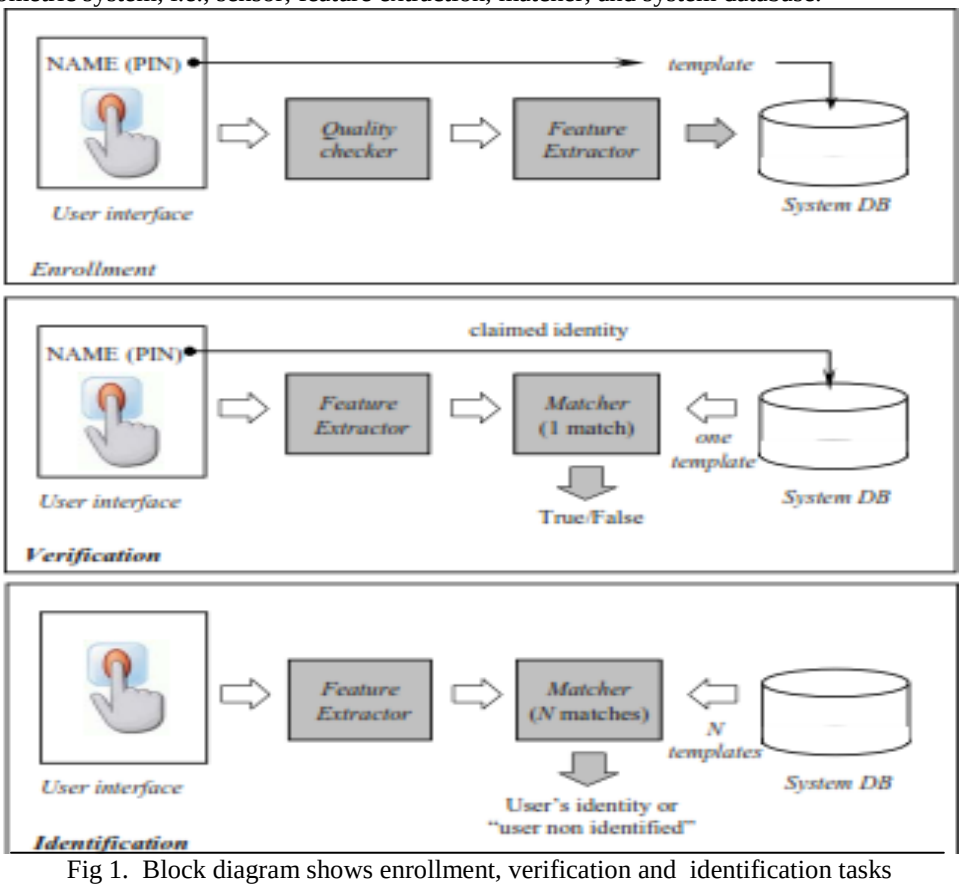


Fig 1. Block diagram shows enrollment, verification and identification tasks

Biometrics is becoming an important international standard as an authentication technology providing cross-border immigration and security controls; however, the case for biometrics in e-government services is more complex. All biometric technologies share the same underlying processes: all operate either in verification (authentication) mode or in a recognition (identification) mode.The selection of a particular biometric is depends on following application which involves a weighting of several factors.

1) Universality:

Universality means that every person using a system should possess the trait.

2)Uniqueness:

Uniqueness means the trait should be sufficiently different for an individuals in the relevant population that is they can be distinguished from one another.

3) Permanence:

Permanence related to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.

4) Measurability :

Measurability is also called collectability ,which is related to the ease of acquisition or measurement of the trait. In addition, acquired data should be in the form that permits subsequent processing and extraction of the relevant feature sets.

5) Performance:

Performance means the accuracy, speed, and robustness of technology used.

6) Acceptability:

Acceptability means how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

7) Circumvention:

Circumvention is related to the ease with which a trait might be imitated using an artifact or substitute.

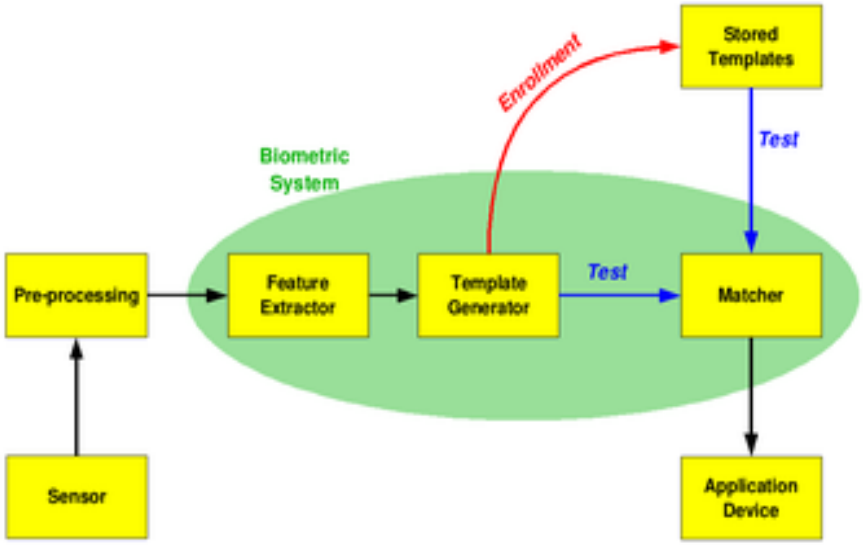


Fig 2. Basic modes of Biometric System

The above block diagram shows the two basic modes of a biometric system[2].First, is verification (or authentication) mode ,the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Second, is identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. If the first time an individual uses a biometric system then it is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment.

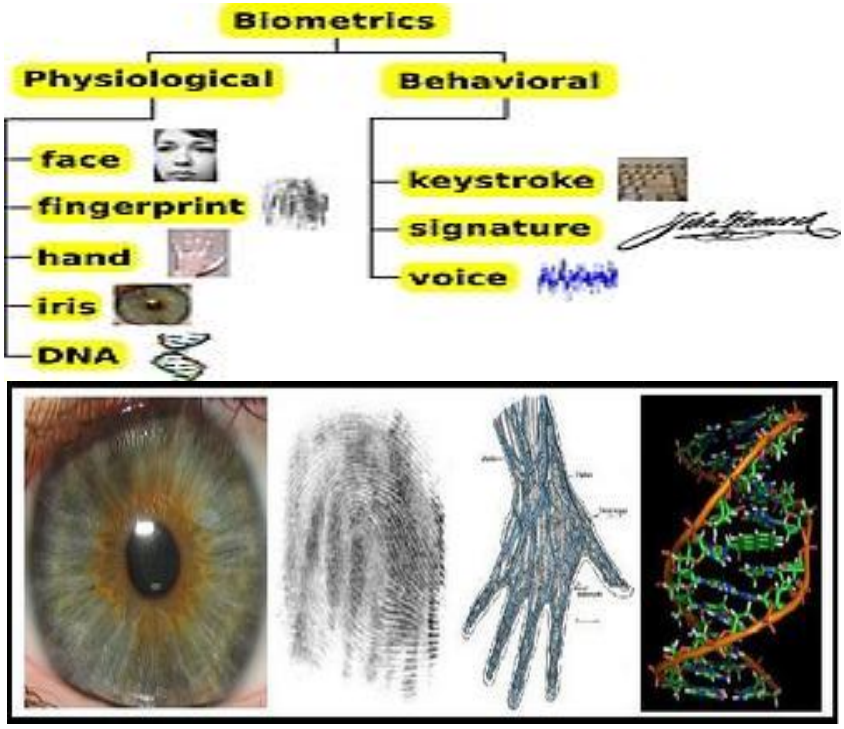
A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

8)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.

9)Verification –

On e 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. Biometrics involves the use of physiological and behavioral characteristics to provide the identification of individuals as applied to physical and network security within a business.



A] Physiological Biometrics:-

1)Face Biometrics:

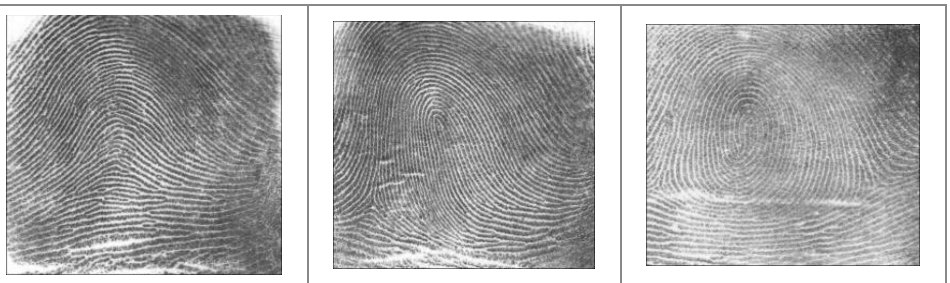
Face recognition is a non-intrusive method and facial images are the most common biometric characteristic used by humans to make a personal recognition. 3D face recognition technology is now commonly used in identification and verification These technology used to identify different facial expressions in blurred light as well. Most 3D face recognition devices perform their identification operation by comparing the biometric pattern with the recorded database in it. With the help of its enhanced integrated algorithms 3D face recognition is more effectively used in law enforcement agencies and corporations.

Fig 3. Face recognition

All biometric systems use the same information for face recognition . The most accepted approaches are based on the position, shape and size of facial features, such as eyebrow, eyes, nose, lips, chin and their spatial association and the overall analysis of face image that represents face as a combination of a number of objects (patterns).

2) Fingerprint Biometrics:-

Fingerprinting is the oldest and most consistently used forms of physiological biometrics..The uniqueness of fingerprints is due to the series of ridges and furrows on the fingers. There are three basic classifications for fingerprints - arch, loop, and whorl.



Arch	Loop	Whorl

Fig 4. Fingerprints

Fingerprints are like graphical flow-like ridges on human fingers. Individual epidermal ridges and valleys have different characteristics for different fingers. The configuration and minute details of individual ridges and furrows are permanent and unchanging for a given finger. Inexpensive, Fast results, Reliable , Established systems , Effective are the some major advantages of use of fingerprints in biometric security. Because of that reason fingerprinting is one of the best methods for quickly identifying individuals. But there is possibility of fake fingerprint identification by making imprints on wax-like substances. This is not widespread but it is a possible threat.

3) Hand Geometry:-

Hand geometry scan require that users place their hands onto a surface with 5 pegs then this aligns the hand , so that the scanner can get a consistent reading on each scan. The scanning is then compared with the required database for verification. A typical scan will take two pictures of the hand: one of the top and one of the side. Hand geometry is the type of physiological biometrics in which the shape of the hand used for authentication purposes. Then these scanning takes various traits of the hand, such as finger length, width and curvature, as well as unique features may be used for identification. It is not a unique form of biometric security. In the hand scanning we conclude that more than one person may have the same or very similar hand shapes. But this is limitation of the usefulness of hand geometry to verification, not identification. Hand geometry is currently in used for physical security purposes, these are building access, due to its ease of use, low cost and relatively impersonal data it uses.

Fig5 . Hand geometry

Implementing a security system based on the hand geometry alone would not be a viable security system, however when combined with fingerprint biometrics ,it is a suitable security system for almost any business need.

4) Iris Biometrics :

The iris is the colored ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different, too. Research shows that the matching accuracy of iris identification is greater than the DNA testing.

Fig 6. Eye biometric

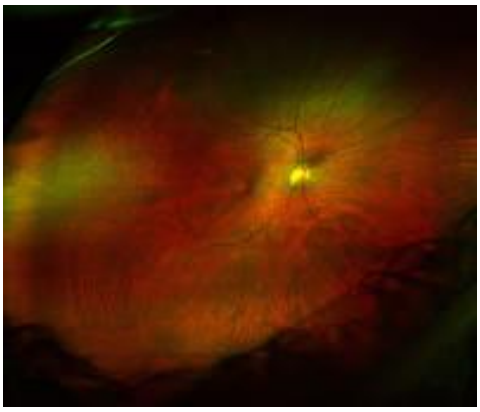


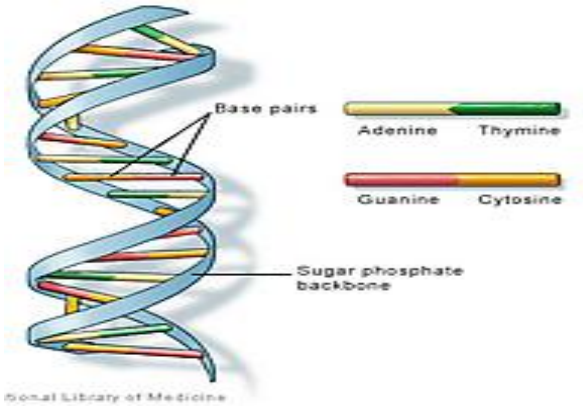
Fig 7Example of a scanned retina(Machine Scanning an Eye)

In Eye biometrics the retina scan machines are fairly expensive and a popular use of this type of security is in government agencies to identify employees.

5) DNA-based Biometrics:

DNA, means Deoxyribo Nucleic Acid which is the one-dimensional ultimate unique code for one'individuality

except for the fact that identical twins have identical DNA patterns.



Following are the some basic steps of DNA profiling :

1. Isolate the DNA means sample can originate from blood, saliva, hair, semen, or tissue
2. Section the DNA sample into shorter segments containing known variable number tandem repeats (VNTRs)—identical repeat sequences of DNA
3. Organize the DNA segments by size
4. Compare the DNA segments from various samples

A professor at National University in San Diego, California is working on creating a portable DNA sequence that will combine existing DNA biosensors with a new device called the ion-selective field-effect transistor (ISFET). This product would allow a handheld device to perform the same activities that currently must take place in a laboratory. These implementation of DNA biometrics into civilian business environments and government for use in physical and network security will expand to a great extent.

B] Behavioral Biometrics:-

1) Keystroke:

Keystroke Dynamics are the type of behavioral biometrics, This is study of how individual humans type on a keyboard, considering factors such as Flight Time (the time it takes to move from one key to another) and Dwell time (the time a person spends on any given key).

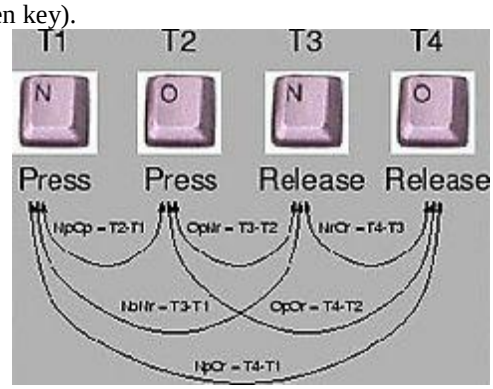


Fig 9. Keystroke Biometrics

These is basis for testing or observing one's pattern for typing is the repetition of typing so that differences can be noted and patterns observed between words.

2) E-Governance

E-Governance means the development, deployment and enforcement of the policies, laws and regulations necessary to support the functioning of a knowledge Society as well as of e-Government. Governments are using the Internet and E-Commerce technologies to provide public services to their citizens.It is the application of information and communication technology (ICT) which helps for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.

3) Requirement of Biometric in E-governance

Biometric is widely used in forensics, such as criminal identification and jail security and also used in government services are as follows-

1) Biometrics used in Banking security, such as electronic fund transfers, ATM security, check cashing and credit card transactions;

2) It used in physical access control, such as airport access control;

3) For accessing the database via login privileges biometrics is used in information system security
4) In the government benefits distribution, such as welfare disbursement programs;
5), To provide a unique identification to the citizens and integrate different government services biometrics used in national-id systems
6)It provides registration facilities for voters and drivers
7) In the customs and immigration for the Immigration and Naturalization Service Passenger Accelerated

II. ATTACKS ON BIOMETRIC SYSTEMS

A biometric system is open to attacks on different types of attacks that cam compromise to the security afforded by the system, therefore resulting in the system failure.

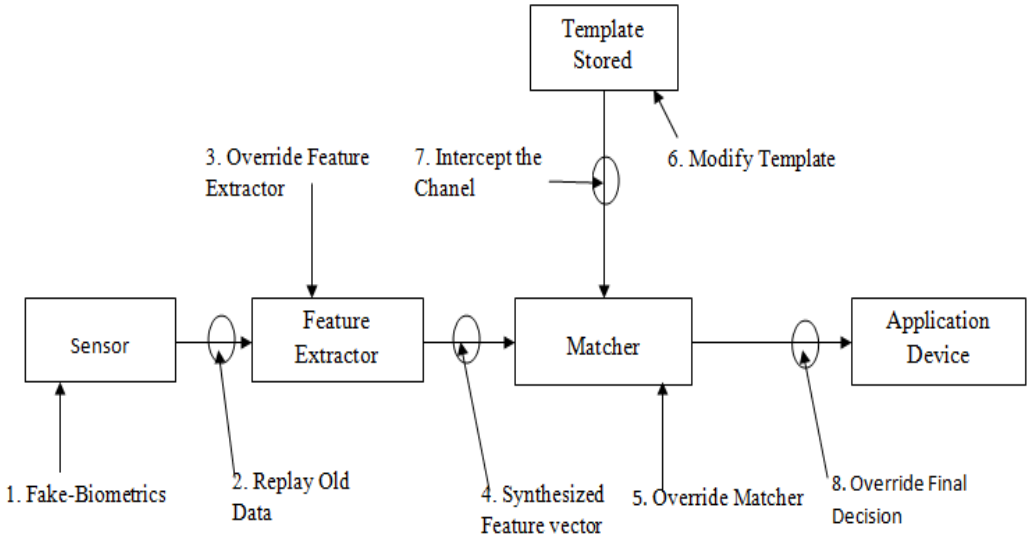


Fig 10 : Possible attacks on biometric system

Above figure shows several different levels of attacks that can be launched against a biometric system.
1)In fake biometric trait objects are used during the identification checking process. The fake biometric is the reproduction of original biometric and contains the same properties, such as an artificial finger .
2) The biometric data of an authenticate user is hacked and this data is submitted to the system repeatedly and because of that authenticate user will never get access to the services of system.
3) The matcher program may be changed with another program that results always true, therefore unauthorized user may also have the access to the system.
4) The modification of the template in the database may also result into security break and New templates may be replaced by with old templates.
5) The data may be altered when transmitting between various modules of the system.

III. PROPOSED SYSTEM

Following are some solution for secure authentication in E-Governance .

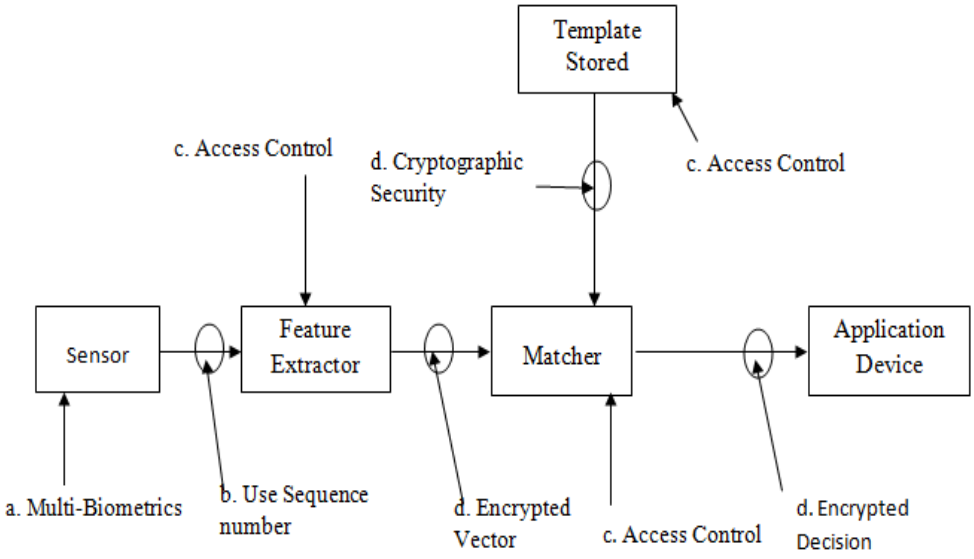


Fig 11: Solution to remove vulnerabilities in system

1) If a fake biometric is presented (camouflage attack) on biometric authentication system, the solution is to use multi-biometrics.
2) The protection to reply attack can be provided by using the sequence number, if a system or person request enters the same trait more than specified time, simply reject its request.
3) By the use of multilevel security some attacks can reduced. Implementation of proper access control results into resistance to the attacks on stored template, feature extractor and matcher. Access to data and permission to change the structure of program will require privileges.
4)Data should be encrypted before transmission on the communication channel. Encrypted data should be stored in the database. It should be decrypted only when the actual processing is required. so that if any eavesdropper have access to the data it will get the encrypted form of data that is difficult to interpret.

IV. CONCLUSION

In these paper we discussed the e-Governance and biometric system. We also describe how the biometric systems are applicable to the eGovernance projects. Biometrics technology continues to stride forward with its wider acceptance and its real need in various new security facets of modern society. Here we identify the requirements of biometrics in e-governance and also define how it is applicable and what are the possible attacks on biometric systems.Some security threats on the biometric systems are addressed and solutions to these problems are suggested. Proposed solutions are very much effective in terms of both theory and experiments. If these approaches are used in the e-Governance system they will ensure system's accuracy, reliability, security and efficiency. The proposed system can be implemented in e-Governance services like citizenship records, police records, ration card application, agriculture services, hospital services, BPL services and pension scheme, recruitment, online exams and results.

REFERENCES

[1] Frank Bannister and Regina Connolly, "New Problems for Old? Defining e-Governance", proceedings of the 44th Hawaii International Conference on System Sciences – 2011
[2] Piyush Morwal ,Parvinder Singh ,Rajkumar Tripathi,"Security in e-Governance using Biometric" International Journal of Computer Applications (0975 – 8887) Volume 50 – No.3, July 2012
[3] 1 R.HiI1, "Retina Identification" Biometrics, Personal Identification in Networked Society (Anil Jain, Ruud Bolle,Sharath Pankanti Eds.) 1999.
[4] L O'Gorman, "Fingerprint Verification"Biometrics, Personal Identification in Networked Society (Anil Jain, Ruud Bolle, Sharath Pankanti Eds.)1999.
[5] A.K. Jain, R. Boole and S. Pankanti, "Biometrics:Personal Identification in Network Society". Kluwer Academic Publishers, 1991.
[6] S.M.Lucas, "Face Recognition With The Continuous n-tuple Classifier".
[7] Vaclav Matyas, Zdenek Riha, "Biometric Authentication Systems".
[8] Biometrics Newsportal.com. "DNA Biometrics." Biometric News Portal. 04/03/2008. http://www.biometricnewsportal.com/dna_biometrics.asp
[9] J. L. Wayman, "Fundamentals of Biometric Authentication Technologies", International Journal of Image and Graphics, Vol. 1, No. 1, pp. 93-113, 2001.
[10] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

