International Research Journal of Applied and Basic Sciences
© 2013 Available online at www.irjabs.com
ISSN 2251-838X / Vol, 6 (11): 1609-1618
Science Explorer Publications

Biometric Recognition Systems: A Survey

Ali Heydarzadegan[1],Mohsen Moradi[2], Mehrdad Moradi[3],Alireza Toorani[4]

1. Department of Computer Engineering,Beyza Branch,Islamic Azad University,Beyza,Iran
2. Department of Computer Engineering, Ghir–o-karzin center,Islamic Azad University,Firoozabad,Iran
3. Young Researchers and Elite Club,shiraz Branch, Islamic Azad University, shiraz, Iran
4. Department of Computer Engineering,Beyza Branch,Islamic Azad University,Beyza,Iran

Corresponding Author email: A.heidarzadegan@yahoo.com

ABSTRACT: Today, due to the increasing importance of information and willingness of people for information security, using old tools such a password alone is not responsive and reliable, so scientists have been looking for more reliable ways and one of the most successful founded ways are using Biometric science. A biometric recognition system should provide reliable detection. Approve and determine whether that person is herself/himself or not. Biometric is used in different systems, including security of computer systems, electronic banking, mobile computing, credit cards, etc. Based on biometric a person can be identified who she/he is, what she/he has (key, cards, etc), or what she/he knows (passwords or etc). In this paper we discuss about the science of Biometric and reasons of using it and types of it, and also evaluate strengths and weaknesses of different types of it and finally by using statistical quality control we compare various biometric methods and determine which type is better.

Keywords: Security ; Biometric ; Authentication , Statistical Quality Control

INTRODUCTION

"Biometric" word is combination of two Greek words bios (life) and metrikos (estimate). Biometric science is a identification of people through his human body profile that includes fingerprints, palm, face, signature, handwriting, iris and retinal scans, and voice. Today in many areas we need devices that can identify individual human identity. Furthermore, the ID and password Cards that today are used can restrict access, but these methods can easily be broken and are therefore unreliable. Biometric cannot be borrowed, forgot, bought and it is virtually impossible to falsify it. In biometric, body members are considered that their use is more convenient and available. Each of the methods that used has strengths and weaknesses and by combining other security methods the existing weaknesses can be eliminated. A biometric system basically is a pattern recognition system that can identify a person based on her/his vector-specific physiological or behavioral characteristics. Characteristics vectors typically are stored in the database after extraction. A biometric systems based on physiological characteristics basically have high reliability. In this paper various biometric techniques and application methods are discussed and compared, also we compare different methods by using of statistical quality control.

BIOMETRIC SYSTEMS

Biometric systems should have significant percentage in reliability in order to detecting the people and give access to write them correctly. In comparison with traditional methods of identification such as passwords and ID cards, benefits of biometrics are : (1) cannot be borrowed. (2) cannot be stolen. (3) are not lost or forgotten (4) are not broken. Usually a biometric system with helping pattern recognition algorithms try to extract some characteristics (features) of the person's behavior or physiological structure and then save these features in the database (for detection and confirmation of identity). Systems that operate based on physiological symptoms are much more reliable than behavioral systems. A biometric system consists of four fundamental parts.

Sensor Module: sampling part that collect raw data needed. Like a fingerprint image.

Feature Extraction Module: processing part for feature extraction of pervious stage information.

Matching Module: will the information collected data match the pattern or not? For example, detects whether the data can be owned by a finger or not, if matched it can be stored or goes to the next stage for identification.

Decision-making Module: is a part that compare input data (features) with the data stored and if the level of similarities is above the reasonable percentage then gives permission to user , otherwise gives an error message.

biometric features that are used must have the following four characteristics:
Universality : all people have it.
Distinctiveness : not be the same in two persons.
Permanence : should not change over time.
Collectability : can be collected.

MODERN METHODS IN BIOMETRIC

In this section, conventional and non conventional methods of biometric will be introduced and details of the processing equipment and algorithms will not be introduce here, and only the advantages and disadvantages of each methods are expressed. the two fields of biometrics can be used separately: Identification: this field is trying to determine the exact identity of the person. Verification: In this field it investigate that whether the person's identity is claimed or not. Systems that are capable of identification, surely they can do to verify, but not vice versa. Biometric is divided into three groups: physical characteristics, behavioral characteristics, and chemical characteristics.

Physical characteristics

Physical assessment is based on an individual's physical characteristic in a person. Body organs assessment is the oldest identification methods which are developed with growth of technology and various methods. Other methods of this class such as diagnosed through the iris, retinal capillaries, etc can be named.
Behavioral characteristics: Behavioral techniques is based on work done by the user. Such as signing, say a phrase, signatures, typing rhythm, sound, etc.

Chemical characteristics

Chemical techniques is based on chemical property of the user, such as body odor, blood sugar, DNA, etc.

BIOMETRIC METHODS

Here we investigate some of the biometric methods.

Finger print

Lines on the fingertips of all human beings are considered by scientists for long time. On the other hand these lines for each person are unique, many years ago those fingerprints are used in criminology, and today they are used in the biometric science. The most common method that are used in biometric method is fingerprint and for using it, special fingerprint scanners are used, including: optical scanners, ultrasound scanners and semiconductor capacitors scanners. Perhaps in future, we can use fingerprint scans instead of typing password to check our emails, or exchange in e-commerce or online banks. However, fingerprint analysis of some people such as the workers who work hard with their hands or addicted people is difficult, but the entire problem in many cases for using fingerprints has been successful. “Fig. 1.a”. some types can be similar to this ,is method of palms (Palm Print) and the Foot print also can be pointed. “Fig. 1.b”.Using biometric fingerprint is the most common and inexpensive and at the same time one of the most reliable identification methods.

Hand and finger geometry

This method, finger length and diameter, and the joint location, shape and size of palms are very important . To scan the surface of the palms we can use scan page for the correct hand fitting, geography of palms after a while over the years and age and also by hand surgery will change, So by using this method the obtained scan must update when necessary and after a period and create a new scan to identify individuals. Therefore, this method is useful in cases that can be used continuously and people identified with this method are available, however, geometrical structures of different people are not really a different phenomenon and may be found in several people that they have the same profile, So this method is not used for identification among mass users and used only for confirming identity usually (after the initial identification such as fingerprints) or to enter a room in a department (Department entrance is limited by biometric methods) “Fig. 1.c”.

Face recognition

One of the investigated methods for human identification, face recognition by computer systems, which is usually identified as face recognition. In Recognizing of a face image, the input image, according to information in the database, should be recognized. The database contains characteristics of the face image of identified people. Face Recognition in image is done in two steps: (1) position and boundary of the face or

faces in the images that contain objects and different areas are recognized, (2) in the marked face of the image, the necessary feature was extracted and recognition was done. That is for example including identifying the components of the eyes and determining their positions and modes. Work performed for the extraction of image characteristics is done on two kinds of images (front images and profile images) and because the profile (lateral) images containing less information than front images, study are focused more on front images. Basically the difference and diversity in the face of people are too much so that cannot be classified in the specific categories or groups, fixed feature extraction of a face image from the features extracted arises challenges in recognizing of a face image because for example the person changes because the image conditions are changes, and due to the similarity and diversity of face images of people even sometimes the reverse face features were extracted from one person. “Fig. 1.d”.

***Retina* Scanning**

Different people have different retinal designs and each person has unique pattern of blood vessels in her/his retina and by model of the retinal blood vessels we can identify people because the pattern s of those blood vessels are different even in identical twins. So in this method identification has been done by pattern of blood vessels in the retina. A special camera can scans pattern of blood vessels in retina and it uses low-power infrared laser. Many people do not interest in this method because the laser beam used. Additionally, people think that the retina does not change over time but medical research shows that some diseases affect the retina and change its pattern. “Fig. 1.e”.

Iris

In 1936 an ophthalmologist (frank Burch) proposed the people identification by using the iris pattern. Iris of different people are totally different; the iris structure formation is started in third month of fetal, and completely stabilized in the eight months. Appearance and complex structure (Pattern) to the iris gives us the opportunity to extract many comparable features. Image of the surface of the iris is not working very hard but have making trouble. For example, if ambient light is changed or if angle of rotation of the eyes is not appropriate and also if the contrast, resolution and image focus are changed, the possibility of errors are very high. This method also has the ability to recognize to identity people. In the iris scan, a special camera is used to scan the iris vessels and according the extraction of large number of attributes and compare them; a reliable method is created “Fig. 1.f”.

Handwriting & Signature

Signature is defined as: "the name of the person by his or her written and set of quick hand movements that are labeled on paper. Features founded in a signature can be categorized in three groups, general, information networks and structure characteristics.General. characteristics, characteristics that are used in the classic pattern recognition problems. Characteristics of the networked information are calculated as the image area divided to a network includes 96 rectangular region (12 * 8) and characteristics of each region is studied separately. To obtain the structural characteristics, occurrence matrix of image signature should be used simultaneously. In this method we can also use the static mode and dynamic mode of sign to confirm identity. In dynamic methods it uses handwriting recognition and signature recognition algorithms. These methods analyze the way the individual pens for writing a word constant (signed) move. Common features for comparison are speed, direction and rate of displacement pressure of pen on touch screen or paper noted. Static feature of signature (final form of signature) is also very widely used to confirm identity and one of the first authentication methods but will not be handwriting Recognition. for recording a signature a special scanner is used, the scanner not only scans the signed form, but also scan how to measures, for example signifying the area that pen pressure is high or pen move fast to contrary to the areas that the thin line you've drawn or drawn with care and more relaxed, and by using this method forging signatures is impossible. However, this method is best used in cases where a lot of people are using their signatures otherwise this method need to be update. This method can be used in distances signing of important contract and also in banks.“Fig. 1.g”.

How to type with the keyboard (KeyStroke)

Experts believe that each person typing on the keyboard , a specific behavior pattern for typing keyboard uses. The method is also called typing rhythm. Maybe this seems a little strange but people's typing patterns are different with others, in this system, users frequently enter a specific word and the ways that they type (time intervals between the impacts of entering key) are recorded and then analyzed. This method cannot be efficiently used for identification but only to confirm the identity in some cases. This method has been used to enhance security in a number of notebook and personal computers “Fig. 1.h”.

Voice

This method is familiar for all people, because for example in telephone conversations, we can identify the other side person easily and without seeing her/him. In processing systems this field called “the Speaker Verification” and many algorithms have been introduced for this purpose. Remember Speaker Verification with Speech Recognition has a large difference. In Speech Recognition try to automatically find out the person’s (no matter who) words or a letters that have been pronounced. Researching in this field is important to give the command, training and understanding to or from robots [15]“Fig. 1.i”.

How Motion (Gait)

This method is one of the new methods that had not been officially used, and further research will be required. This method doesn’t have high accuracy and can be used where high security doesn’t need. The most important advantage of this method is that it can recognize a person identity remotely (such as images in the closed surveillance camera network), but other methods such as fingerprint biometric requires close cooperation of the person and system to record information. In this system, how movements of different organs of the body in walking are analyzed. Footpace is one of the possible behavioral actions and maybe changes over time. On The other hand, since this method requires video processing, this is a method with heavy processing and therefore it is expensive. For this reason this method is not common yet “Fig. 1.j”.

Ear

Here two forms of identification are used: ear shape and structure are different between individuals “Fig. 1.k”. Echo of output sound from the ear cannel for each individual is different with another person “Fig. 1.l”. This method didn’t have high efficiency and reliability to confirm the identity and only used in the few cases.

Vein & Vascular Patterns

In this method, images of individual vessels under the skin are produced and processed, and their structures are analyzed. The structure of the vessels is unique for different people. There are different methods for imaging; the most common of them are infrared cameras and infrared touch thermal sensors. This method is more secure than fingerprint methods and the geometric shape of hand because the shape and skin tone does not influence the outcome of this system. “Fig. 1.m”.

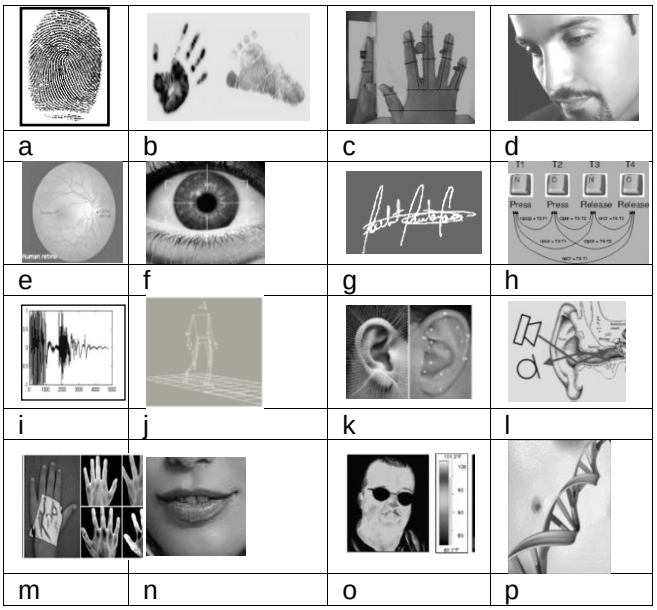

Figure1. Biometric Methods.

Lips

This type of biometric hasn't developed and applied yet. Biometric by lips used as one of the three following methods : Lips Print: Like fingerprints with the difference that edge effects of lip are recorded. Lips like fingers have similar unique curves and lines that dedicated to each individual. This method is rather reliable. Lips Movement: this method like gait is a behavioral method and helps us to recognize the speaker. This method is not precise and can be used only for confirming identity. Lips Shape: only can be used to confirm identity, and not conventional “Fig. 1.n”.

Skin Pattern Recognition

In this method , facial wrinkles is evaluated. This structure, like fingerprints is different between people.

Facial Thermo gram

In this model imaging of face is done by the infrared camera. Different parts of the face are seen in the picture based on the amount of heat and temperature (a map of the face is prepared) Since the accumulation of vessels under the skin of everybody has a different shape, the color differentiation between different parts of the face remains fixed. However, distinction and difference in color in these two maps have not changed. However, this system due to various limitations is not common yet “Fig. 1.o”.

Smile

Difference between the face in normal mode and smile mode are analyzed.

Nail

This method is completely new and extensive . research has not been done on it. By nail the two forms of biometric are used. Meat strings under the nail (Nail Bed): If we look at the soft layer under the nail at the microscopic scale, We can found that there are parallel and series bumps. This section contains capillaries, nerves and etc. over the years these bumps growth or become wider, but in each case there are existed. It is claimed that the structure and form of this strings like fingerprints and iris are unique in different people. Nail RFID: This method is used very rarely. In this method, a RFID microchip placed on the surface of the nail and calculates the capacitive properties of the upper surface of the nail and the meat surface under the nail. This capacitance for each individual is unique.

Electromagnetic spectrum of skin

In this method, by light emitting diodes (LED), a series of pure light with different wavelengths radiated to the skin surface and then by using a number photo diodes the wave intensity reflected from the skin surface is recorded and finally data are analyzed. The amount of light absorption and reflection (generally each wave proportion to its wavelength) by the skin of each person is different from others and this method is based on this story.

DNA

DNA is the basis of life that made by dioxide ribose - phosphate polymer, in fact it consists of four basic Hydrolytic including adenine, guanine, cytosine and Timidity . In fact, DNA is a chemical self constructive code. Undoubtedly Deoxyribonucleic Acid is one of the safest authentication methods. DNA, one-dimensional code and is unique to each individual. However this method is most accurate form of biometric security, but has not been used in the network and places and etc security because this method is not fast at all and a cost-effective automated process for it has not been introduced yet (the process to obtain this code, need to have some special tools and chemical materials). However, the structure of DNA is rather the same in twins and in identical twins are quite similar and this is a large drawback of this method but does not decrease the accuracy of this method for identification “Fig. 1.p”.

Display parts of the body temperature

Different parts of the body or an object, based on its type radiate amount of infrared radiation. The method is a general method to obtain the data of image and can be exploited for imaging in many fields mentioned above, such as fingerprint, palm, veins under the skin, ears, etc. In this method, the thermal radiation pattern of the individual face, hands or even individual vessels are captured by infrared camera, then appropriate processing are done. These patterns are unique to each person. To obtain this kind of raw information from individuals is not difficult but the imaging is difficult. Because, if a person is in an environment with a strong heat source or for example if a cup of hot tea placed in her/his hands, all calculations become wrong. Therefore, for using this form of biometrics, a special room is considered and certainly due to spend the time, cost and etc the user is not comfortable.

OTHER METHODS

In this section, we study and just introduce some non-conventional methods: heart and blood signals (electrocardiogram), perfume and smell of each individual (odor), Reflection of acoustic waves in the head, electrical resistance of skin (Skin impedance), the appearance fists (Knuckle creases Articulations), finger skin wrinkles (Finger wrinkles), how to grip objects (Dynamic Grip Recognition), the sound of bones taken from a finger after stimulation acoustic pulse (Bone sound transmission), magnetic waves published by the human (Bioelectric field), Eye movement tracking, the level of corneal topography (Corneal surface topography), the

three-dimensional fingerprints (3D Finger surface), signal spectrum of Brain EEG, the sinuses figure of frontal (Frontal Sinus Recognition).

COMPARISON OF USAGE OF METHODS

In this section we compare the more common biometric methods. Here shows a summary of the features of biometric identification methods .

Fingerprint: Fingerprints of people are different and its characteristics are suitable for identification. Advantages: very low error rate, 1 error in one million. Drawbacks : nuisance for user.

Face: Identifying by characteristics of individual faces. Advantages: over ten years is used. Drawbacks: large data volume raises costs and time some users have complained about to store information of their faces

Palm : This method is based on physical size of the hands and fingers work. Advantages: it used more than ten years. drawbacks: the amount of differences in some cases is not enough.

Palpitations of Heart: Devices such as electro cardio gram, records heart palpitations. It has yet to research.

Iris: laser light or infrared iris imaging is done. Advantages: very reliable with very low error, drawbacks: the fear of the user to put their eyes under light.

Retina: Imaging of the retina. Advantages: very reliable with very low error, drawbacks: the fear of the user to put their eyes under light.

Voice: Analysis of user voice. Advantages :Top users simply accept it. Drawbacks: difficulty in finding the words and paying fast, heavy and slow processing.

Key stroke: Beat of input characters are analyzed. Advantages: cheap and acceptance by users Drawbacks: time-consuming to investigate and variability of key impacts

Signature: Key features of signature. Advantages: accepted by the users Drawbacks : high and variability of speed and time signature mode

Vessels Scan: Vessels of the palm are imaged with infrared light. Advantages :simply accepted by users Drawbacks : high cost and time-consuming Biometric System Errors

Biometric system is able to confirm that you're the person who claims or not. Also it can get your information and compare it with your files that you have saved in the past, to recognize your identity. In fact, acknowledgement is compared one by one. All biometric systems use human characteristics, but which method is better and more precise is related to security levels used in the system, the number of people who use this method and accuracy of the system. Most vendors, to measure the amount of security coefficient, take the following factors and review the system to these measures :

False Accept Rate (FAR): the number of people that systems accept them incorrectly.

False Reject Rate (FRR): the number of people that system reject them incorrectly.

Failure to Acquire Rate (FTA): the number of times must a user introduce her/his feature to system till system knows her/him.

BIOMETRIC SYSTEM ERRORS

Biometric matching system return a matching score s (usually a single number) that specifies the similarity between input and database information (matching quality), The higher the value is, the more confident the system is for matching to be equal. A threshold t for the system decision is considered that the system can deduce that biometric sample pairs produced their scores is equal or bigger than t that means the person can have access to the system. If the score is less than t, i.e. there is no matching between person and pattern and she/he not have access to the system. If the scores of sample pairs are different it is called impostor distributed. If the scores of sample pairs are the same it is called genuine distributed “Fig. 2”.

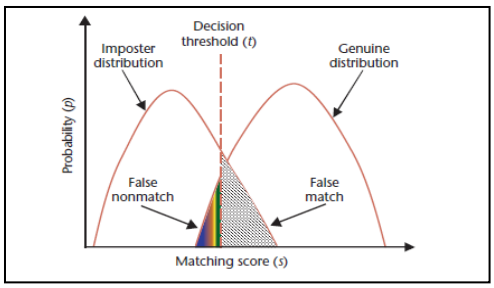

Figure2. Biometric System Error Ratess

PROPOSAL PLAN

In this paper a number of biometric methods in terms of various criteria are compared and the performance of each method are specified with Low(L), Medium(M) and High(H). “Table. 1” .Then, based on

statistical quality control (SPC) we show which biometric method is in control and which is outside the control or which method is better than the rest. For this purpose, the diagram of the Avg($\bar{x}$), standard deviation or range deviation (R) diagram of defective items (D) and control chart the number of defects (C) are calculated and then the good practices are identified. In order to draw diagrams we should score We tested each method on different samples and specified their performance on low, medium, high. the AVG ($\bar{x}_i$)of each sample, the domain(R_i) of each sample, the total avg ($\bar{\bar{x}}$) of each sample and range($\bar{R}$) of each samples are specified through the following : “Equation (1)(2)(3)(4)”.

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

$$\bar{\bar{x}} = \frac{\sum_{i=1}^{m} \bar{x_i}}{m} \quad (2)$$

$$R=XH-XL \quad (3)$$

$$\bar{R} = \frac{\sum_{i=1}^{m} R_i}{m} \quad (4)$$

m is the number of samples (13), n is the sample size (10) that is 13 sample with size 10 . also x_i is sample i, x_n is the greatest amount h and x_i is smallest amount. To obtain high and low degree of efficiency we use the upper acceptable limit (UCL) and lower acceptable limit (LCL). : “Equation (5)(6)(7)(8)(9)”.

$$ucl_{\bar{x}} = \bar{\bar{x}} + 3\sigma_{\bar{x}} = \bar{\bar{x}} + 3\frac{\sigma_x}{\sqrt{n}} = \bar{\bar{x}} + 3\frac{\bar{R}}{d_2 \times \sqrt{n}} = \bar{\bar{x}} + A_2 \times \bar{R} \quad (5)$$

$$lcl_{\bar{x}} = \bar{\bar{x}} - 3\sigma_{\bar{x}} = \bar{\bar{x}} - 3\frac{\sigma_x}{\sqrt{n}} = \bar{\bar{x}} - 3\frac{\bar{R}}{d_2 \times \sqrt{n}} = \bar{\bar{x}} - A_2 \times \bar{R} \quad (5)$$

$$X \approx N(\mu, \sigma_x) \quad (7)$$

$$\bar{x} \approx N(\mu, \frac{\sigma_x}{\sqrt{n}}) \quad (8)$$

$$\sigma_x = \frac{\bar{R}}{d_2} \quad (9)$$

A_2 and d_2 are constant coefficient and defined by the sample size in quality control table and we considered 0.31 for coefficient A_2. The diagram of average $\bar{x}$ is specified according to UCL And LCL in “Fig. 3” the quality control diagrams consist of high, low and a central degree.

In “Fig. 3” that’s methods near to centeral line ($\bar{\bar{x}}$) have avarage performance and others that near the high line have good performance and others have low performance.

We use the following “Equation (10)(11)(12)” for controlling sampling deviation range (R).

$$R \approx N(\bar{R} = d_2 \cdot \sigma_x, \sigma_R = d_3 \cdot \sigma_x) \quad (10)$$

$$ucl_R = \bar{R} + 3\sigma_R = \bar{R} + 3d_3\sigma_x = \bar{R} + 3\frac{d_3\bar{R}}{d_2} = \bar{R}(1 + 3\frac{d_3}{d_2}) = D_4\bar{R} \quad (11)$$

$$lcl_R = \overline{R} - 3\sigma_R = \overline{R} - 3d_3\sigma_x =$$
$$\overline{R} - 3\frac{d_3\overline{R}}{d_2} = \overline{R}(1 - 3\frac{d_3}{d_2}) = D_3\overline{R} \quad (12)$$

d_2 and d_3 and D_3 and D_4 are constant coefficient that's are variable by sampling size in quality control table. samples range control diagram are show in "Fig. 4" and it is clear that all samples are in control, for analyzing methods we use "Fig. 3" and "Fig. 4" that are four categories on the following : (1) Iris .(2) Fingerprint, hand geometry, retina, hand veins, DNA .(3) Sound, face, smell, ear .(4) Signature, walking. In conclusion first category has the best performance and other categories in order have decreasing efficiency.
decreasing efficiency.

Calculation based on Lower performance methods (P)

In this part all points out of limit control threshold are more commonplace and we should omit them, because their cost are not reasonable, We should use following "Equation (13)(14)(15)(16)" to draw the "Fig. 5"

$$\overline{p} = \frac{\sum D_i}{mn} \quad (13)$$

$$P_i = \frac{D_i}{n} \quad (14)$$

$$ucl_{\overline{p}} = \overline{p} + 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}} \quad (15)$$

$$lcl_{\overline{p}} = \overline{p} - 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}} \quad (16)$$

D_i identifies failures i

In this diagram UCL is acceptable high limit, LCL is acceptably low limit and $\overline{P}$ The central plot line because it is for defective methods in any way the methods are better if the points are closer to LCL and the more closer to UCL the higher percentage of defective of method. According to the "Fig. 5" Signature and walking template are out of the control methods can be concluded that both methods don't have high accuracy and efficiency rate and they are not reasonable. Accordingly, we can act in two ways: (1) These two methods can be eliminated and the cost is spent on improving them spent on other methods. (2) These two ways can be improved to reach the control threshold.

TABLE1. THE COMPARISONS OF BIOMETRIC CHARACTERISTICS

Biometric Characteristic H:High M:Mediom L:Low	Universality	Uniqueness	Stability	Non-Imitation	Ability/ Collect	Comparability	Performance	Reliability	Relative Cost	Acceptance
Fingerprint	M	H	H	H	H	H	H	H	M	M
Palm Geometry	M	H	H	H	H	H	H	H	M	M
Retina	H	H	H	H	M	H	H	H	M	L
Voice	M	M	H	M	H	M	L	L	M	L
Iris	H	H	H	H	H	H	H	H	M	M
Palm Vessels	H	M	H	H	H	M	M	H	M	M
Signature	L	L	L	L	M	M	L	L	M	M
Face	H	M	M	L	H	M	M	M	H	M
Temperature	H	H	L	H	H	L	M	M	M	H
Odor	H	H	H	L	L	L	L	M	M	M
DNA	H	H	H	L	L	M	H	H	M	L
Walking	M	L	L	L	L	M	H	L	M	L
Ear	M	M	H	M	M	M	M	M	M	L

THE AVERAGE PERFORMANCE OF CONTROL DIAGRAM METHODS(C)

Here, some methods have faults that cause efficiency of these methods become low and we should identify defects. In the "Fig. 6", the M is fault. a defective method means that it has many faults. "Fig. 6"is

poisson distribution. In the performance methods control diagram, the average number of defects of all methods is in control. With using comparison of “Fig. 5”and “Fig. 6” it is clear that witch method has a higher efficiency. By this way we choose the lower and average performance methods. In “Fig. 5” the least defect way of methods are fingerprints, hand geometry, iris, hand vein. and in the “Fig. 6” least defect methods are retina, iris, DNA. The iris is the most common way of these two diagrams. The second group of methods fingerprints, hand geometry, retina the third group of methods are hand vein and face. The fourth group is body temperature and ear The fifth group is sound, smell, DNA the sixth group is signature and walking.

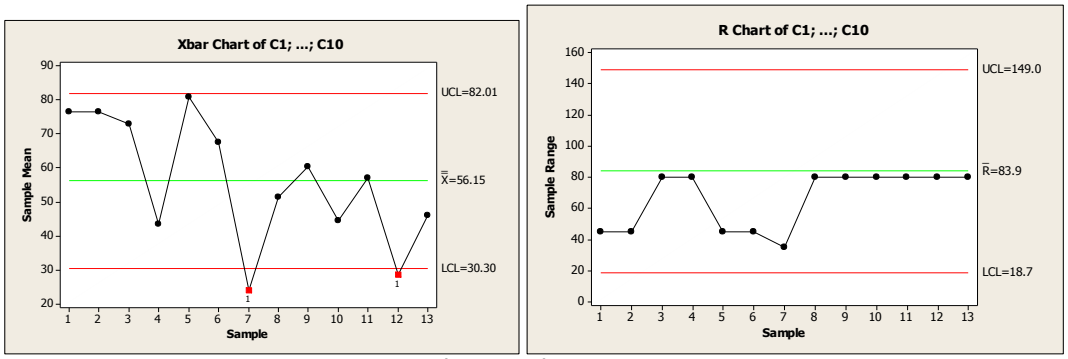

Figure3. Diagram R

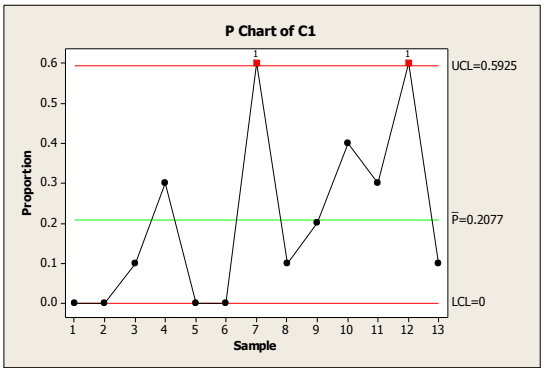

Figure4. Diagram P

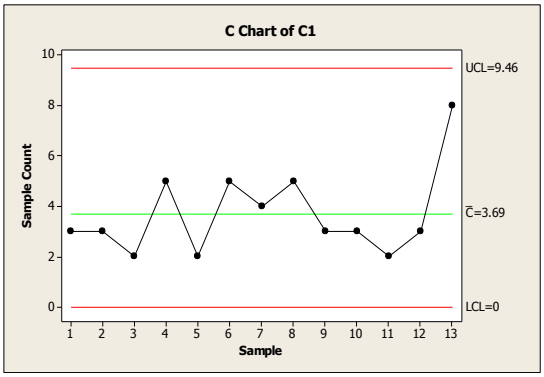

Figure5. Diagram C

CONCLUSION

Biometric offers reliable, non-counterfeit or non-copied methods, especially in cases where information is critical. Some methods have been considered by many organizations today. Applications of biometrics technology are far beyond just to allow a person to issue a special place. Experts are predicting that in the not too distant future, newer techniques are used to identify individuals through biometrics, such as nails and teeth of the original structure, shape of ears, body odor, skin pattern and pulse pattern. In conclusion, If the new method is developed, on the base of the relationships in this paper it can be tested to see whether it is accepted or not .

REFERENCES

Al-Assam H, Jassim S. 2012.Security evaluation of biometric keys. Elsevier 31 P. 151-163,

Anne MP, Canuto FP. 2013.Investigating fusion approaches in multi-biometric cancellable recognition , Elsevier 40 , P. 1971–1980,

Delac K, Grgic M. 2004.A Survey Of Biometric Recognition Methods,46th International Symposium Electronics In Marine, P.16-18 June 2004, Zadar, Croatia , Elmar-

El-Bakry HM, Mohamed H. 2009.Fast Principal Component Analysis For Face Detection Using Cross-Correlation And Image Decomposition, Proc. Of Ieee Ijcnn'09, Atlanta, Usa, June 14-19, P. 2296-2303,

El-Bakry HM, Qiangfu Z. 2004.Face Detection Using Fast Neural Processors And Image Decomposition, International Journal Of Computational Intelligence, Vol.1, No.4, P. 313-316,

ELMIR Y. 2012.Score Level Fusion Based Multimodal Biometric Identification (Fingerprint & Voice) , IEEE.

Girija Ch,d Jucheng Y. 2011.ADVANCED BIOMETRIC TECHNOLOGIES , July,

Hariprasath S. 2012.Multimodal Biometric Recognition Using Iris Feature Extraction and Palmprint Features , IEEE.

Heng FL, Dino I. 2011.Feature selection for support vector machine-based face-iris multimodal biometric system , Elsevier 38 P. 11105–11111,

Jain AK, Ross A, Prabhakar S. 2004An Introduction To Biometric Recognition, Ieee Trans. On Circuits And Systems For Video Technology, Vol. 14, No. 1, P. 4-19, January.

John D, Cathryn D. 2008.Effect Of Severe Image Compression On Iris Recognition Performance, Ieee Transactions On Information Forensics And Security, Vol. 3, No. 1, March

Jucheng Y, Loris N. 2011.STATE OF THE ART IN BIOMETRICS , July,

Jucheng Y, Norman P .2011.ADVANCED RECENT APPLICATION IN BIOMETRICS , July,

Libor M. 2003.Recognition of Human Iris Patterns for Biometric Identification , The University of Western Australia,

Ma L., Tan T, Wang Y, Zhang D. 2004. Efficient Iris Recognition By Characterizing Key Local Variations Ieee Transactions On Image Processing, Vol. 13, No. 6, June

Nicolae D. 2009..A survey of biometric technology basedon hand shape , Elsevier 42 P. 2797 – 2806,

Pathak A, Kumar Z, David D. Handgeometry Recognition Sing Entropy-Based Discretization, Ieee Transactions On Information Forensics And Security, June 2007, V. 2, No. 2, P. 181-187, Jun-2007.

Sana A, Gupta P, Purkait R. 2007.Ear Biometrics: A New Approach. Paper Presented At The Sixth International Conference On Advances In Pattern Recognition Held At Indian Statistical Institute, Kolkata, January 2-4

Sanchez-Reillo R, Alonso-Moreno R.2012. Standardised system for automatic remote evaluation of biometric algorithms , Elsevier 34 P. 413–425,

Soliman HH, Atwan A, Abd Elnasser S.2008.Biometric Identification Using Palm Vein Recognition, Mansoura Journal For Computer Science And Information Systems, Vol4, No. 4, Jan

Sonkamble S, Thool R, Sonkamble B. 2005 – 2010. Survey Of Biometric Recognition Systems And Their Applications, Journal Of Theoretical And Applied Information Technology © Jatit. All Rights Reserved.

Sulochana Sonkamble DrRC, Thool BS. 2008.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 ,

Teddy K. 2005Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition , IEEE.

Wei Han, Cheong- Fat Chan, Chiu Sing Choy And Kong Pang Pun, An Efficient Mfcc Extraction Method In Speech Recognition, IEEE 2006.