ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18714-18717

Multilevel and Biometric-Graphical Secure Authentication System Using Pattern Matching and Gene Based Data Extraction

Soriful Hoque
North Eastern Electric Power Corporation Limited,
Shillong, Meghalaya 793003, India
soriful.hoque@neepco.co.in

Abstract: ***In computer science considering the large scale network and increasing number of application, the protection and security of the system is essential. The Information Technology System is improving day by day. The growing concern of computer science technology creates problem for identity theft problems, hence protection and computer system security is playing vital role. The conventional alphanumeric password protection system is very vulnerable. This kind of alphanumeric password can be traced and difficult to remember for the system user. This leads to a new era of protection and security system in case of authenticity in computer science. In this paper, it is proposed to have very user-friendly secure multilevel biometric graphical authentication system. This kind of authentication system is easy for authorized user but very difficult to un-authorized user to trace. The multilevel and biometric-graphical secure authentication system algorithm described here uses more than one level of authentication system such as face detection, DNA finger printing, image pattern matching and alphanumeric password with image pattern. This algorithm based on entities that are actually bound with the individual at a much secure level than. As a result, they are more reliable since biometric information cannot be lost, forgotten, or guessed easily.***

Keywords: Face detection, pattern matching, DNA pattern matching, image-warehouse and alphanumeric-image pattern.

1. Introduction

Biometrics system is being used in the identification of individuals based on some physical attribute. The physical attributes may be the finger print, face detection, retina scanning and voice detection. This system is widely used in authentication system. The traditional system of alphanumeric password and PIN no protection system in magnetic flip can be damaged and can be read by decoding the flip and can be forgotten and disclosed any time. The biometric technology provides a strong user-friendly authentication solution. The combination of biometric and other protocols can provide a sophisticated highly secure system. Biometrics technology more efficient way of authentication than the more common use of passwords, smart cards, or a combination of the two. The system user need not required to remember the series of passwords. Normal alphanumeric password expires after certain interval of time and need to assign again hence keeping tract is also difficult. Software industries, research institutes, banking organization where the protection and security of the system is extensively experiences for the sensitive data and applications and for all kind of application and systems there may be series of passwords. As a result for ease of use with high level user friendly security system can only be the solution in such case.

The biometric face detection and pattern matching technique is very latest and effective technique to provide high level security. The pattern matching technique is convenient to use in this system of authentication and is very unique. In case of face detection algorithm human face with all its facial appearances including node point, eye, forehead, cheeks etc i.e identification of facial points (nose, eyes, checks, lips, ears etc.) will form one unique pattern for every individual and the analyzing and comparing with pattern matching algorithm this pattern can be identified easily. In case of DNA finger printing this system will extract DNA pattern from skin cell and as well as finger pattern in digital format. And these can easily be matched and compared with the help of pattern matching and gene based clustering technique.

The graphical based user authentication system is very convenient to use in authentication system for easy use. In the paper, it is considered to have an image warehouse for huge collection of images, graphical designs based on the users. Once the user select the graphical password mode the image warehouse will be shown and the user can select the images and can mark them and can arranges as according or draw shape on the image as desired and the mark as graphical password.

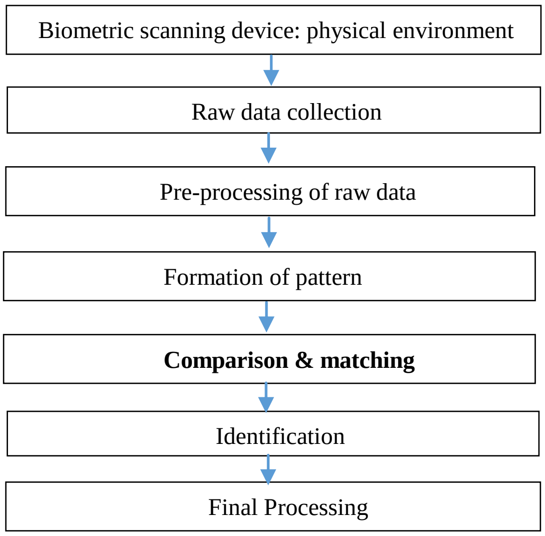
The alphanumeric graphical pattern in this case the user can type the common words as desired like pet name, mother name, birth place etc on the image pattern and marked as alphanumeric graphical password.

This paper illustrates the multilevel highly secure password protection system including face detection, DNA fingerprinting, graphical image pattern and alphanumeric image pattern password protection system.

2. Pattern matching technique using Gradient & Pearson co-efficient method:

Pattern is considered as unique sequence of data. It is extracted from the raw input data that is collected from the biometric device.

The following process is involved in the pattern recognition:

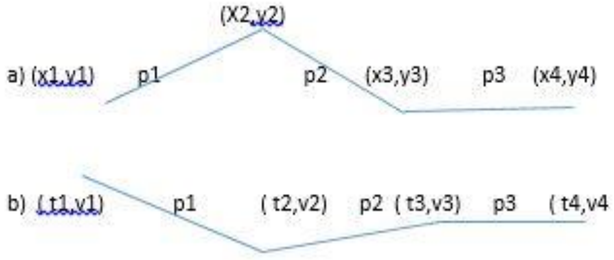


Physical environment: In this environment physical biometric data is collected like face detection, finger print etc. These data are stored in digital format. These data consists of noise data also i.e unwanted signal pattern which can be removed in the pre-processing phase.

Raw data collection: The raw data collected from the biometric device are arranged in sequential manner in binary format. The binary data is converted to decimal format and with these decimal format sequential data a grid is formulated for grid based analysis.

Pre-processing of raw data: The collected raw data consists of noise data. The noise data is removed before from the sequential grid. The nosy data can be identified by the comparing nearest sequential data difference. The difference of sequential data is categorized as +1, 0 and -1. The data difference beyond this range are identified as noisy data and are removed and rearranged the grid.

Formation of pattern: The pattern formation is done by finding the slope or gradient of the consecutive points and formed one two dimensional matrix. For example,



The slope between two coordinates of pattern (a) & (b) can be calculated as, Gm(slope)=(Y2-Y1)/(X2-X1) .

The slopes of consecutive coordinates of the patterns is stored in the two dimensional matrix as below

	p1	p2	p3
a	+0.52	-0.64	0
b	-0.34	+0.24	-0.12

Comparison & matching: The comparison and matching of the patterns can be done with Pearson's Correlation Coefficient Algorithm. Pearson's correlation coefficient measures the linear relations or association between two variables X and Y, giving a value between +1 and −1 inclusive, where 1 is total positive correlation, 0 is no correlation, and −1 is total negative correlation. This algorithm identifies how much similar are the two variables X and Y.

The formula for calculating Pearson's correlation coefficient [ρ (rho)] is mentioned below:

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y}$$

where:

cov is the covariance

σ_X is the standard deviation of X

The formula for ρ can be expressed in terms of mean and expectation.

The covariance can be calculated as below:

$$\operatorname{cov}(X,Y) = \mathrm{E}[(X-\mu_X)(Y-\mu_Y)]$$

The standard deviation of X can be calculated as below:

In the case where X takes random values from a finite data set x1, x2, ..., xN, with each value having the same probability, the standard deviation is

$$\sigma = \sqrt{\frac{1}{N}\left[(x_1-\mu)^2+(x_2-\mu)^2+\cdots+(x_N-\mu)^2\right]}, \text{ where } \mu = \frac{1}{N}(x_1+\cdots+x_N),$$

Then the formula for ρ can also be written as

$$\rho_{X,Y} = \frac{\mathrm{E}[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X \sigma_Y}$$

where:

cov and σ_X are defined as above

μ_X is the mean of X

E is the expectation.

For the pattern (a) and (b) the Pearson's Correlation Coefficient (ρ) value can be calculated as below:

µ(mean) value for pattern a: [+0.52 +(-0.64)+ 0]/3=-0.04

µ(mean) value for pattern b: [-0.34 +0.24+ (-0.12]/3=-0.07

Standard Deviation for pattern a:

σ(a)=1 /3(√[0.52-(-0.04)]2+[-0.64-(-0.04)]2+[0-(-0.04)]2)
=0. 2250

Standard Deviation for pattern a:

σ(b)=1 /3√[-0.34-(-0.07)]2+[0.24-(-0.07)]2+[-0.12-(-0.07)]2)
= 0.0898

Hence Pearson's Correlation Coefficient (ρ) for point p1 of pattern a and b.

ρ (a,b) for p1= { 0.52-(-0.04)}{-0.34-(-0.07)}/(0. 2250 x 0.0898)

ρ (a,b) for p1<0, hence part p1 for a and b pattern are negatively co-related.

The calculated Pearson's Correlation Coefficient (ρ) are categorized in the following ranges:

$$\text{If} \quad \begin{matrix} \rho < 0 \\ =0 \\ >0 \end{matrix} \left.\vphantom{\begin{matrix} a \\ b \\ c \end{matrix}}\right\} \begin{matrix} -1 \\ 0 \\ +1 \end{matrix}$$

Considering these ranges the two dimensional matrix can be formulated as mentioned below which called Regulation Matrix is:

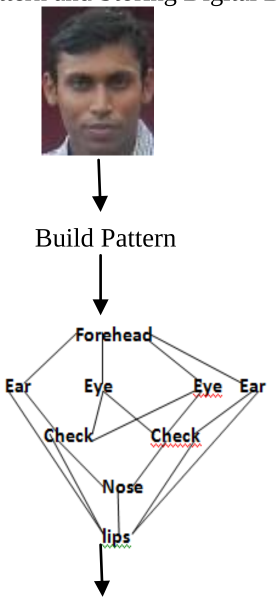
$$\begin{array}{c|ccc} & p1 & p2 & p3 \\ \hline a & -1 & -1 & 1 \\ b & -1 & -1 & 1 \end{array}$$

From the above regulation matrix the two patterns (a) and (b) can easily be compared. The two parts p1 & p2 of pattern (a) and (b) have negative correlation and part p3 has positive correlation i.e p3 of both patterns is similar.

3. The Algorithm

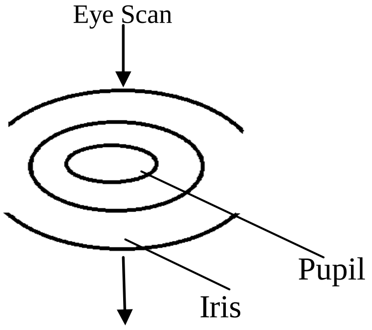
a) Face detection:

1. Face will be detected through high resolution camera.
2. Digital Image Processing.
3. Identification of facial points (nose, eyes, checks, lips, ears etc.)
4. Building pattern and Storing Digital Data to Database.



b) Eye Scanning:

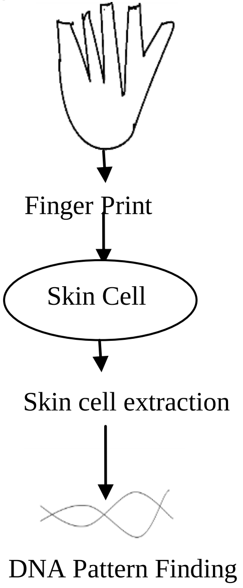
1. Scan Eye with fine camera.
2. Digital Image Processing.
3. Distinctly Identify Retina and Pupil Location.
4. Building Pattern and Storing Digital Data to Database.



Location Identification

c) DNA Extraction:

1. Biometric Finger Print System
2. DNA Can be Extracted from Skin i.e. Finger Print.
3. Every Individual has unique DNA pattern.
4. After getting DNA Pattern Store Digital Data to Database.

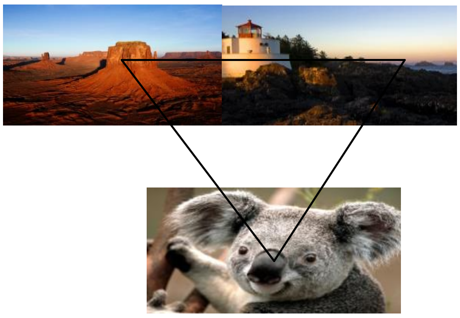


d) Graphical Password:

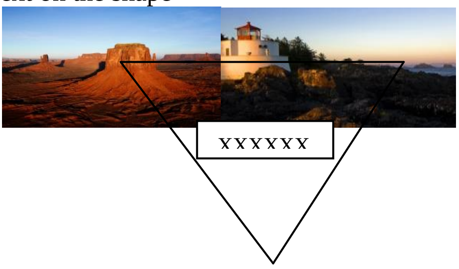
1. Image Warehouse
2. User will select Images.
3. After selection User can form one Pattern or can enter text on that Pattern.
4. Image with Pattern and Text will store in the Database.

i. Image Gallery

ii. Choose Images & Join Centre Points in sequence and Make a Shape



iii. Write text on the shape



4. Conclusion

The objective of these paper is to build an authentication system which is secure and user friendly. The system designed here to provide multilevel high security authentication system. It has been observed that in today's world the most vulnerable aspect of the system is security and security system should be convenient for the system user but difficult to predict for system hacker and non-authenticate user. The traditional alphanumeric password can easily be predicted and hence vulnerable to use in system. It is difficult to remember for system user the alphanumeric password when system user uses complex alphanumeric password. The biometric pattern is unique identity that only restricted to user only. This is one high level security system and very easy to remember. After that the graphical password option user can select some pictures which he can easily remember and can join them in suitable structure as he like. This is second level of security which is also easy for system user but difficult to predict for non-authenticate user. The algorithm designed here is implemented by using the concept of gradient and Pearson co-relation method. The gradient concept is used here to form patterns and the similarity of these patterns are identified by using the Pearson co-relation method. Every set of biometric and graphical pattern is stored in two dimensional matrix. Checking and identification can easily be done simple comparison algorithm and hence the authentication can be checked and allowed user to access the system only after successful matching and security scan. The system developed give idea and fulfil all basic user requirements for simple use of graphical and biometric password. There is always a scope for improvement of any algorithm designed, how efficient and fruitful the system may be. The most important aspect of the system is that how flexible is the system to adapt the future modifications. This system has factored into different sections and modules to adapt any further modifications. All possible efforts has been put forward to make system efficient and user-friendly. This work presents a multilevel and biometric-graphical secure authentication system using pattern matching and gene based data extraction which easily reflects our effort to design the system efficient and user-friendly.

References

[1] Banfield J. D. and Raftery A. E.: "Model based Gaussian and non-Gaussian clustering", Biometrics 49, September 1993, pp. 803-821.

[2] Byers S. and Raftery A. E.: "Nearest Neighbor Clutter Removal for Estimating Features in Spatial Point Processes", Technical Report No. 305, Department of Statistics, University of Washington. [Available at http://www.stat.washington.edu/tech.reports/tr295.ps]

[3] Devore J. L.: 'Probability and Statistics for Engineering and the Sciences', Duxbury Press, 1991.

[4] Ester M., Kriegel H.-P., Sander J., Xu X.: "A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise", Proc. 2cnd Int. Conf. on Knowledge Discovery and Data Mining, Portland, Oregon, 1996, AAAI Press, 1996

[5] Ester M., Kriegel H.-P., Xu X.: "Knowledge Discovery in Large Spatial Databases: Focusing Techniques for Efficient Class Identification", Proc. 4th Int. Symp. On Large Spatial Databases, Portland, ME, 1995, in: Lecture Notes in Computer Science, Vol.951, Springer, 1995, pp.67-82.

[6] Fayyad U. M.,.J., Piatetsky-Shapiro G., Smyth P.: "From Data Mining to Knowledge Discovery: An Overview", in: Advances in Knowledge Discovery and Data Mining, AAAI Press, Menlo Park,1996, pp. 1 - 34.

[7] Gueting R. H.: "An Introduction to Spatial Database Systems", in:The VLDB Journal, Vol. 3, No. 4, October 1994, pp.357-399.

[8] Kaufman L., Rousseeuw P. J.: "Finding Groups in Data: An Introduction to Cluster Analysis", John Wiley & Sons, 1990.

[9] McKenzie M., Miller R., and Uhrhammer R.: "Bulletin of the Seismographic Stations", University of California, Berkeley. Vol.53, No. 1-2.

[10] Muise R. and Smith C.: "Nonparametric minefield detection and localization", Technical Report CSS-TM-591-91, Naval Surface Warfare Center, Coastal Systems Station.

Author Profile

Soriful Hoque received the B.E. degree in Computer Science & Engineering from Jorhat Engineering College, Jorhat, Assam, and India in 2010. During 2010-2011, he worked as Software Engineer, during 2012-2013, he worked as Assistant Professor at AMU, Aligarh, India and during 2013 he worked as Junior Research Fellow in Speech Processing & Acoustic and tonal features of languages at IIT Guwahati, Assam, and India. He is now working as Officer-IT at NEEPCO Ltd., Shillong, India.