International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 22nd Sept2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **IMPLEMENTINGELLIPTIC CURVE BASED KEY GENERATION USING BIOMETRICS**

Volume 06, Issue 08, Pages: 312– 319.

Paper Authors

P.SAI SOWJANYA,DR.O.SRINIVASA RAO

UCEK, JNTK, Kakinada.

IMPLEMENTINGELLIPTIC CURVE BASED KEY GENERATION USING BIOMETRICS

[1]P.SAI SOWJANYA, [2]DR.O.SRINIVASA RAO

[1]M.Tech (CSE) student, Dept of CSE, UCEK, JNTK, Kakinada

[2]Associate Professor, Dept of CSE, UCEK, JNTUK, Kakinada

ABSTRACT-

Now a day's online exam has become one of the prominent and most important aspects of our lives, but there is no guaranty of genuinity of the result in the online examination processes. In many of online examinations the location of the proctor varies from the location of the examinee, there is no guaranty in the authorization of users to the examination and no guaranty in trusting the examination center head that monitors the students during the examination process. Due to the increase in the distance, chances of doing malpractice and misbehaving during the examination increases. To avoid such situations, the examinee has to be constantly monitored and should able to stop the examination based on learner's behavior during the examination. Many techniques were proposed for providing security during conduct of exams. This paper studies various authorization and authentication techniques namely unimodal, multimodal, hardware interaction and data visualization techniques. The paper also proposes a Biometric Device Based Fraud Detection based Online Test [BFDOT] and Behavior identification through Visualization Techniques [BIVT] that avoids and performs more effectively compared with the existing systems.

KEYWORDS- Fraud Detection, Behavior identification, malpractice, Data Visualization, Biometric Devices.

I INTRODUCTION

In online exams the location of the proctor and examinee are at different locations since the communication is through online using internet. Due to the increase in the distance, chances of doing malpractice increases and identification of misbehaviors of the examinees is quite difficult. To avoid such situations, the examinee behaviors have to be constantly monitored during the time of examination. The first step of Monitoring can be done by using authentication techniques i.e. identifying the examinee is correct person who is having eligibility to write the exam, sometimes the person who was registered for the exam is different from person who is writing the exam. So that authentication plays a major role in identifying the correct user,this is done by an providing username and password, biometric methods like face, finger prints, iris identification techniques and any group cryptography techniques. Authentication is a process that permits an entity to establish its identity to another entity [1]. Authentication methods are of three types namely passwords, tokens and biometrics. With the use of passwords, only authenticated users are logged in. Conditions such as, the password should contain minimum of eight characters; one letter, one number, one special character etc are provided to make the passwords strong enough for intruder attacks. Passwords should be often changed to avoid the risk of stealing and guessing. The second mode of authentication is the use of tokens. Some of the applications of the tokens are physical keys, proximity cards, credit cards, Asynchronous Transform Mode (ATM) cards. They are simple in usage and easy to produce. To avoid the risk of stealing, these tokens are used along with the Personal Identification Number (PIN). The last mode of authentication is biometrics. In this method the user enrolls by providing a sample physical characteristic, which is converted from analog to the digital form. This conversion is stored in a template, which is later verified with the new sample provided by the user at the time of authentication. If the two samples match with a slight variance then the user is authenticated. Biometrics authentication can be applied in the fields of facial recognition, finger prints, hand geometry, keystroke dynamics, hand vein, iris, retina, signatures, voice, facial thermo gram, Deoxyribonucleic acid (DNA). There are a varying number of authentication systems namely central authentication systems, multi factor authentication system, split authentication system and message authentication system. Central authentication system authenticates users remotely using a central authority system across large number of systems. Applications of this system are Remote access dial in user service, Terminal access controller access control system, Kerberos and Diameter. The multi factor authentication system combines multiple authentication factors into a single model, thus increasing the reliability and security. Application of this system is usage of ATM card with PIN number. Split authentication system, splits the authentication among two parties. The two parties should submit their passwords or cryptographic keys to encrypt or to decrypt a message. In Message authentication system, the message is authenticated by using message authenticated code (MAC). The message authenticated code is generated by combining message with a secret key shared by both the sender and the receiver. On receiving the message, the receiver recomputed its own MAC and compares it with received MAC. If any change is found, then the message is said to be altered. Digital signatures are used to ensure authenticity and non-repudiation. The term data visualization can be described as the graphical representation of the given data. It makes an overview of entire data, thus making the viewers to easily interpret the data.Animationhelps in the representation of the data by showing thevariation of the plot with respect to time. For visualizing high dimensional data, icon based, hierarchical, geometrical and pixel oriented techniques are used [3]. In icon based, there are a number of varying techniques namely churn off faces, star glyphs, stick figure, shape coding, color icon, texture. Chertoff face represents a data set and each feature in the face represents a dimension. Star glyph represents data by using a single point with equally angled rays. Here each ray represents a dimension, and the length of the ray represents the value of the dimension. Stick figure maps two attributes to the display matrix and the remaining to the length, thickness, color of limbs. In Shape coding each data item is visualized by using a pixel of arrays. According to the attribute values the pixels are mapped onto a color scale which helps in visualization of the multi dimensional data. In color icon, the pixels are replaced by arrays of color fields that represent the attribute values. Texture helps to gain knowledge about the overall relation between the attributes in addition to the data items. Section 2 summarizes the methods introduced far for providing security during conduct of online exams.

II RELATED WORK:

There are a number of methods available in hierarchical techniques namely dimensional stacking, fractal foam, hierarchical axis, worlds within worlds, tree map [2][3]. Dimensional stacking divides the given data into two dimensional subspaces which are stacked into each other. Later from those subspaces, only attributes are chosen for visualization. This technique is useful for discrete categorical or binned ordinal values. Fractal foam depicts the correlation between the dimensions by the usage of circles. The starting dimension is represented in the form of circle. Later other circles are attached to the first circle, which represent the other dimensions. The size of the circles represents the correlation between the dimensions. In Hierarchical axis the axis is applied in a hierarchical manner. This technique helps in plotting many attributes on one screen. Worlds within Worlds divides the given data space into three dimensional subspaces. This technique helps in generating an interactive hierarchy display, which allows the further exploration of n-dimensional functional spaces. Tree map divides the given screen into a number of regions based upon the attribute values, in a hierarchical fashion. It helps in obtaining an overview of large datasets with multiple ordinal values.The varying techniques in geometrical methods are parallel coordinates, Andrew's curves, multiple views, radical coordinate visualization, polyviz, hyper slice, hyberbox, star coordinates, table lens[2][3]. Parallel coordinates makes use of the parallel axes in representation of the dimensions. A vertical line is used for projection of each dimension or attribute. Andrew's curves plot each data point as a function of data values, by using the equation

$$F(t) = x\frac{1}{\sqrt{2}} + x2.\sin(t) + x3.\cos(t) + x4.\sin(2.t) + x5.\cos(2.t) + \cdots,$$Equation 1 [2]

Where, x= (x1,x2,…xn) and xn are the values of the data points for the particular dimension. Multiple views are used for the data sets that contain diverse attributes. This method reveals the correlation and disparities between the attributes thus making a visual comparison for better understanding. In Radical coordinate visualization, n number of lines extends from the centre of the circle and end at the perimeter. Each line is associated with one attribute. Data points with similar or equal values lie close to the centre. Polyviz technique represents each dimension as a line. The position of the data points depends upon the arrangement of the dimensions. This technique provides more information by giving an inner view of data distribution in each dimension. Hyper slice contains the matrix graphics representing a scalar function of the variables. This technique provides an interactive data navigation over a user defined point. Hyper box is depicted in two dimensional data space. This technique is helpful in mapping variables to the size and shape of the box. In star coordinates technique, the data items are represented as points and attributes are represented by axis arranged on a circle. The length of the axis determines the attribute contribution. Table lens technique uses rows and columns for representing the data items and attributes. The information among rows and columns is interrelated which helps in analyzing the trends and the correlation in the data. The methods that were included in pixel oriented techniques are namely space filling curve, recursive pattern, spiral and axes technique, and circle segment and pixel bar chart [3]. Space filling curve provides clustering of closely related data items, thus making the user to easily understand the data. Recursive pattern follows a generic recursive scheme where, the arrangement of line and columns are performed iteratively and recursively. Spiral techniques arrange the pixels in a spiral form, depending on the distance from the query. Axes techniques improve spiral techniques, by adding feedback to the displacement. In circle segment the attributes are arranged on the segments. The data point that is assigned is available at the same location on different segments. Pixel bar chart presents the direct representation of the data

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

values. Each data item is represented by a single pixel and is placed in the respective bars. Color is the widely used feature in the feature extraction process [4]. The following are the advantages of using color feature namely robustness, effectiveness, implementation simplicity, computational simplicity, low storage capability. The color of an image is represented through color model. A color model is specified in terms of 3-D coordinate system and a subspace within that system where each color is represented by a single point. There are three color models namely RGB, HSV, Y C_b C_r. RGBcolors are called primary colors and are additive. By varying their combinations, other colors can be obtained. In HSV, the representation of the HSVspace is derived from the RGB space cube, with the main diagonal of the RGB model as the vertical axis in HSV. As saturation varies from 0.0 to 1.0, the colors vary from unsaturated (gray) to saturate (no white component). Hue ranges from 0 to 360 degrees, with variation beginning with red, going through yellow, green, cyan, blue and magenta and back to red. HSV is calculated by using the formula

$$H = \cos^{-1}\left\{\frac{\left(\frac{1}{2}[(R-G)+(R-B)]\right)}{\sqrt{(R-G)^2+(R-B)(G-B)}}\right\} S$$

$$= 1 - 3[\min(R,G,B)\,]/V$$

V=1/3(R+G+B)

Equation 2 [4]

YC_bC_r is a color space used in the JPEG and MPEG international coding standards. Formula used in calculation is Y = 0.299R+0.587G+0.114B

C_b= -0.169R-0.331G+0.500B

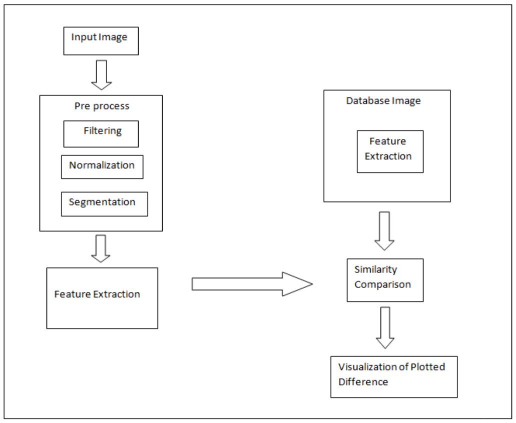
C_r = 0.500R-0.419G-0.081B Equation 3 [4]

The second feature that can be extracted from an image is texture [4].Texture has been one of the most important characteristic which has been used to classify and recognize the objects and have been used in finding similarities between images in multimedia databases. Texture alone cannot find similar images, but it can be used to classify textured images from non-textured ones and then be combined with another visual attribute like color to make the retrieval more effective. There are 4 methods in texture extraction namely statistical, geometrical, model based, signal processing methods[5].Statistical methods help in defining the qualities of texture in the spatial distribution of gray values. We use {I(x,y),0<=x<=N-1,0<=y<=N-1}to denote N*N image with G gray levels. In statistical methods we have 2 types namely co-occurrence matrices and auto correlation features. In Co –Occurrence Matrix, Spatial gray level co-occurrence estimates image properties related to second-order statistics. The gray level co-occurrence matrix P_d for a displacement vector d = (dx, dy) is defined as follows. The entry (i,j) of P_d is the number of occurrences of the pair of gray levels ofi and j and which are a distance ‘d’ apart. Formally, it is given as $P_d(i,j) = |\{((r,s),(t,v): I(r,s) = I, I(t,v) = j\}|$Equation4 [5] where, (r, s), (t, v) € N*N, (t, v) = (r + dx, s+ dy), and │.│ is the cardinality of a set. The second type is the auto correlation feature, which is used to assess the amount of regularity as well as the fineness/coarseness of the texture present in the image. Formally, the autocorrelation function of an image I (x,y) is defined as follows:

$$\frac{\sum_{u=0}^{n}\sum_{v=0}^{n}\left(I(u,v)I(u+x)(v+y)\right)}{\sum_{u=0}^{n}\sum_{v=0}^{n}I^2(u,v)} \quad \text{Equation5 [5]}$$

III PROPOSED SYSTEM

In this paper a multimodal technique is proposed for providing security. This includes authentication of the student at the beginning of the exam and later continuous monitoring of the student through webcam. The detection and comparison of the student’s face and behavior is done in two steps. Firstly preprocessing is done to the image through filtering, normalization and segmentation. Later in the second step, feature extraction is done based on the color, texture and shape of the obtained image.



The technique that is implemented in the feature extraction is Discrete Cosine Transformation method. Then these obtained features of the input image are compared with the features of the database image through Euclidean distance measure. Later the plotted difference is represented by using two dimensional data visualization techniques. Through these plots, the proctor can easily visualize any change noted in the student behavior. This approach thus employs a full time security for online exams.

Figure1: Architecture for Fraud Detection based Online Test [FDOT] and Behavior identification through Visualization Techniques [BIVT]

KEY GENERATION:

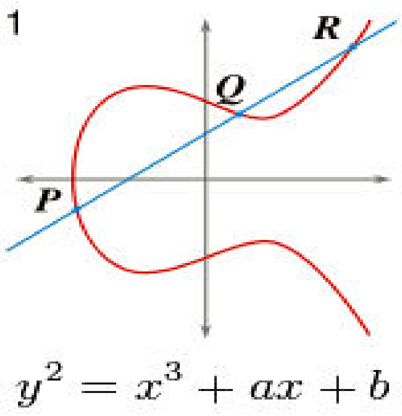


Fig 3 The fig 3 show is simple elliptic curve.

The equation of an elliptic curve is given as, $y^2≡(x^3+ax+b)$ mod P Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd'within the range of **'n'**.

Using the following equation we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and'd' **is the private key.**

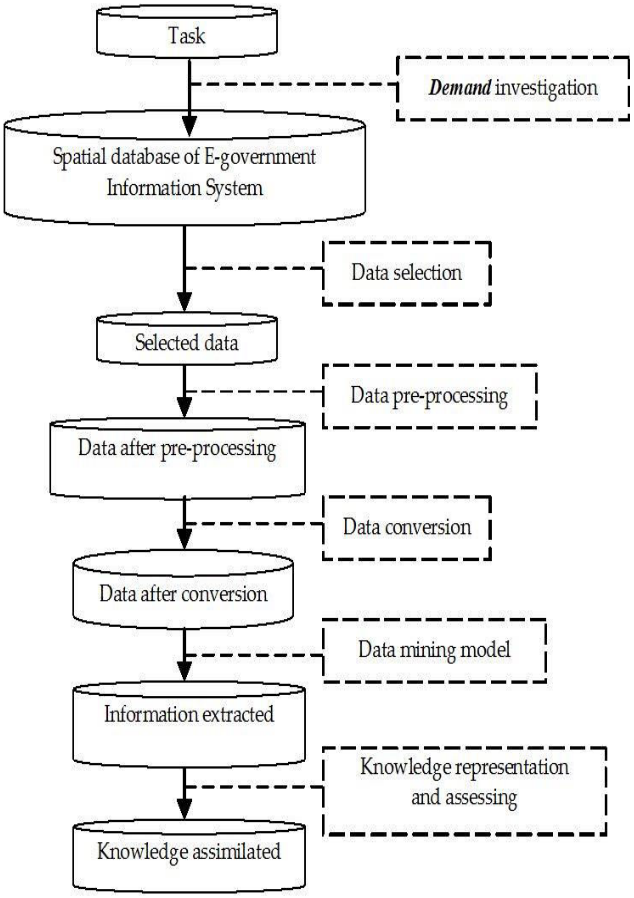
Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k*P

C2 = M + k*Q



C1 and C2 will be send.

Decryption

We have to get back the message ‘m’ that was send to us,

M = C2 – d * C1

M is the original message that we have send.

Proof

How do we get back the message?

M = C2 – d * C1

‘M’ can be represented as ‘C2 – d * C1’

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)= M (Original Message)

Data Visualization:

Data visualization provides a graphical representation of data, documents, and structures, which turns out to be useful for various purposes. Data visualization provides an overview of complex and large data sets, shows a summary of the data, and helps humans in the identification of possible patterns and structures in the data. Thus, the goal of data visualization is to simplify the representation of a given data set, minimizing the loss of information.Different data visualization techniques for varying dimensional data, Scatter plot, survey plot, line graph and bar charts are used for visualizing two dimensional data. The same techniques are used in visualization of three dimensional data, by addition of the third dimension perpendicular to the remaining two dimensions. Icon based, hierarchical methods,
geometrical methods and pixel oriented techniques are used for visualizing high dimensional data. By usage of these techniques, tracking of the student behavior is done and continues monitoring is provided thus implementing an enhanced security in online exam. The overall verification is shown in thefollowing flow chart.

CONCLUSION

In this paper, a set of authentication techniques are discussed. They include passwords, tokens, and biometrics. Special conditions are involved, to make the techniques to be strong enough to the intruder attacks. Varying authentication systems are discussed namely central authentication system, multi factor authentication system, split authentication system and message authentication system. This paper discuss a multi model authentication technique, that helps in continues monitoring of the student. The behavior of the student is visualized by using different visualization techniques.

REFERENCES

[1] Christopher Mallow," Authentication Methods and Techniques"

[2] Kim Bartke, 2005" 2D, 3D and High-Dimensional Data and Information Visualization", Seminar on Data and Information Management

[3] Winnie Wing-Yi Chan, 2006; "A survey on Multivariate Data Visualization", Department of Computer Science and Engineering. Hong Kong University of Science and Technology

[4] RyszardS.Choras, 2007,"Image Feature Extraction Techniques and their Applications for CBIR and Biometric System", International Journal of Biology and Biomedical Engineering

[5]AndrzejMaterka and Michal Strzelecki, 1998 "Texture Analysis Methods – A Review", Technical University of Lodz, Institute of Electronics ul. Stefanowskiego

[6] MihranTucerya, Anil K. Jain, 1998, "Texture Analysis", World Scientific Publishing Corporation.

[7] Aamer. S. S. Mohamed, Ying Weng, Jianmin Jiang and Stan Ipson, 2008 "An Efficient Face Image Retrieval through DCT Features" School of Informatics, University of Bradford
BD7 1DP, UK. { A.S.S.mohamed, Y.Weng, J.Jiang1, S.S.Ipson }@Bradford.ac.uk ,Signal and image processing

[8] Benavides, J.; Demianyk, B.; McLeod, R.D.; Friesen, M.R.; Laskowski, M.; Ferens, K.; Mukhi, S.N.; 2011" 3G Smartphone Technologies for Generating Personal Social Network Contact Distributions and Graphs " , 13th IEEE International Conference on e-Health Networking Applications and Services(Healthcom)

[9] ImY.Jung, Yeom, H.Y.; 2009 "Enhanced Security for Online Exams using Group Cryptography", IEEE transactions on Education

[10] Sonal Tiwari, DeeptiRazdan, PrashantRichariya, ShivkumarTomar, 2011, "A web usage mining framework for business intelligence", 3rd International Conference on Communication Software and Networks

[11] Shengqiong Yuan, Aurélien Tabard, Wendy Mackay; 2008,"StreamLiner: A General-Purpose Interactive Course-Visualization Tool", International Symposium on Knowledge Acquisition and Modelling Workshop

[12] C.M AlthaffIrfan, Syusaku Nomura, Karim Ouzzane, Yoshimi Fukumura.,2009 " Face-based Access Control and Invigilation Tool for e-Learning Systems", International Conference on Biometrics and Kansei Engineering

[13]Elisardo Gonzalez Agulla, Rifon, L.A. Castro, J.L.A. Mateo, C.G., 2008 "Is my student at the other side? Applying Biome tric Web Authentication to E-Learning Environments ", Eight IEEE International Conference on Advanced Learning Technologies, ICALT

[14] Wen-Bin Hsieh; Jenq-ShiouLeu; 2011;" Design of a time and location based One-Time Password authentication scheme ", 7thInternational Wireless Communications and Mobile Computing Conference, IWCMC

[15] TaiwoAyodele, Charles.A.Shoniregun, Galyna Akmayeva,2011,"Toward e-learning security: A machine learning approach", International Conference on Information Society(i-society)

[16] Nawfal.F.Fadhal, Gary B Wills, David Argles, 2011"Transparent authentication in E-Learning ", Conference on Information Society (i-society)

[17] Kikelomo Maria Apampa, Gary Wills, David Argles,2010,"An approach to presence

verification in summative e-assessment security", International Conference on Information Society(i-society)

[18] Nasser Modiri, Ahmad Farahi, SnazKatabi, 2011,"Providing security framework for holding electronic examination in virtual universities.", 7th International Conference on Networked Computing and Advanced Information Management(NCM)

[19] Levy, Y., Ramim.M.Michelle, 2009 "Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)", Interdisciplinary Journal of E-learning and Learning Objects (IJELLO);

[20] Asha, S. Chellappan, C., 2008 "Authentication of e-learners using multimodal biometric technology ", International Symposium on Biometrics and Security Technologies

[21] ImY.Jung, Yeom, H.Y.; 2009 "Enhanced Security for Online Exams using Group Cryptography", IEEE Transactions on Education

[22] GennaroCostagliola, Vittorio Fuccella, Massimiliano Giordano, Giuseppe Polese, 2009 "Monitoring Online tests through Data visualization",IEEE Transactions on Knowledge Data and Engineering

[23] http://www.facedetection.com/facedetection/dataset.h