JOURNAL OF PURE AND APPLIED MICROBIOLOGY, Aug. 2015. Vol. **9**, p. 25-29
SPECIAL ISSUE ON RECENT RESEARCH CHALLENGES IN BIO-MEDICAL APPLICATIONS

A Novel Face Authentication Using ECC

Srinivasan Nagaraj[1] and G.S.V.P. Raju[2]

[1]Department of CSE, GMRIT, GMR Nagar, Rajam - 532 127. Andhra Pradesh, India.
[2]Department Of CS & ST, Andhra University, Vishakapatnam - 530 003, India.

(Received: 14 March 2015; accepted: 03 May 2015)

Integrity, non repudiation, confidentiality, and authentication are important entities in information security . cryptography is the field of writing a secret code . Biometric identity authentication systems are based on the biological uniqueness of a person like face, voice, finger print, iris, gait, hand geometry or signature. Identity authentication using the face or the voice information is a challenging research area that is currently very active.In this paper progress on new method using combination of PCA and ECC to identify and authenticate a person based on face. ECC is very effient interms of its performance and operations with respective constrained devices. Using this we can simply identify a person based on his/her face . as this is the simple method to implement and required less computational time.This method of implementation is economy and also effieceint.

Key words: ECC, XOR, Encryption, Decryption.

A *Biometric is* called as a distinctive, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Five of the most used physical biometric patterns analyzed for security purpose are fingerprint, hand, eye, face and voice. Biometric authentication of a person is highly challenging and complex problem. A significant research effort has gone into this area and a number of research works were published, but still there is an immense shortage of accurate and robust methods and techniques.Biometric identity authentication systems are based on the biological uniqueness of a person

like face, voice, finger print, iris, gait, hand geometry or signature. Identity authentication using the face or the voice information is a challenging research area that is currently very active, mainly because of the natural and non-intrusive interaction with the authentication system. An identity authentication system has to deal with two kinds of events: either the person claiming a given identity is the one who he claims to be called client or if it is not then it is an impostor. Moreover, the system may generally take one decision either accept the client or reject him and decide he is an impostor. Low resolution camera is used to capture image for face recognition module, the preprocessing algorithm are employed like filtering to remove high frequency noise. The geometric normalization is used to remove the variation between size with orientation and its location of the face in the image. The feature extraction module uses principal component analysis (PCA) decomposition on the training set, which produces the Eigen vector and Eigen values. Cryptography is the division of information security that covers the learning of algorithms and protocols which secure data. It has been extensively used in intelligence and other areas like Wars as a tool for maintenance communications secret.

There are many different aspects of security that includes various threats and cryptography is not alone sufficient by itself. There are some specific security requirements which including:

* To whom all correspondence should be addressed.
E-mail: sri.mtech04@gmail.com

Authentication

It provides that the authenticity of one entity to allow or not to allow access of resources.

Confidentiality

It can be defined that the message cannot be modified by anyone except the intended receiver.

Integrity and Non-repudiation

That it provides integrity (originality) and non repudiation of resources.

Elliptic curve cryptography

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987)and Victor Miller (Miller 1986)independently proposed the public key cryptosystems using elliptic curve. Since , many researchers have spent for years together studying the strength of ECC and improving techniques for its implementation.

The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem.

In this paper for the purpose of the encryption and decryption using elliptic curves we consider the equation of the form

$$Y^2 = x^3+ax+b$$

Elliptic Curve Domain Parameters are D = (q, FR, a, b, G, n)

•***q***: prime power, that is q = p or q = 2^m, where p is a prime

•***FR***: It is the field representation of the method used for representing field elements Î F_q

•***a, b***: field elements, they specify the equation of the elliptic curve E over F_q,

$y^2 = x^3 + ax + b$

•***G***: A base point represented by G= (x_g, y_g) on E (F_q)

•***n***: Generated Prime number.

Background work

Face Detection

In General We can the Locate face in a given image and also second method is to Separate it from the scene.

Face Normalization

1. The image is rotated to an align the eyes.
2. Image is scaled to make the distance between the eyes are constant. The image is cropped to a lesser size.
3. The mask is apply that zeros out pixels not in an oval which contains the typical face and the oval structure is generated analytically.
4. Histogram equalization is used to smooth the distribution of gray values for the non-masked pixels.
5. The image is normalized so the non-masked pixels have mean zero and standard deviation one.

PCA Algorithms

The Principle Component Analysis.

The principal apparatus of the sharing of faces or the eigenvectors of the which covariance matrix of the set of face images.

Implementation methodology

In face recognition technique it have two phases.

a. Face Recognition.
b. Face identification.

Face Recognition

For recognition the face, capture the image using small resolution camera. Captured image is input to the matlab. as a result it produces the nXm matrix. Now read the every point from the matrix and apply the xor operation each point. It produces the resultant point which is taken as message for the authentication. Now read the diagonal points from the matrix. Now store the points in elliptical curve using ECC implementation.

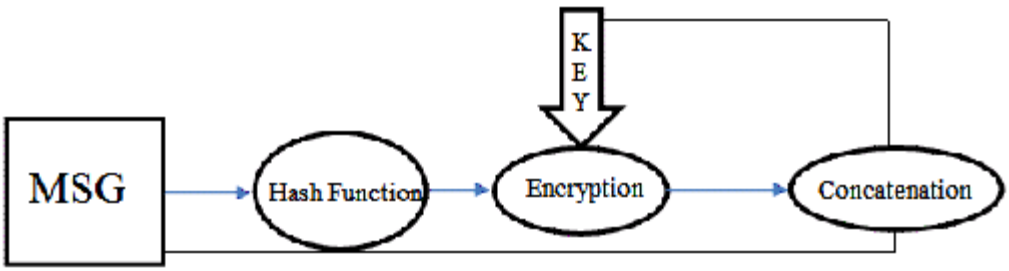

Fig.1. Block diagram of the system modle

In authentication process read the diagonal elements which are stored in elliptical curve by decryption method in ECC. Read the resultant which is used as key for encryption in authentication process. Now apply the hash function on message and encrypt it with key. Resultant is concatenated with the key and original message. Now this value is stored in database for identification.

ECC Implimentation

In ECC implementation we have 3 stages.

1. Defining standard curve and point generation.
2. Encryption.
3. Decryption.

Standard Curve And Point Generation

An elliptic curve E(Fp) over a finite field Fp is defined by the parameters a, b ÎFp (a, b satisfy the relation $4a3 + 27b^2$ ¹ 0), consists of the set of points (x, y) Î Fp, satisfying the equation

$$y2 = x3 + ax + b.$$

The set of points on E(Fp) also include point 'O' is the point at location infinity , which is the identity element under addition. The Addition operator is defined under E(Fp) , it can be seen that E(Fp) forms an abelian group under addition.

The addition operation in E (Fp) is specified as follows:

P + O = O + P = P.

If P = (x, y) ÎE (Fp), then (x, y) + (x, – y) = O. The point (x, – y) ÎE (Fp) and is called the negative of P and is denoted as –P)

If P = (x1, y1) ÎE (Fp) and Q = (x2, y2) ÎE (Fp) and P ¹ Q, then

R = P + Q = (x3, y3) ÎE (Fp),

Where

$X3 = l^2 – x1 – x2.$

y3 = l (x1 – x3) – y1 And l= (y2-y1) /(x2-x1)

i.e. the sum of two points can be visualized as the point of intersection of E(Fp) and the straight line passing through both the points.

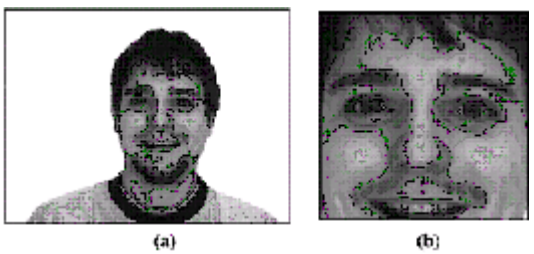

Fig.2. A face imge of AR database (b) face region

Let P = (x, y) Î E(Fp). Then the point Q = P + P = 2P = (x1, y1) Î E(Fp),

where $x1 = l^2 – 2x$, y1 = l (x – x1) – y, and l = (3x2 + a) / 2y. This operation is also called doubling of a point and can be visualized as the point of intersection of the elliptic curve and the tangent at P.

The reason for choosing prime fields is that distinct additive and multiplicative inverses exist for each number i.e. 0 to (P-1) in the field of the prime number P.

Point generation

There is constant need for a database of the elliptic curve points and a code to scan all Y co-ordinates that can satisfy the elliptic curve equation for the given X co-ordinate has been included.

Equation of the elliptic curve: y2 mod p=(x3+ax+b) mod p

Where, p is a prime number.

Algorithm: Inputs: p, a, b

a. Enter the input data.

b. x=[0: p-1]

c. For each value of x, check which values of y from 0 to (p-1) satisfies the equation.

d. Display the required point.

For example:

p=211, a=0, b=-4

X	Y
167	30
167	181
179	12
191	15

Point encryption

Step1: Read the values of diagonal points from the image input Matrix.

Now apply the encryption procedure as follows

Let E be an elliptic curve and P Î E be a point of order n. Given a point Q Î E with Q = mP, for a certain m Î {2, 3… m – 2}.

Find m in the above equation holds.

E.g. for Pa" (2, 2) and Qa" (153,108), such that Q=5P, then the discrete logarithm of Q to the base P is 5.

ECC Key exchange

Global Public Elements

Eq (a, b) elliptic curve with parameters a, b& q in the equation

Y2 mod q=(X3+aX+b) mod q

Q Base point on elliptic curve
User A Key Generation
Select private key kA, kA< n
Calculate public P P=kA × Q
User B Key Generation
Calculate public M M=kB × Q
Generation of Secret Key by user A
P1=K=kA × M
Generation of Secret Key by user B
P2=K=kB × P
The result of two calculations produce the same result because
kA × M = kA × (kB × Q) = kB × (kA × Q) = kB × P
To break this scheme the attacker must be able to compute k given G &kG, which is found tobe tough.

Elliptic curve encryption

1. Consider a message 'Pm' is sent from A to B. 'A' chooses a random positive integer 'k' , a private Key 'nA' and generates the public key PA = nA × G and produces the ciphertext 'Cm'
2. consisting of pair of points Cm={ kG , Pm + kPB }.where G is the base point choosen on the Elliptic Curve, PB= nB × G is the public key of B with private key 'nB' .

Elliptic curve decryption

To decrypt the ciphertext, B multiplies the 1st pointin the pair by B's secret & subtracts the resultfromthe 2nd point

Pm + kPB - nB (kG) = Pm + k (nB G) – nB (kG) =Pm

Face Identification

In identification process apply the same producer for reading image and compare it stored database. If the both the values are matched then authentication is successful.

Face recognition

Face recognition systems architecture performs the basic three tasks:

1. Acquisition(Detection,Tracking of face-like images)
2. Feature extraction (Segmentation,alignment & normalization of the face image)
3. Recognition

Step1:Capture the face and input it to the matlab.
Step2:Use PCA computing representation whichproduces capture Image as nXm matrix.
Step3: read the points from the matrix.
Step4: each point undergoes into XOR operation with another as a result finally it produces one point.
Step5: now read diagonal points from the matrix.
Step6: Store the points in elliptical curve using ECC implementation.

After calculating the results these values are undergoes into face identification module which identifies the face with existing image.

Face detection

Step1.Read the point(x) which is result of xor of every point.
Step2: Read diagonal points from elliptical curve which Are stored in elliptical curve by decryption method.
Step3: Read the point(y) which is resultant of **XOR** of diagonal Points.
Step3:Hash function is applied on x.
Step4: Now encryption method is applied on result using y as key.
Step5: Concatenate the result, x, y.
Step6: Result is stored in database.

Face Identification

Compare the result with existing database value .if both matches then provide the authentication.

Parameter Based Facial Recognition

unambiguous to match an individual's Facial image is analyzed and reduced to small set of parameters describing prominent facial features. Major features analyzed are: eyes, nose, mouth and cheekbone curvature These features are then matched to a database.

CONCLUSION

Biometric identity authentication systems are based on the biological uniqueness of a person like face, voice, finger print, iris, gait, hand geometry or signature.Using this we can simply identify a person as this is the simple method to implement and required less computational time than others. Identity authentication using the face or the voice information is a challenging research area that is currently very active.In this work we implemented security for face (authentication) using ECC algorithm.In this , the regions are then compared on a pixel-by-pixel basis with an image in the database Advantage is that the image preprocessing is simpler. ECC is very effient interms of its performance and operations with respective constrained devices. Using this we can simply identify a person based on his/her face . This is the simple method to implement and required less

computational time.This method of implementation is economy.

ACKNOWLEDGEMENT

I extend my sincere thanks to Dr .G.S.V.P .Raju for their suggestions and guidance in completing the Work. The work deliverables be timely scheduled so as to encourage a stable development and thus leading to the appropriate completion of the Work. The lectures of the course Cryptography and image processing used for good understanding of the various concepts involved in face recognition.

REFERENCES

1. M. Turk and A. Pentland. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, 1991; **3**(1).
2. C. Nastar and M. Mitschke. Real-Time Face Recognition Using Feature Combination. In *Proceedings of the Third IEEE International Conference on Automatic Face and Gesture Recognition*, Nara, Japan, April 1998
3. J. Gilbert and W. Yang. A Real-Time Face Recognition System using Custom VLSI Hardware. Harvard Undergraduate Honors Thesis in Computer Science, 1993.
4. J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 1993; **15**(11): pp. 1148 – 1161.
5. Fazl-Ersi, E.; Tsotsos, J.K.; , "Local feature analysis for robust face recognition," IEEE Symposium on Computational Intelligence for Security and Defense Applications , page.1-6 July 2009.
6. Delac K., Grgic M., Grgic S., "Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set, *International Journal of Imaging Systems and Technology*, 2006; **15**(5): pp. 252-260.
7. D. Bryliuk and V. Starovoitov, "Access Control by Face Recognition using Neural Networks and Negative Examples, 2nd International Conference on Artificial Intelligence, pp. 428-436, Sept 2002.
8. Wright, J. and Yi Ma and Mairal, J. and Sapiro, G. and Huang, T.S. and Shuicheng Yan "Sparse Representation for Computer Vision and Pattern Recognition" *Proceedings of the IEEE,* 2010 **; 98:** pp 1031 -1044 .
9. R. P. Wildes, "Iris Recognition: An Emerging Biometric Technology," *Proc. of the IEEE*, 1997; **85**(9): pp. 1348-1363.
10. Y. Zhu, T. Tan, and Y. Wang, "Biometric Personal Identification Based on Iris Patterns," *Acta automatica sinica*, 2002; **1**.
11. J. Daugman, United States Patent No. 5,291,560 (issued on March 1994). Biometric Personal Identification System Based on Iris Analysis, *Washington DC: U.S. Government Printing Office*, 1994.