Network Security Using ECC with Biometric

Dindayal Mahto and Dilip Kumar Yadav

Department of Computer Applications
National Institute of Technology, Jamshedpur
Jharkhand, PIN- 831014, India
{dindayal.mahto,dkyadav1}@gmail.com

Abstract. The popular asymmetric cryptography is RSA but most of the RSA–based hardware and software products and standards require big cryptographic keys length for higher security level. The existing asymmetric cryptography algorithms need the storage of the secret keys. Stored keys are often protected by poorly selected user passwords that can either be guessed or obtained through brute force attacks. This is a major weakness of the crypto-system. Combining biometrics with cryptography is seen as a possible solution. This paper discusses the network security using Elliptic Curve Cryptography with contactless palm vein biometric system. It provides more security with less key length and also there is no need to store any private key anywhere. It focuses to create and share secret key without transmitting any private key so that no one could access the secret key except themselves.

Keywords: Elliptical Curve Cryptography (ECC), Biometric, Palm Vein, MD5, Rivest Shamir Adleman (RSA).

1 Introduction

We are living in cyber age, where most of the information is produced with the help of computers and computer networks, which provides platform to do e-commerce tasks, online banking, and sharing of information and many more, and while more than two parties communicate to each other then they worry about confidentiality, data integrity, non-repudiation and privacy etc. [1]. In order to mitigate these issues, we can apply cryptography with biometrics. Cryptography is a kind of secret writing by which two parties can communicate with secret messages [2]. Most of the researches have demonstrated that biometric is the ultimate solution for identification and authentication, since it is proved as reliable and universally acceptable identification/authentication methods in many application areas [3].

Due to the popularity of biometrics and cryptography, the information security is becoming as a common demand in all applications area. Biometric is referred as automatic system that uses measurable, physical or physiological characteristics or behavioral traits to recognize the identity of an individual. Biometrics offers greater security in identification/ authentication system. However, the security level of the network can be further enhanced using cryptography and biometrics.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 842–853, 2013.

To secure the communication currently there are two popular kinds of cryptographic protocol namely symmetric key and public key protocol. In symmetric key protocol such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) [2], a common key is used by both sender and receiver for encryption and decryption. This system provides high speed but have the drawback that a common key must be established for each pair of participants. In public key protocol there are two keys, public key and private key by which message can be encrypted and decrypted. One is kept private by owner and used for decryption. The other key is published to be used for encryption. Some of the most useful example of the public key cryptography is RSA, ElGamal and Digital Signature Algorithm (DSA) [4]. Although, these algorithms of asymmetric crypto-systems are slower than that of the symmetric crypto-systems but they provide high level security. Due to comparative slowness of the public key cryptography algorithms, dedicated hardware support is desirable. RSA is used in most of the network and standards that uses public key cryptography for encryption, decryption and digital signature. The length of the keys for RSA has been increased in recent years, and this is putting a heavier load on the application of RSA. It creates extra computation cost and processing overhead. However, ECC compared to RSA, offers higher security per bit with smaller key size. It provides higher security per bit. Since ECC has smaller key size, hence it also reduced the computation power, memory and bandwidth.

Therefore, in this paper a model has been proposed for network security using ECC with biometric. In this model, keys are generated from palm vein biometric which are used for encryption and decryption in the ECC for identification and authentication.

This paper is organized as follows. In section 2, we provide the review of the elliptic curve cryptography, why we use elliptic curve cryptography instead of RSA or other cryptography system, the implementation method of ECC and its mathematical operation and method for finding all points on the elliptic curve on which we have to encrypt the message. We describe the Elliptic Curve Diffie-Hellman Algorithm (ECDH) in this section for generating key. In section 3 we describe about the biometric and importance of palm over the biometric, why we use palm instead of iris, finger, face, retina or other biometric. In section 5 we describe how can we encrypt and decrypt the message by the help of palm as a private key. In section 6 we describe the result and discussion. We conclude the paper in section 7.

2 Elliptic Curve Cryptosystem

In 1985, Neil Koblitz [4] and Victor S. Miller [5] independently proposed the use of elliptic curve cryptography. Since 1985, there have been a lot of studies concerning elliptic curve cryptography. The use of ECC is very inviting for various reasons [1, 3, 6, 7]. The first and probably most important reason is that ECC offers better security with a shorter key length than any other public-key cryptography. For example, the level of security achieved with ECC using a 160-bit key is equivalent to conventional public key cryptography (e.g. RSA) using a 1024-bit key [4]. There are huge importances of shorter key lengths especially in applications having limited memory resources because shorter key length requires less memory for key storage purpose. Elliptic curve cryptosystems also require less hardware resources than conventional public-key cryptography. Now at the security level ECC is more secure than RSA. RSA can be cracked successfully, uses 512 bits and for ECC the number of bits is 97, respectively. It has been analyzed that the computation power required for cracking ECC is approximately twice the power required for cracking RSA. ECC provides higher level of security due to its complex mathematical operation. Mathematics used for ECC is considerably more difficult and deeper than mathematics used for conventional cryptography. In fact this is the main reason, why elliptic curves are so good for cryptographic purposes, but it also means that in order to implement ECC more understanding of mathematics is required. A short introduction to mathematics behind elliptic curve cryptosystems is given in this paper; however, this paper should give a good overall picture of ECC and its implementation issues.

2.1 Mathematics Behind ECC

Cryptographer noticed that elliptic curves behaved conveniently when operations were performed with prime modulus. That means cryptographer elliptic curve is in the form $y^2 \bmod p = (x^3 + ax + b) \bmod p$ where $4a^3 + 27b^2 \neq 0$ and p is a prime number and a, b is the parameter of the curve, here variables and coefficient are all restricted to elements of a finite field. There are two families of elliptic curve are used in cryptography application [8, 9, 10].

1. Elliptic Curves over $GF(2^m)$
2. Elliptic Curves over Z_p.

In Elliptic curves defined over $GF(2^m)$, the variables and co-efficient all take on values in $GF(2^m)$ and in calculation performed over $GF(2^m)$.

In Elliptic Curves over Z_p, we use a cubic equation in which the variables and co-efficient all take on values in the set of integers from 0 through (p-1) and in which calculations are performed modulo p.

This paper is based on the Elliptic curves over Z_p.

For example, let us take our elliptic curve is

$$y^2 \bmod 11 = (x^3 + ax + 2) \bmod 11 \tag{1}$$

2.2 Arithmetic Operation in ECC

The rule of mathematical operation on elliptic curve is different from the rule conventional mathematical operations. If we want to add two points of elliptic curve then we have to follow given below rule. For this and all arithmetic operation there are some rules which are as follows [8, 9,10].

The rules for addition over $E_p(a, b)$. For all points P, Q Є $E_p(a, b)$:

Rule 1: P + O (Infinity) = P

Rule 2: If P = (x_1, y_1), then P + $(x_1, -y_1)$ = O.

Rule 3: *If* $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$ *with* $P \neq -Q$, then R = P + Q = (x_3, y_3) is determined by the following rules:

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p \tag{2}$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p \tag{3}$$

where,

$\lambda = ((y_2 - y_1) / (x_2 - x_1)) \bmod p$, if $P \neq Q$

and,

$\lambda = ((3x_1^2 + a) / 2y_1) \bmod p$, if $P = Q$

Rule of Multiplication: It is defined as repeated addition.

Suppose P is a point on elliptic curve P = (x_1, y_1)

Thus 8*P =P+P+P+P+P+P+P+P

=2P+2P+2P+2P

=4P+4P

2.3 Points on ECC

For any operation on elliptic curve, first of all we have to find the all point of that curve [10]. Thus for finding the point on the curve firstly we have to chose any elliptic curve. Suppose $y^2 \bmod p = (x^3 + ax + b) \bmod p$ is an elliptic curve where $4a^3 + 27b^2 \neq 0$. Then points on this curve are the set $E_p(a, b)$ consisting of all pairs of integers (x, y), which satisfy the above equation together with the point Zero. Method for finding the points on the curve is as follows:

Points on ECC

Step1. Determine the L.H.S of elliptic curve for all (x, y) € Z_p.

Step2. Determine the R.H.S of elliptic curve for all x, y € Z_p.

Step3. Choose the Pair of corresponding value of x and y as a pair for all x, y € Z_p for which L.H.S. = R.H.S.

Step4. All pairs of such (x, y) are the point on the curve.

Example

If in above curve, value of p=11, a=1, b=1, then points on the elliptic curve are (0,1),(2,0),(3,3),(3,8),(4,5) etc.

2.4 ECDH (Elliptic Curve Diffie-Hellman Algorithm)

Elliptic curve Diffie-Hellman algorithm is the Diffie-Hellman algorithm for the elliptic curve [3, 8]. The original Diffie-Hellman algorithm is based on the multiplicative group modulo *p*, while the elliptic curve Diffie-Hellman (ECDH) protocol is based on the additive elliptic curve group. We assume that the underlying field *GF* (*p*) is selected and the curve *E* with parameters *a*, *b*, and the base point *P* is set up. The order of the base point *P* is equal to *n*. The standards often suggest that we select an elliptic curve with prime order, and therefore, any element of the group would be selected and their order will be the prime number *n*. At the end of the protocol the communicating parties end up with the same value *K* which is a point on the curve. A part of this value can be used as a secret key to a secret-key encryption algorithm.

Suppose there are two users Alice and Bob. According to the Diffie-Hellman the key generation and exchange is as follows.

```
Key generation and key exchange

Step 1: Alice uses his palm vein feature for his private key $d_A$ which less than n.
Step 2: Alice generates a public key $P_A = d_A * G$; the public key is a point in $E_p(a, b)$.
Step 3: Bob similarly uses his palm vein features for his private key $d_B$ which is
        less than n.
Step 4: Bob computes a public key $P_B = d_B * G$.
Step 5: Alice generates the secret key
        $k = d_A *$        $P_B$.
Step 6: Bob generates the secret key
        $k = d_{\mathbf{B}} *$        $P_A$.
```

By exchanging the key through this method both Bob and Alice can communicate safely. Bob can use the secret value he computed to build an encrypting key. When Alice gets the message from Bob, she uses the secret value she computed to build the decrypting key. It is the same secret value, so they use the same key. Thus what Bob encrypts Alice can decrypt.

3 Why PALM?

Palm vein authentication uses the vascular patterns of an individual's palm as personal identification data. Compared with a finger [18] or the back of a hand, a palm has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification. The palm is an ideal part of the body for this technology; it normally does not have hair which can be an obstacle for photographing the blood vessel pattern, and it is less susceptible to a change in skin color, unlike a finger or the back of a hand. The deoxidized hemoglobin in the vein vessels absorb light having a wavelength of about 7.6 x 10.4 mm within the near-infrared area [19]. When the infrared ray image is captured, unlike the image seen in Fig.1, only the blood vessel pattern containing the deoxidized hemoglobin is visible as a series of dark lines (Figure 5). Based on this feature, the vein authentication device translates the black lines of the infrared ray image as the blood vessel pattern of the palm (Figure 6). The palm vein sensor (Figure 7) captures an infrared ray image of the user's palm. The lighting of the infrared ray is controlled depending on the illumination around the sensor, and the sensor is able to capture the palm image regardless of the position and movement of the palm.[20]

Palm vein offers contactless authentication and provides a hygienic and noninvasive solution, thus promoting a high-level of user acceptance. Fujitsu believes that a vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body.[20]

4 Previous Works

The main problem of asymmetric cryptography is the management of private key. No one should be able to access someone else's private key. They need to store in such a place which is protected from unauthorized accessing. This is vulnerable for attacking by hackers. This creates big problem in asymmetric cryptography. Thus it can be solved by the use of biometric template. Private Key can be generated directly by the biometric template. Since private key can be generated dynamically from one's biometric template, so there is no need to store private key anymore and network becomes more secure and safe. But there are very little work has been done in the field of ECC with the help of biometric. Some of the suggested approaches are given. [1], [22], [23]. However these biometrics have lots of issues regarding training, capturing image, easily obscured by eyelashes, eyelids, lens and reflections from the cornea, lack of existing data deters ability, cost, voice can be captured while uttering the password, a camera can photograph an iris from across the room, and fingerprints left on surfaces can be lifted hours later [23] etc. For some individuals, the iris image capturing is very difficult. Iris recognition system requires lots of memory to be stored. It is easily absurd by eyelash, eyelids, lens and reflection from the cornea. People are not much familiar with iris recognition system yet, so there are lots of myths and fears related to scanning the eye with light source. Iris recognition system works on the basis of acquisition of iris image, but acquisition of an iris image needs more training and attractiveness than most other biometrics. It cannot be verified by human too. The most problem with iris recognition system is its expensiveness. Lifang et al.[22] have generated cryptographic key from user's face features and then the key has been applied in DES algorithm for encryption and decryption purposes and same way Fabian et al.[23] have generated cryptographic key from user's voice while speaking a password, but no further implementation of key has been described on their paper.

As palm vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body. We are generating cryptography keys from user's palm vein and then the generated key are used as user's secret keys for ECC.

Hence in proposed method we are using palm vein as a secret key instead of other biometric.

5 Proposed Work

In this paper we are using palm vein features of senders' and receivers' for generating secret keys, then the keys are used in Elliptic Curve Cryptography to provide network security while sending the information from sender to receiver and vice versa.

5.1 Method for Generating Public Key and Private Key

First of all users' palm features are scanned through Palm Vein scanner and then same are filtered for registrations purpose known as enrollment and later palm features are used for authentication.

Fig. 1. ATM with palm vein pattern authentication sensor unit

Fig. 2. Palm vein access control unit

Fig. 3. ATM for convenience stores with downsized palm vein pattern sensor unit

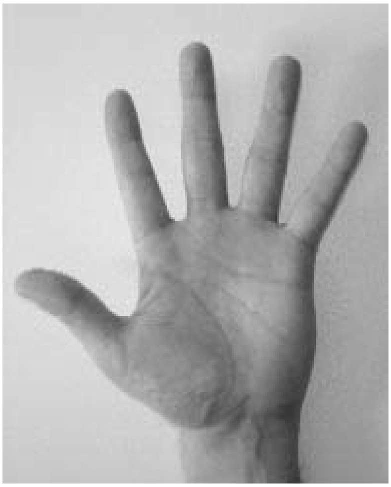


Fig. 4. Visible ray image

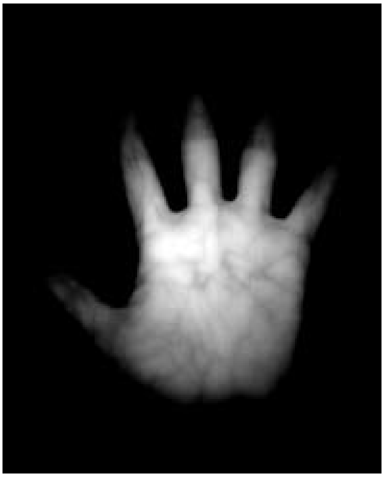


Fig. 5. Infrared ray image

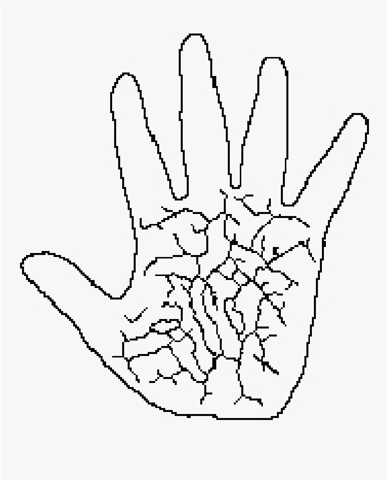


Fig. 6. Extracted vein pattern

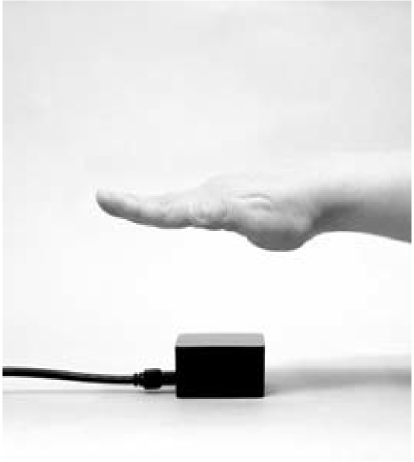
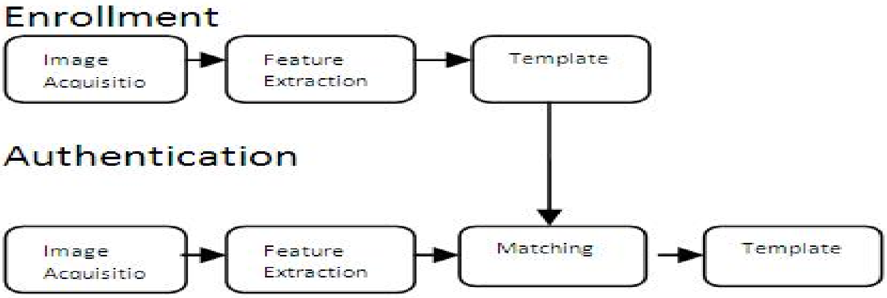


Fig. 7. palm vein sensor

Palm vein authentication process consists of two essential procedures: enrolment and authentication. Taking the following steps completes each procedure:



To generate private key, we take the palm vein of the user and generate its hash value by the help of MD5 cryptographic hash function [9]. This resultant hash value is the private key of the user. Suppose this value is d_A for use Alice and d_B for user Bob.

Now to generate public key in elliptic curve cryptosystem by the help with this private key is as follows:-

Step1: Both user choose the same large prime ‘p’ and the elliptic curve parameter ‘a’ and ‘b’ such that

$$y^2 \bmod p = (x^3 + ax + b) \bmod p;$$
$$\text{where, } 4a^3 + 27b_2 \neq 0$$

Step 2: Now choose any one point G(x, y) from this elliptic curve. This point is called the base point of the curve.

Step3: Compute $P_A = d_A * G(x, y)$

This P_A is called the public key of user Alice.

To generate public key of user Bob same operation can be performed by the help with private key of user Bob.

5.2 Message Encryption

Suppose user Alice wants to send a message to user Bob, then first task in this system is to encode the plaintext message m to be sent as a point P_m (x, y). It is the point P_m that will be encrypted as a cipher text and subsequently decrypted. After mapping of points [17] with user message characters on elliptic curve, they can encrypt the message by following steps

Step 1: Suppose Alice encodes the message m as $P_m = (x, y)$

Step 2: Alice takes his private key from his palm vein feature suppose it is k and produces C_m consisting of the pair of points:

.

$$C_m = \{k * G, P_m + k * P_B\}$$

Here C_m is a cipher text, Alice sends this cipher text to Bob.

5.3 Message Decryption

For Message decryption Bob has to do following procedures.

Step 1: Bob multiplies the first point in the pair by his secret key and subtracts the result from the second point:

$$P_m + k * P_B - d_B * k * G$$
$$= P_m + k(d_B G) - d_B(k * G)$$
$$=Pm$$

Step 2: The message P_m is the required message of Bob, which is sent by Alice.

6 Result and Discussion

Traditional methods for implementing public key infrastructure, encryption and decryption techniques face lots of problem such as key management, key storing, key privacy etc. Our proposed approach can handle such problems. Here we are using palm vein features as a private key so that there is no need to store any private key and also palm vein has lots of merits over other biometrics (i.e., it is most user friendly and cheaper too). Palm vein recognition also has some outstanding features like universality, permanence, uniqueness and accuracy. As we are using ECC, so we can achieve high level security with very shorter key size. Thus it also solves the key size problem. ECC requires very complex mathematical operation (because of elliptic curve Diffie-Hellman problem, which is harder than discrete logarithmic problem) therefore security strength per bit is also very high.

We have implemented ECC portion of this proposed work in MATLAB R2008a under Microsoft Windows platform. It asks all related parameters and then generates cipher-text in one graph and decrypted-text in another graph.

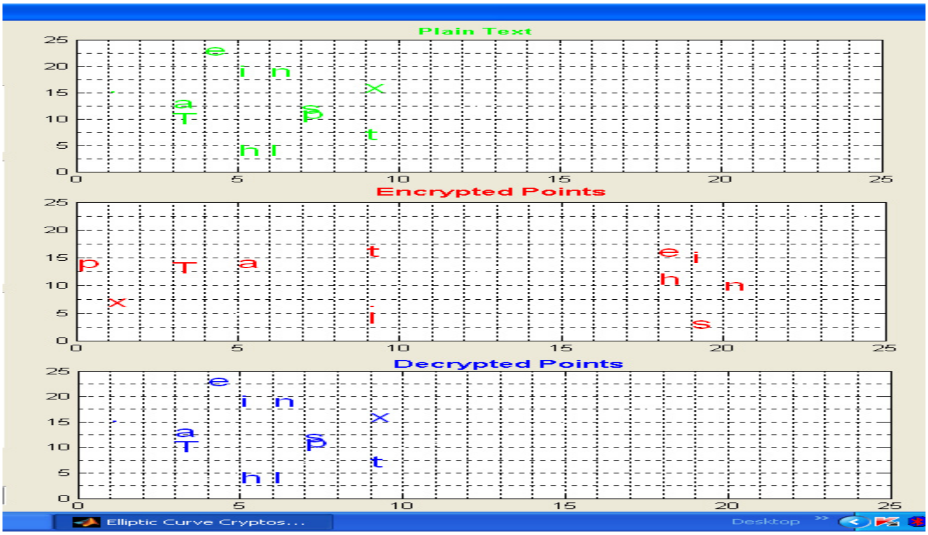


Fig. 8. Elliptic Curve Cryptography Software Implemented in MATLAB (r2008a)

7 Conclusions

In this paper, network communication becomes very secure with the help of ECC and palm vein biometric. The main advantage of ECC is that it requires very less key size and gives high level of security with cheapest biometric recognition system and there is no need to store any private key anywhere. Palm vein authentication technology offers contactless authentication and provides a hygienic and non-invasive solution, thus promoting a high-level of user acceptance. A vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body. Thus the proposed model provides a very secure network communication system.

References

1. Mohammadi, S., Abedi, S.: ECC based Biometric Signature: A new approach in electronic banking security. In: International Symposium on Electronic Commerce and Security (ISECS 2007), pp. 763–766 (2008), doi:10.1109/ISECS.2008.98
2. Stallings, W.: Cryptography and Network Security Principles and Practices, Edition Fourth. Pearson Prentice Hall (2007)
3. Nandini, C., Shylaja, B.: Efficient Cryptographic key Generation from Fingerprint using Symmetric Hash Functions. International Journal of Research and Reviews in Computer Science (IJRRCS) 2(4) (August 2011)
4. Mel, H.X., Baker, D.: Cryptography Decrypted. Addision-Wesley (2011)
5. Koblitz, N.: Elliptic Curve Cryptosystem. Mathematics of Computation (48), 203–209 (1987)
6. Miller, V.S.: Uses of Elliptic Curve in Cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
7. Prasanna Ganesan, S.: An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptogphy. In: ICACC, pp. 107–109.
8. Zhou, X.: Elliptic Curves Cryptosystem Based Electronic Cash Scheme with Parameter Optimization. In: Pacific-Asian Conference on Knowledge Engineering and Software Engineering (KESE 2009), pp. 182–185 (2009), doi:10.1109/KESE.2009.55.
9. Kumar, M.: Cryptography and Network Security, Krishna Prakashan Media (P) Ltd. 2nd edn. (2007)
10. Anoop, M.S.: Elliptic Curve Cryptography, An implementation tutorial, Tata Elexsi Ltd., Thiruvananthapuram, India
11. Doshe, C., Lange, T.: Arithmetic of Elliptic Curves. In: Cohen, H., Frey, G. (eds.) Handbook of Elliptic and Hyper Elliptic Curve Cryptography, ch. 13. Chapman and Hall/CRC, Taylor and Francis Group (2006)
12. Ahmad Jhat, Z., Hussain Mir, A., Rubab, S.: Palm Texture Feature for Discrimination and Personal Verification. In: Third international Conf. on Emerging Security, System and Technologies (SECURWARE 2009), pp. 230–235 (2009), doi:10.1109/SECURWARE.2009.42
13. Udb –Din, H., Al-Jaber, A.: Securing online shoping using biometric personal authentication and stagenography. In: ICTTA 2006, pp. 233–238 (2006)
14. Woodward, J.D., Orlans Jr., N.M., Higgins, P.T.: Biometrics The ultimate reference. Dreamtech Press (2003)
15. NSTC on Biometrics, `http://www.questBiometrics.com`
16. Biometric-Comparison, `http://biometric.pbworks.com/w/page14811349/advantagedisadvantage`
17. Nanawati, S., Thieme, M., Nanavati, R.: Biometrcs Identity Verification in a networked world, 1st edn. Willey Computer Publishing (2002)
18. Rao, O.S.: Efficient mapping method for elliptic curve cryptosystems. International Journal of Engineering Science and Technology 2(8), 3651–3656 (2010)

19. Miura, N., Nagasaka, A., Miyatake, T.: Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles. In: Proceedings of the 9th IAPR Conf. on Machine Vision Applications (MVA 2005), Tsukuba Science City, Japan, pp. 347–350 (2005)
20. Bio-informatics Visualization Technology committee, Bio-informatics Visualization Technology, p. 83. Corona Publishing (1997)
21. Watanabe, M., Endoh, T., Shiohara, M., Sasaki, S.: Palm vein authentication technology and its applications. Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4- chome, Nakahara-ku, Kawasaki, 211-8588, Japan
22. Zhanga, P., Hub, J., Lic, C., Bennamound, M., Bhagavatula, V.: A pitfall in fingerprint bio-cryptographic key generation. Computers & Security 2(4) (August 2011)
23. Wu, L., Liu, X., Yuan, S., Xiao, P.: A Novel Key Generation Cryptosystem Based on Face Features. In: Precedings of the ICSP 2010. IEEE (2010)
24. Monrose, F., Reiter, M.K., Li, Q., Wetzel, S.: Cryptographic Key Generation from Voice. In: Proceedings of the 2001 IEEE Symposium on Security and Privacy (May 2001)