Bulletin of Electrical Engineering and Informatics
Vol. 4, No. 1, March 2015, pp. 67~72
ISSN: 2089-3191

A Bio-Crypto Protocol for Password Protection Using ECC

Srinivasan Nagaraj*[1], GVSP Raju[2], G Apparao[3], B Kishore[4]
[1]Dept. of CSE, GMR Inst. Of Technology GMR Nagar, Rajam, AP
[2]Dept. Of CS&ST, Andhra University, Vishakapatnam-530003
[3]Dept. of CSE, GITAM Univ. Vizag – 530045, AP
[4]Dept. Of CSE, Manipal Univ
*Corresponding author, email: sri.mtech04@gmail.com[1], gsvpraju2011@yahoo.com[2], gapparao@gmail.com[3], kishore.gmr@gmail.com[4]

Abstract

In information security the following security parameters like, integrity, non repudiation and confidentiality, authentication must be satisfied. To avoid thievery of organization resources it needs be secured in more efficient way and there is always demand for different levels of security attacks include virus, brute force and Eveadroper in business that organizations make use of voice biometrics an attractive low-cost. Voice biometrics is the cheapest among the other biometrics and used all levels for management to buy readily available metric and it is the way of identifying individuals remotely with high level of accuracy. In this work, we have been designed a new password- authentication approach that provides security using voice biometrics for authentication and uses the device itself into an authenticator which uses voice itself as its passwords and we are primarily interested in keys that can be temporally reproduced on the same device from the same user's voice. Public and private keys are generated randomly from the user's voice and stored in the voice file (.wav). This Method uses voice recognition, include the operation of register (recording feature) or voice prints and storing of one or more voice passwords into the database. It uses ECDSA to perform the authentication process that matching the voice sample with the database. The recognition, entity makes the database to decide that the sample is matched to perform an operation or not. Our proposed approach generates cryptographic keys from voice input itself and this algorithm developed an adhoc basis. It can effectively defend attacks specially brute force attack in system networks.

Keywords*: ECC, Prime, Public key–Y, ECDSA*

1. Introduction

Biometric is an either physiological or behavioral feature of individual that can distinguish from one personality and that can be secured used for identification or verification of identity. They classified into two types [1-5]:

1. Psychological: The different psychological attributes are iris, fingerprints, hand, retinal and face recognition
2. Behavioral: The different behavioral attributes are voice, typing pattern, signature.
   - Following are the metrics of Biometrics: FTE – Failure To Enroll, FTA – Failure To Accept, FAR – False Acceptance Rates, and FRR – False Reject Rates
   - The Various Biometrics Usability issues are: user acceptability and Knowledge of technology and familiarity with biometric characteristic experience with device.

Voice Biometric Disadvantages include:

- Local acoustics and Background noise
- Device quality and Illness, emotional behavior
- Time consuming enrollment and Large

These physical parameters are the basic constant body points that produce the sound waves of the human voice, are calculated as vectors and measured as a voice print.

Mathematically, sound is represented as a sequence of values, forming a temporal series. There are several techniques to extract features of time series and analyze the original sound waveform, without needing to individually analyze each point of the time series [6-7]. The result of a biometric measurement of the voice is totally dependant on [8-11]:

Received October 6, 2014; Revised December 12, 2014; Accepted January 3, 2015

1). Input
It refers to the biometric sample, such as a voice print, taken and stored in a database. Input quality, the most important factor, is greatly affected by the type of input device (professional microphone, Cell phone, for example) and environment (noisy street vs. quiet office).
2). Accurate mathematical algorithms,
Accurate mathematical algorithms: Algorithms are a set of precise steps that describe a limited procedure or task. Algorithms in biometric systems are used to find out whether a sample matches the stored input. The more precise the algorithm, the more accurate the matching process
3). Computing power.

1.1 Elliptic Curve Cryptography

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. Mohsen [11] and Neal Koblitz [12] independently proposed the public key cryptosystems using elliptic curve. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation. The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem.

In the present paper for the purpose of the encryption and decryption using elliptic curves it is sufficient to consider the equation of the form

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

To increase the security and make use of the biometric features of generating private keys and producing Elliptic Curve domain parameters, this proposed system combined the elliptic curve and biometric features to harden the seed that will be used to generate the curve against the cryptanalysis.

The intended system uses “voice‟ as an input data to help generating the intended Elliptic Curve parameters. The generated parameters will be used in the cryptographic process such as Elliptic Curve Cryptography.

1.2 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***: field representation of the method used for representing field elements (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.

Take the secret key as the x value and calculate the y value using the ECC equation.
Y^2 = x^3 + ax + b, from this, we get point x, y on the curve.

2. Proposed Method of Implementation

2.1 Generating Cryptographic Keys:

- **Voice Recognition**
  Voice recognition process the word spoken is taken as input to program. Speech recognition is the process by which a computer (or other type of machine) identifies spoken words. Basically, it means talking to your computer, and having it correctly recognized what you are saying. Voice or speech recognition [7] is the ability of a machine or program to receive and interpret dictation, or to understand and carry out spoken commands.
- **Voice Verification**
  In the proposed system only voice will be interaction tool to a user with the system for registration and verification, as Figure 1.

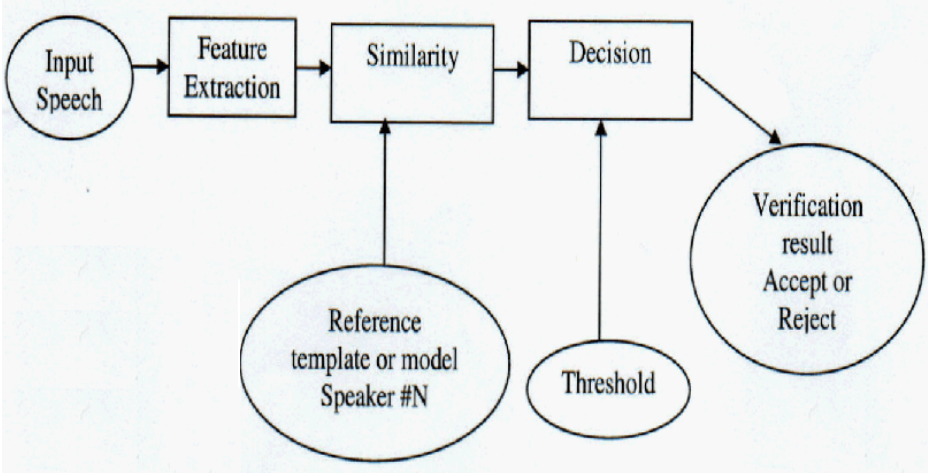

Figure 1. voice verification

For the voice recognition part the following steps have to be followed:

i) At first, we have to provide the user details (features) as input in the form of voice asked by system.
ii) The system will then generate a ".wav" file and the generated file will be saved in the database for future references and generate the Peak values for each samples.
iii) At the time of log in by the user, it performs comparison of user needs to provide the same information given at the time of registration and the system compares the recorded voice with the one saved in database.

If both match, user logs in successfully or accept sample otherwise not or reject the sample.

In the proposed system, we advocate research into the generation of cryptographic keys from voice input, as Figure 2. We are primarily interested in keys that can be temporally reproduced on the same device from the same user's voice, and that is un guessable to an attacker who captures that device. This appears to be a harder problem than building a speech based reference monitor, since a solution to our problem can be used to build a reference monitor directly: the reference monitor would take the cryptographic key derived from the voice signal as input, and compare it to what the key was supposed to be (just as a password-based login program does).The goal of un guess ability precludes perhaps the most natural approach to deriving a repeatable key from a spoken utterance: i.e., apply automatic voice recognition to recognize the password spoken, and then simply use the password as a cryptographic key.
The threshold value is calculated as the mean of all the peaks belonging to the voice file

$$\mu_k = \frac{1}{N_k} \sum_{q=1}^{N_k} x_q$$

Where μ_k is the threshold value, N_k is the number of peaks.

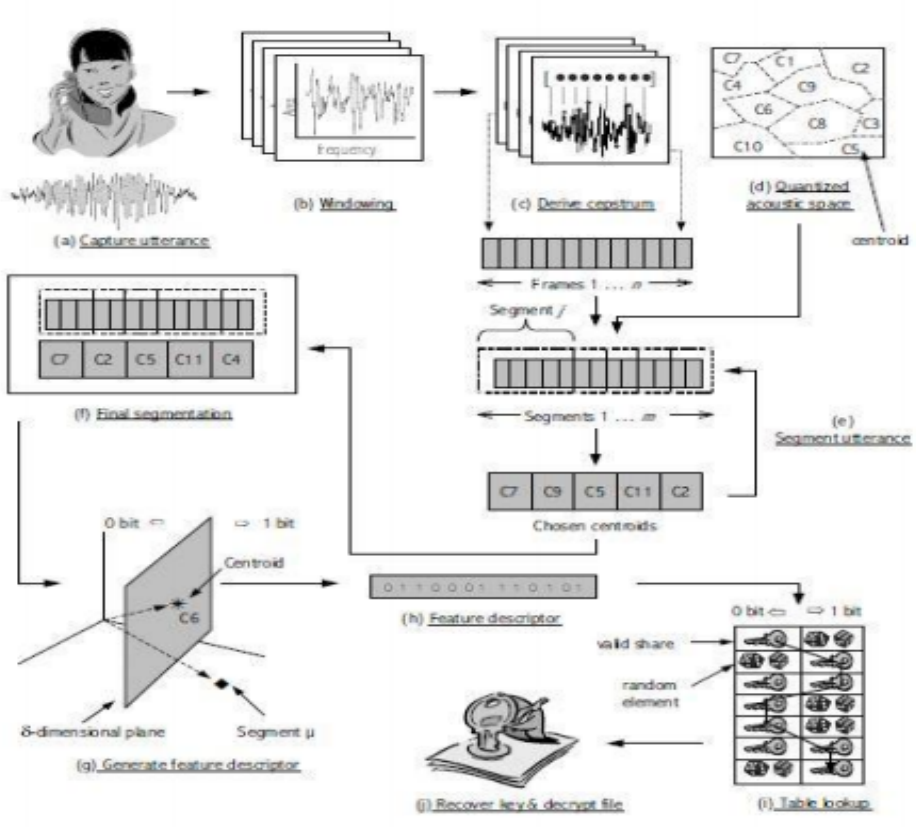

Figure 2. Key generation from voice features

In attributing **corresponding** we used two methods. In the first method centroids from the row and column is found. For recognition the minimum Euclidian distance between the input utterance of an unknown microphone and the stored database should less than the threshold value.

The curves are generated using an ECC based technique that employs secured domain parameters generated to afford high authentication. The curves are generated using an ECC based technique that employs secured domain parameters generated to afford high authentication. The key is randomly generated and therefore, can always be changed or updated after a biometric sample is acquired. The voice input is taken with the microphone and keys are generated from the same voice file stored which is used for ECDSA to provide high level authentication.

3. Elliptic Curve Digital Signature Algorithm (ECDSA)

Digital signature based on an elliptic curve defined over a prime finite field Zp, select a large prime p and choose the parameters a and b for the curve, and base point G of high order n, meaning that n × G = O for a large n. Now randomly **(Assume Blum Blum random algorithm)**

Select X, 0≤ x ≤ n − 1, to serve as your private key. Select only peak with **MAX_VAL=PRIME.**

Next you calculate your public key Y by Y = X × G.

You will make p, a, b, G, n and Y publicly available and you will treat **X as your private key.**

Generate random number K such that 0 < K <n − 1. By one-time and you will discard K after each use.

The digital signature you construct for M will consist of two parts that we will denote sig1 and sig2.

You construct sig1 by first calculating the elliptic curve point K × G and retaining only its x-coordinate modulo n:

$$sig1 = (K \times G)x \bmod n$$

Should the modulo operation produce a zero value for sig1, you try a different value for K.
You next construct sig2 by $sig2 = K^{-1} \cdot (M + X \cdot sig1) \bmod n$, where K^{-1} is the multiplicative inverse of K modulo n that can be obtained by applying the theorem of extended Euclid's Algorithm.
The two signatures for these two documents will look like:
$sig1 = (K \times G)x \bmod n$
$sig2 = K^{-1} \cdot (M - X \cdot sig1) \bmod n$
$sig'1 = (K \times G)x \bmod n$
$sig'2 = K^{-1} \cdot (M' - X \cdot sig'1) \bmod n$.
It compares, if both signatures are same then it accepts otherwise rejects.

Figure 3 and Figure 4 show the capture of the login screen and login change password screen of the research.

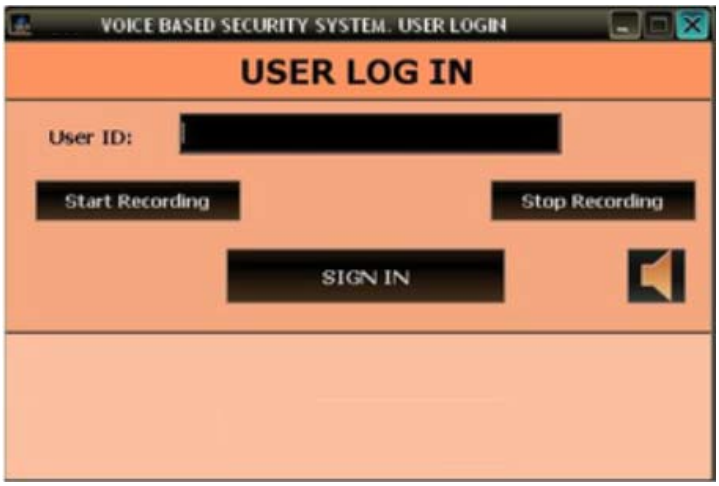

Figure 3. Login screen

Figure 4. Login change password screen

4. Conclusion

Nowadays, voice biometrics is a competitive threat to the more invasive, traditional methods of identification and verification. Our proposed method is comparatively good performance at key generation and the confidential data is highly safe and reliable. Elliptic curve Cryptography is an advanced algorithm which provides more security than any other public key cryptographic algorithm does not provide more security when compared to ECC.

In this paper, we have been designing a new approach that provides security for systems using voice biometrics for authentication and the device used into an authenticator which uses voice itself as its passwords and we are primarily interested in keys that can be temporally reproduced on the same device from the same user's voice. Public and private keys are generated randomly from the user's voice. It includes the operation of selection and register or storing of one or more voice passwords. It uses ECDSA to perform the authentication process that matching the voice sample with the database.

References

[1] Stallings W. Cryptography and Network Security: *Principles and Practices*, 3rd edn.Pearson Education. 2004.
[2] "A New Substitution Block Cipher Using Genetic Algorithm" in FICTA-2013, Srinivasan Nagaraj1, DSVP Raju2, and Kishore Bhamidipati- SPRINGER, Verlag. 2013.
[3] Erik Olson, Woojin Yu. "Encryption for Mobile, Computing"
[4] Ye Zhu, Yuanchao Lu and AniVikram. "On Privacy of Encrypted Speech Communication". *Dependable and Science Computing IEE Transaction*. 2012; 9(4).
[5] U Mahalakshmi and VS Shankar Sriram. "An ECC Based Multibiometric System for Enhancing Security". *Indian Journal of Science and Technology*. 2013; 6(4).
[6] Ann Cavoukian and Alex Stoianov. "Biometric Encryption Chapter from the Encyclopedia of Biometrics". *Office of the Information and Privacy Commissioner*.
[7] D SravanKumar, CH Suneetha and A Chandrasekhar. "Encryption of Data Using Elliptic Curve Over Finite Fields". *Distributed and Parallel Systems*. 2012; 3(1).
[8] K John Singh and R Manimegalai. "A Survey on Joint Compression and Encryption Techniques for Video Data". *Journal of Computer Science*. 2012; 8(5).
[9] Tin Lai Win and Nant Christina Kya W. "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)". *World cademy of Science, Engineering and Technology*. 2008.
[10] Krishna AVN, Vishnu Vardhan B. *Utility and Analysis of some Encryption algorithms in E learning environment*. International Convention Proc. Of CALIBER, 2006. 02-04 Feb. 2006, Gulbarga, India.
[11] Mohsen Machhout et.al. Coupled FPGA/ASIC implementation of elliptic curve crypto-processor. *International Journal of Network Security & its Applications*. 2010; 2(2).
[12] Neil Koblitz. "An Elliptic Curve implementation of the finite field digital signature algorithm". in Advances in cryptology, (CRYPTO 1998), Springer Lecture Notes in computer science. 1998: 1462: 327-337.