A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme

Alok Kumar Vishwakarma[1] and Atul Kumar[2]

[1] *Periyar Maniammai University/IT, Thanjavur, India*
Email: alokkmr461@gmail.com
[2] *Periyar Maniammai University/CSE, Thanjavur, India*
Email: {j.atulkumaran}@gmail.com

Abstract **— The significant improvement in the information and communication Technology (ICT) from last few decades increases various new needs. E-Governance system has also no exception. People are approaching to fulfill their dreams. In the case of M-voting the security is the major issue. Democracy Needs all and only the authorized voters can vote and each eligible voter can vote but not more than once. To achieve these voters need to be registered properly and authenticated. This paper presents a novel approach to provide secure mobile voting based on Biometrics in conjunction with elliptic curve cryptography and steganography (ECC-stegano scheme).**

Index Terms **— Cryptography, Steganography, Biometrics, M-Voting, Information Security**

I. INTRODUCTION

The importance of an improved mobile voting system is beneficial to both Government as well as citizens. By the use of improved security mechanisms only the valid and authorized voters can vote and not more than once. This can be done with the help of WAP mobile phone which is camera equipped with internet connectivity and the voting application installed. The data exchange between the voter and authentication server is carried out with the help of encryption and decryption technique. It uses both Elliptic curve cryptography and steganography for encryption and decryption. With the help of steganography the data can be hided over the insecure channel.

II BENEFITS OF M-VOTING

The M-voting provides several benefits and flexibility due to its enhanced security and user friendly features. Some of the major benefits include

A. Reduced Cost- As the existing methods takes lot of human effort and materials which is expensive. By The use of this method the cost can be greatly reduced

B. Increased Participation- The effective participation is important in democracy. People who are citizen of the India working abroad or out of their states, in that case they can easily vote. As Government provided if the person staying at different place of country rather than its native more than six months then the voter id should be issued but sometimes the people staying at different place for some sort of time less than that or went on trip. In that case this method will be more useful and secure.

C. Greater accessibility for Disabled- This method is more useful for the People who are disabled and cannot go to vote at centers. It is a better option for them

D. Security and flexibility- As this present method uses two factor i.e. Biometrics and ECC-Stegano scheme (Elliptic Curve Crypto-Stegano Scheme) which will provide the enhanced security than the previous existing methods.

III. PROPOSED SCHEME

This proposed scheme based on the face and voice recognition to describe the authentication in real life. Biometrics characteristics cannot be lost or forgotten and are extremely difficult to copy, share and distribute. It requires the person to be present physically. The reason behind the use of the face and voice recognition is the two persons may have the same facial structure and also it is chance that two persons may have the same voice pitch but its impossible and rare that two person with same facial geometry as well as same voice pitch. This kind of security provides the better authentication than any other method. It also combined with the ECC (Elliptic Curve Cryptography) and Steganography to enhance security over insecure channel. The following figure represents the general authentication model.

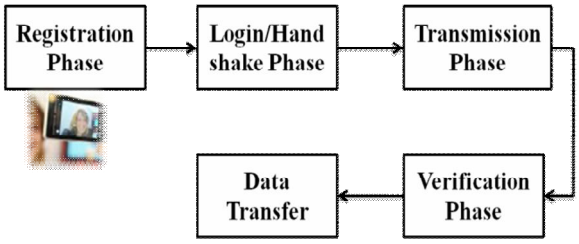

Figure1: General Authentication Model

A. Authentication Process- The authentication process can be done in following different phases.
1) Registration Phase- The registration can be done

either personally or remotely using the mobile by the user. During the recognition phase the following steps are performed by the authentication server. i. Biometric data of the voter is captured, preprocessed and features are extracted. The feature templates are formed and stored as enrolled templates. These saved templates are referred during the verification phase. Face and voice samples are taken in this scheme for the purpose of final template storage in the database. ii. The voter is also given a V-Id (voter-Id) as well as a password. The following figure depicts the registration phase.

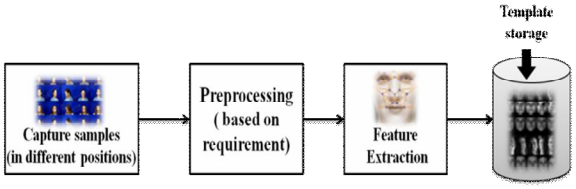

Figure2. Registration Phase

B) Login/Handshake Phase- when the voter wants to login into the server or account the authentication server required to enter his voter-id and password. The authentication server performs the following preliminary steps.

i. Checks current time stamp (T) of the users machine.

ii. Verifies the initial login details i.e. V-Id and Password.

iii. If the prior information is correct then the voter is redirected to the biometric authentication phase and voter is asked to start video and voice transmission through mobile.

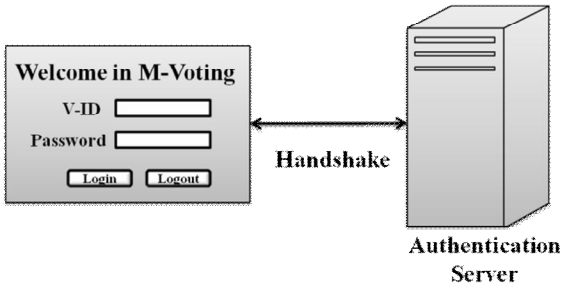

Figure 3 : Login/Handshake phase

C) Transmission Phase- This phase takes care of transmitting information through the internet over insecure channel.

i. in order to avoid the interruption of hackers the data is encrypted using ECC [1] and hidden into some images and videos using steganography.

ii. Even if the transmitted data is suspected by the hacker he cannot extract the secret data or cannot make any change in formation transmitted over the channel.

D) Verification Phase- After receiving the login information and the stego file the authentication server performs the following steps.

i. the server applies the reverse of the embedding secret data procedure to recover the biometric information from the stego file

ii. Applies the reverse ECC algorithm to decrypt the information. iii. Checks the validity of time stamp with the current date and time. If the time limit is within the specified time stamp then it accepts the login request otherwise it rejects the login request. iii. Once the biometrics is derived from the stego file the face and voice recognition [2, 3] takes places and the suitable candidate (voter) matched from the database and provides the authentication.

E) Data Transfer over the channel- The data transfer over the unsecure channel securely is a challenge because lot of intruders and hackers may interrupt the communication and can change the information. To overcome with this difficulty we propose the use of Elliptic Curve Crypto-Stegano scheme. The login information is encrypted before the data transfer and sent over the channel using WTLS protocol. During the data transfer the time stamp is checked and it's provided that the data transfer should take place within the specified amount of time so that the chance of getting interrupted by the hackers and intruders can be reduced. The face recognition can provide for continuous authentication and can be accepted by once the user is successfully authenticated. The encryption is done using the elliptic curve cryptography algorithm and hidden into the images or video files using steganography. This will make it more secure.

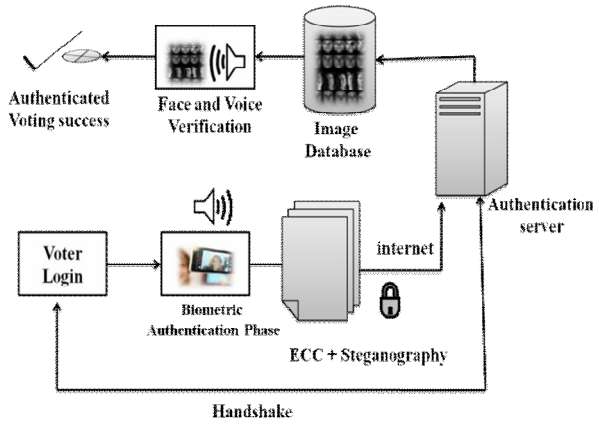

Figure 4: Data Transfer over the channel

F) Mutual Authentication- once all the phases are completed authentication result is generated by the authentication server. This can be done by using MAC

or sending a sms to the user. This will further strengthen the security aspect of the proposed scheme. And it serves as an alarm in case of fault intrusion. In case of voice transmission the user is asked to speak the text displayed on his authenticity window of his mobile which is dynamic and these changes each time the user wishes to login. The server matches the speech with the text. This way it provides another option for secure voice authentication.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve cryptography (ECC) [1, 4] is a Public key cryptography. In Public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key where as the public key is distributed to all users taking part in the communication. The mathematical operations of ECC is defined over the elliptic curve y2 = x3 + ax + b, where 4a3 + 27b2 ≠ 0. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

A. Elliptic Curve Point Addition and Doubling-

A cryptosystem generally requires the use of an algebraic group- a set of elements with custom-defined arithmetic operations. Elliptic curve groups used in cryptography are defined over two kind of fields: GF (p), where p is a prime and GF (2^m) where each element is a binary polynomial of degree m (that can be represented as an m-bit string since each coefficient is either 0 or 1); but it is easier to illustrate Group operations by first examining curves over real Numbers. Figure 5 shows point addition on an elliptic curve. The curve equation is y2 = x3 + ax + b with a = -4, b = 4. To add two points, draw a line through them and reflect the third point, where this line intersects the curve, in the x-axis.

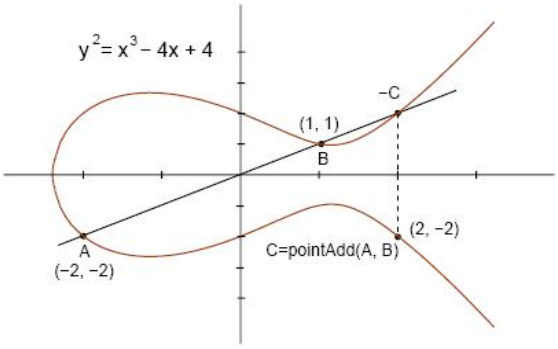

Figure 5

Algebraically, the result of adding points A (xA, yA) and B (xB, yB) is C (xC, yC) such that

xC = s2 – xA – xB , yC = -yA + s(xA – xC)

Where s = (yA – yB)/ (xA – xB) is the slope of the line through A and B. When A equals B, the line through A and B degenerates to the tangent at A (see Figure 6) and s = (3xA2 + a)/2yA.The result of adding A and -A is defined to be a special point called the point at infinity

B. Scalar Point Multiplication-

The main cryptographic operation in ECC is scalar point multiplication which computes Q = kP, a point P is multiplied by an integer k resulting in another point Q on the curve. Scalar multiplication is performed through a combination of point additions and point doublings, e.g. 11P = 2((2(2P)) + P) + P*. Each curve has a specially designated point G called the base point chosen such that a large fraction of the elliptic curve points are multiples of it. To generate a key pair, one selects a random integer k which serves as the private key, and computes kG which serves as the corresponding public key.

C. What makes ECC hard to crack-?

The security of ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), i.e. finding k, given P and Q = kP. The problem is computationally intractable for large values of k. Among other things, this makes it possible for two entities to agree on a shared secret across an insecure communication channel without revealing that secret to an eavesdropper. This secret can then be used as a key to encrypt/decrypt sensitive information.

V. STEGANOGRAPHY

Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the

processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganlysis is process to detect of presence of steganography [5]. In this article we have tried to elucidate the different approaches towards implementation of steganography using 'multimedia' file (text, static image, audio and video) and Network IP datagram as cover. Hiding information into a media requires following elements

1. The cover media(*C*) that will hold the hidden data
2. The secret message (*M*), may be plain text, cipher text or any type of data
3. The stego function (*Fe)* and its inverse (*Fe-1*)
4. An optional stego-key (*K*) or password may be used to hide and unhide the message

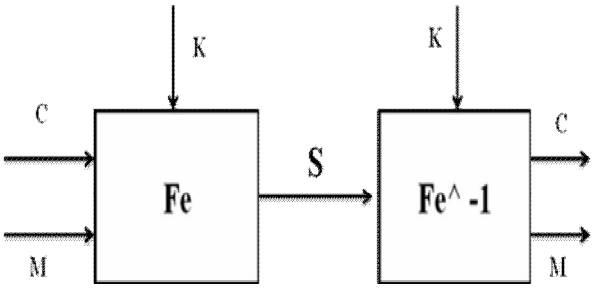

Figure : 7 Steganography Process

VI. ELLIPTIC CURVE CRYPTO-STEGANO SCHEME

The idea behind this scheme is very simple that is, it is the combination of above two algorithms Elliptic Curve Cryptography and Steganography. Because of this it is called as Elliptic Curve Crypto-Stegano Scheme. As the security over the network is a big challenge, this method enables us to enhance the security. In this at first the ECC algorithm is applied on the voter's id as well as image and voice data. It is encrypted and hidden in an image using steganography. After applying the steganography it's very difficult for the hackers to identify that the image which is sent over the network contains any information. If in case the hacker or intruder find out the information which we are sending after applying this scheme, then also he cannot understand the information hidden in the image because of ECC algorithm encryption. As this encryption technique is more secure and hard to crack due to difficulty of solving the Elliptic Curve Logarithm problem. So it will provide the enhanced security over the insecure channel. The use of WTLS protocol makes this much more secure and hard to hack the system.

VII. IMPLEMENTATION

For implementation of this proposed method the voter must be equipped with a mobile phone with camera and the capability of browsing the internet through WAP (Wireless Access Protocol). Apart from this a dedicated standalone client-server application is needed for the successful realization of communication between the user and the authentication server. The authentication server must provide the user with the necessary software. A java web application is the best option for that because the java applications are platform independent and more secure as it provides the better security options. By using the java a better interactive and feature rich software can be developed for this application.

VIII. CONCLUSIONS

Since the general security requires Democracy, privacy, accuracy, fairness, variability, and recoverability which is provided by this Novel approach and it provides the enhanced security over the previous methods with the use of new approach ECC-Stego scheme. As the technology evolves the new advancements will come in the area of information and confidentiality protection which will give a better technology experience to the future generation.

ACKNOWLEDGEMENT

I am thankful to my all staff Members and HOD IT who helped and supported me in publication of this paper.

REFERENCES

[1] Elliptic Curve Cryptography-good enough for government work, SIAM News, Volume35, Number 8,October2002 by Barry A.Cipra.

[2] Forgery Quality and its implications for Behavioral Biometric security, IEEE Transactions on systems, Man and Cybernatics-Part B: cybernatics volume 37, No 5, October 2007 by Lucas Ballard, Daniel Lopresti.

[3] Fusing Face Verification algorithms and Humans IEEE transaction by Alice J.O'toole Hervé Abdi, Fang Jiang, and P. Jonathon Phillips.

[4] Elliptic Curve Cryptography – How it Works Sheueling Chang, Hans Eberle, Vipul Gupta, Nils Gura, Sun Microsystems Laboratories.

[5] Steganography and Steganalysis: Different Approaches Soumyendu Das Information Security ConsultantKolkata,India, Subhendu Das STQC IT Services, Kolkata, India Bijoy Bandyopadhyay Institute of Radio physics & Electronics, University of Calcutta, Kolkata, India, Sugata Sanyal Tata Institute of Fundamental ResearchMumbai,India.