Enhanced Security Using Biometrics and Elliptic Curve Cryptography

Himanshu Ganu
BE IT Student
SAKEC
Mumbai,India
himanshu.ganu@gmail.com

Soniya Jadhav
BE IT Student
SAKEC
Mumbai,India
soniya3105@gmail.com

Neeraj Mhatre
BE IT Student
SAKEC
Mumbai,India
neerajmhatre4@gmail.com

Gargi Patil
BE IT Student
SAKEC
Mumbai,India
patilgargi16@gmail.com

Pramila Shinde
Assistant Professor
SAKEC
Mumbai, India
sakec.pramilas@gmail.com

Abstract—Biometric Systems are systems which acquire, process, analyze and match Biometric credentials with those that are present in the Database providing Verification and Validation.Nowadays, simple biometrics like fingerprints and face recognition can be replicated with some effort. This compromises the level of security. However, combining two or more features like Fingerprint and Face as an authentication parameter, we can group together the features which will significantly increase the level of security as it will be much harder for unauthorized people to replicate both fingerprint and facial characteristics of a user. This paper discusses the systems which provide secure verification to incorporate the method with Elliptical Curve cryptographyusing Genetic Algorithm. Elliptic Curve Cryptography is based on a curve which is generated such that a line passing through any two points of the curve will surely pass through a third point somewhere along the curve. Points generated using Elliptic Curve cannot be regenerated by reversing the algorithm. This makes it very secure to generate encryption keys.

Keywords-*biometrics, elliptic curve cryptography, ECC, genetic algorithm, GA, security, multimodal, identification, verification.*

*****

I. INTRODUCTION

In this rapidly developing world of technology, security is the main concern. Knowledge based security techniques like Passwords, ID's and Pins are slowly losing their level of security. These credentials, if in the unauthorized people, may compromise Integrity and Confidentiality aspects of security. To overcome disadvantages of said conventional system, Biometric systems are used. The term biometric is derived from two Greek words: bios, which means life and matrons, meaning measure. Biometric characteristics include Face, Ears, Iris, Fingerprint, Voice and Signature. Nowadays, just a single Biometric parameter as a credential does not provide sufficient security. Hence, there is a need to develop "Multimodal" Biometric Security Systems. Multimodal means, the combination of two or more biometric features to provide higher degree of security.

II. ABBREVIATIONS

Following abbreviations have been used throughout this document.
ECC: - Elliptic Curve Cryptography
GA: - Genetic Algorithm
DB: - Database

III. BIOMETRIC SYSTEM

There exist two processes in the Biometric System[1].

I. Verification is the confirmation of a genuine identity claim.

II. Identification is to find the user based on their Biometrics.

Registration is the process in which the user provides their Biometrics to be stored in a database which will be later referred during the verification or identification process. This image undergoes various image processing techniques like Feature Extraction, Noise Removal, etc.

ISSN: 2321-8169
396 – 398

During Verification, user's biometrics are acquired and matched with the existing ones in the Database. If verified, the user is granted access to the requested resources.

IV. PREREQUISITIES

A. *Elliptic Curve Cryptography*

Elliptic Curve Cryptography[1] is a public key based cryptography technique based on algebraic structure of an elliptic curve over a finite field. Elliptic Curve has a property that any two points in the elliptic curve is used to produce a new point on the curve. Elliptic Curve Cryptography generates keys through the properties of the elliptic curve equation instead of the traditional method of generating huge primes. An elliptic curve is an algebraic curve defined by an equation of the form: y^2=x^3+ax+b. ECC gives rise to algebraic structures that offer higher strength-per-bit. Elliptic Curve Cryptography is the second generation public key system based on RSA algorithm and Diffie-Hellman key exchange algorithms. The proposed system uses iris and fingerprints as input data to help generate the intended Elliptic Curve parameters. ECC has a very short encryption key which is faster and requires very less computing power as compared to its predecessor RSA algorithm.

B. *Genetic Algorithm*

A genetic algorithm is a method for solving both constrained and unconstrained optimization problems based on a natural selection process that mimics evolution. At each step, the genetic algorithm randomly selects individuals from the current population and uses them as parents to produce the children for the next generation[5]. Over successive generations, the population evolves toward an optimal solution. Genetic Algorithm uses operators such as reproduction, crossover and mutation to get the next generation which provide a better fitness function. Thus, Genetic Algorithm provide a systematic random search[4].

C. *Multimodal Biometric Systems*

Multimodal Biometric Systems are systems that are capable of acquiring, extracting, storing and combining various biometric features, combining them together to form an extra layer of security. Multimodal Systems work by acquiring two or more modalities and extracting their features. These modalities are then subsequently stored in the database. The combination of these stored modalities provides an extra layer of security. Multimodal Biometric Systems are said to be more reliable than Unimodal Biometric Systems because of the presence of multiple, independent traits[3]. Multimodal Biometric Systems also reduce the false acceptance and false rejection rates that are very much prevalent in the Unimodal Biometric Systems.

V. PROPOSED SYSTEM

A. *With Elliptic Curve Cryptography*

The user's biometric[3] modalities are acquired, resized and fused together to form a single image. Using fixed points, a, b and prime number p, elliptic curve is generated. This elliptic curve is then made to overlap with the fused image[2]. One Time Password or OTP is generated and sent to the user by using encrypting above points by using key. The user is given the access only if the password is valid.

B. *With Multimodal Biometric System*

The Multimodal Biometric Systems is an application of the combination of two or more biometric modalities in verification\authentication systems. Images of the biometric modalities are stored in the database in their raw format. Next they are processed and feature extraction is done. The features are then made into a template. A decision function then integrates multiple options. The input is the matched with the template in the database. If the template and the input matches, then the user is authenticated.

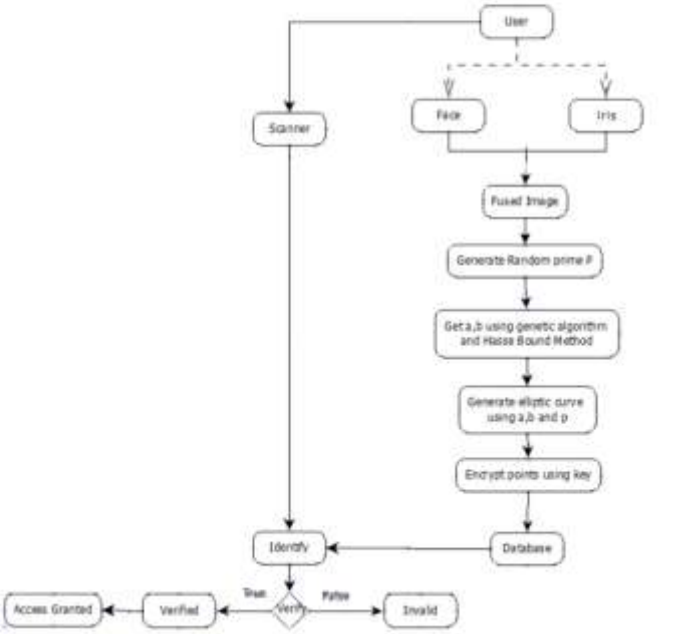

Fig 1: Proposed System

VI. RESULTS

Sets of fingerprint and iris will be taken along with some other random samples of the same. The performance can be measured by false acceptance and false rejection rates. According to the proposed system, two ratios will be calculated for each biometric feature. If both ratios are above a certain threshold value, then access will be granted to the user. The use of multiple biometrics as well as ECC highly increases security as well as reduces false acceptance rates. False rejection is reduced by finding some average constant which allows some difference in biometrics but does not increase false acceptance due to the presence of another biometric. The False Acceptance Rates and the False Rejection Rates together can be used, with the Close match identification to further improve the verification and validation process.

VII. CONCLUSIONS

The system uses Multimodal Biometric features of the user. The use of fused images provides an excellent level of authentication and security. The Elliptic Curve Cryptograph [1] method provides an OTP for authentication whereas Multimodal Biometric System reduces the false acceptance and false rejection rates considerably as compared to the Unimodal counterpart. The proposed system shows a great deal of promise when it comes to enhancing security.

ACKNOWLEDGMENT

We express our sincere thanks to our project guide at SAKEC for the technical guidance, suggestions, motivation, help and facilities provided to us for the successful completion of our synopsis work and for monitoring our progress periodically and solving all our practical problems during our project work. In the end we would also like to thank all those who were directly or indirectly involved with this project.

REFERENCES

[1] Anu Rathi, Divya Rathi, Rani Astya, Dr. Parma Nand, “Improvement of existing security system by using Elliptic Curve and Biometric Cryptography”, in International Conference on Computing, Communication and Automation (ICCCA2015)

[2] Laiphrakpam Dolendro Singhand Khumanthem Manglem Singh “Image Encryption using Elliptic Curve Cryptography”, in Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[3] V. S. Shankar Sriram, Rahul Ramdas, Rashmi Sahay, G.Sahoo “Optimizing Elliptic Curve Domain Parameters Using Genetic Algorithms”International Journal of Secure Digital Information age, ISSN: 0975-1823, Vol-1, No-2.

[4] S. Pramela Dev, Sindhuja K “A Public Key Cryptosystem using ECC and Genetic Algorithm”, in International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February – 2014.

[5] Miss Komal R. Hole, Prof. Vijay S. Gulhane, Prof. Nitin D. Shellokar “Application of Genetic Algorithm for Enhancement and Segmentation.” In International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013