Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 477–488
DOI : 10.47974/JDMSC-1884

Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

Pratik Gite †
Department of Computer Engineering
St. John College of Engineering and Management
Palghar (East)
Mumbai
Maharashtra
India

Mirzanur Rahman §
Department of Information Technology
Gauhati University
Assam
India

Kirti Rahul Kadam ‡
Department of Management
Bharati Vidyapeeth Institute of Management (Deemed to be University)
Kolhapur
Maharashtra
India

* *E-mail:* **dankan.v@bmsit.in (Corresponding Author)**
† *E-mail:* **pratikgite135@gmail.com**
§ *E-mail:* **mr@gauhati.ac.in**
‡ *E-mail:* **kirti.kadam@bharatividyapeeth.edu**

G. Manivasagam [@]
Department of CS & IT
Jain Deemed to be University
Bangalore
Karnataka
India

K. D. V. Prasad [#]
Department of Research
Symbiosis Institute of Business Management
Hyderabad
Telangana
India

and

Department of Research
Symbiosis International (Deemed to be University)
Pune
Maharashtra
India

Abstract

Biometric systems have taken the front seat as having core foundations in 21stcentury digital information technology, biometric systems hold a position therein or authentication processes. But the growing complexity of cyber threats requires greater security practices. This paper presents an innovative biometric security approach based on the combination of ECC and more advanced session keys. The goal is to strengthen biometric systems against sophisticated cyber threats ensuring fast and effective authentication methods. The proposed approach takes advantage of ECC's strength in generating secure biometric data along with session keys dynamically to build a more resilient, yet flexible, security model. It is shown on the simulations that security metrics increase significantly in terms of resistance to common cryptographic attacks and data breaches without decreasing the system performance. This study describes not only the current vulnerabilities in biometric security systems towards more secure and reliable authentication systems by the convergence of biometric data to advanced cryptographic techniques.

Subject Classification: *68P25, 68P01.*

Keywords: *Biometric security, Elliptic curve cryptography (ECC), Enhanced session keys, Cybersecurity, Authentication systems, Cryptographic attacks, Data protection.*

[@] *E-mail:* **mani.mca.g@gmail.com**
[#] *E-mail:* **kdv.prasad@sibmhyd.edu.in**

1. Introduction

The digital age evolves over time, biometric security has gained immense importance in the field of technology. The introduction of biometric systems in different industries such as phones security and border control shows increasing people trust their biological features for identification[1,2]. This change is mainly caused by the very non-copyable nature of biometric data, which provides a much higher level of security than standard password-based solutions[3]. This paper seeks to address these challenges by combining super session keys exist in enhanced elliptic curve cryptography (ECC), which is famous for its good security property with the sizes of the key being relatively small, both safety and efficiency are taken into consideration. The strengthened session keys provide a secondary layer of security, contributing to the robustness and decreased susceptibility to attacks of the system [4]. This innovative approach is aimed at enhancing the security of biometric systems to a great extent and minimizing incidents like privacy breaches, identity thefts. This research has a great potential impact.

2. Literature Review

A comprehensive literature review of biometric security landscapes has shown a variety of approaches, results, and immanent flaws for the last few years. Researchers work by [5,6] have emphasized the credibility offered by the biometric systems in achieving reliable user authentication through bio-identification. Yet, they also point to major issues of security, especially in relation to the biometric data storage and transfer. In the world of cryptographic techniques, elliptic curve cryptography (ECC) has been a common technique due to its increased level of security and efficiency compared with other techniques discussed by [7] comparative analysis on crypto algorithms. Because of the significant magnitude and increased security strength that ECC achieves with its smaller key size, securing confidential data is enabled in a favorable manner. In spite of its benefits, ECC has not been widely applied in biometric systems because the integration is too complex and calculation overheads are significant. The idea of the session keys as a mechanism to bring about security has been discussed by [8,9], this being proven that they are capable of providing temporal communication avenues which are safe from threats[10]. Yet their research identifies a missed opportunity exploiting session keys that facilitates dynamic security within biometric systems calling for

continuous authentication over long- term periods. The effort, therefore of this research is to close such gaps by means of combining stratified session keys with ECC in biometric security systems[11]. Through the integration of session keys that enable dynamic security and ECC, which offers sound encryption, this study offers a fresh solution whereby the risks in today's biometric systems are addressed. This integration is also assumed to, not only increase the level of safety for biometric data storage as well as transmission but also to create a mixed sharpness and changeability that most current systems lack.

3. Proposed Method

In modern society, an identity is perhaps the biggest hurdle to cross. There are several schemes to identify and verify but the most accurate ones in these lie in biometrics[12]. According to Berger and Luck, biometrics refers to a set of unique and observable physical or behavioural characteristics that could be used for automatic recognition or verification of an individual's identity[13].

Figure 1

Key Classifications of Fingerprints

Fingerprint is a structure of pattern containing ridges and valleys. In a fingerprint image, ridges are portrayed as dark lines; while the valleys

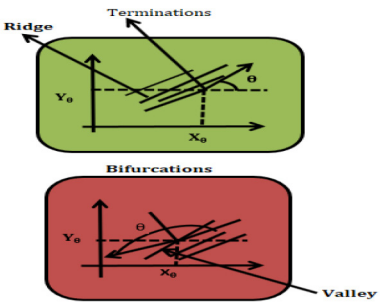

Figure 2

Cessation and Division of Ridges

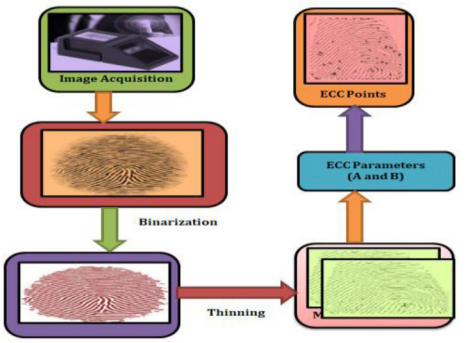

Figure 3

Phases in Fingerprint Pre-Processing

between these expressed in white spaces. There are three primary types of singular regions: loop, delta, and whorl. These singularities contribute to the classification of fingerprints into five major categories[14,15]: Whurl, Right Loop, Left Loop, Arch and Tented Arch. These key fingerprint classes are depicted in Figure 1, which have significant importance in worldwide identification processes. The samples of termination and bifurcation characteristic points shown in Figure 2 are among the most critical items in this classification procedure.

Elliptic Curve Cryptography (ECC) parameters for fingerprints are generated through several key processes[16]. This includes the fingerprint preprocessing, extraction of ECC parameters and computing the public key value.

After preprocessing, the next step will be the determination of ECC parameters and creation of an ECC points. Figure 3 provides the outline of these steps in fingerprint based ECC parameter generation process.

Various thresholding methods are documented in the literature, each with its unique approach: Global Thresholding, Thresholding with Iterative Application of the Laplacian Operator[17]. Finalize these techniques, adaptive thresholding stands one recommended approach for its fast and reliable performance which is highly deployed application finger-prints analysis[18,19]. Under adaptive thresholding, the algorithm is able to respond to variations that occur in an image. The approach works very well if one has a complicated pattern that needs special attention like fingerprints require which must be retained at all costs.

$$I_n(n_1, n_2) = \{I \text{ if } I_{old}\ (n_1, n_2) \geq Mean\ 0 \qquad ow \tag{1}$$

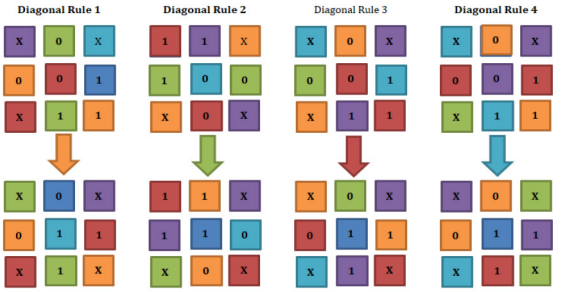

Figure 4

Principles of Diagonal Rules

Figure 5

Narrowed Fingerprint

For adaptive thresholding during binarization, the value of each pixel in the image is replaced with either a 1 or a 0. This task is made by a pixel's intensity comparison to the mean it local neighborhood. The process can be summarized by Equation 1, which essentially states that: If the value of a pixel's intensity exceeds the meancomputed, within its neighbourhood then it is set as 1 (indicating valley). On the other hand, if the intensity of a pixel is less than or equal to the local mean, then it will take 0 value (Ridge). Figure 4 shows these four diagonal thinning rules from [20]. These diagrams depict the usage of rules to refine the ridge patterns into a single-pixel width, without affecting their structure in any way.

The image in Figure 5 would be an excellent demonstration of how the central line thinning algorithm streamlined the fingerprint image for analysis to preserve essential features needed to achieve accurate identification.

4. Elliptic curve primitives Algorithm

ECC primitives are defined with regards to the field operations. These field operations are the basis of ECC and carry out calculations within the framework of elliptic curves. The key operations in ECC include:

Point Addition: This includes two points on the ellipse. Lines joining two points P and Q generate a third point R on the curve resulting from obeying certain geometric and algebra rules.

Point Doubling: This is a degenerate case of point addition corresponding to the same two points. It involves finding a new point on the curve which can be considered the double of the original one.

Scalar Multiplication: This is the operation of scaling a point on the curve by a scalar. First, this operation is the core of ECC and serves as its source of security. It involves repeated point additions.

Point Subtraction: This is the opposite operation of point addition. With the given points P and Q taken on the curve, point subtraction finds a third point R where adding R to nearest Q then gives back point P.

Field Inversion: In this operation field element is inverted, and this is very important for the algebra of elliptic curve.

Field Multiplication and Division: These operations comprise multiplication and division of field elements.

In this work, the presented design utilizes a primary field for ECC implementation. In the level of elliptic curve, affine coordinates and certain algorithms are used for important operations such as point addition and point doubling.

5. Results and Discussion

This study highlights its improvement in biometric environments by the integration of ECC. This result conforms to the claims in [19] that ECC is capable of protecting sensitive data. In addition, the integration of upgraded session keys brings a variable element to biometric security which partly overcomes limitations identified in [20] such as cited. Table 1 shows elliptic curve points from a sample fingerprint, using the ECC109(107,47) curve. In this table, a standard point for elliptic curve cryptography G is chosen as the 'G' point. As seen in Table 2, ECC domain parameters and public key values were derived from fingerprints. The analysis of this data results in the following conclusions: parameters 'A' and 'B', G point, and associated public key for each permutation of a fingerprint are unique and different from one another. This singularity brings out the idiosyncratic element and stability of the ECC parameters and public keys produced from the distinct characteristics of each fingerprint. Figure 6 compares the UQI of prints from both old and proposed approaches. As shown in Figure 6, the recovery of image quality

after an attack is observed by analyzing it which reveals that even when an adversary has managed to execute the attack on the transmitted image, it does not affect the quality of the recovered image. Figure 7 demonstrates the indices of similarity based on diversified approaches of fingerprints. When an intruder attacks the transmitted image, the analysis of Figure 7 discloses that fingerprint recovered is compatible with non-degraded biometric sample as shown by a substantial level of similarity.

Table 1

Elliptic Curve Data Points

(1 40)	(1 68)	(7 103)	(7 8)	(9 39)	(9 70)
(9 43)	(9 67)	(11 22)	(11 87)	(12 15)	(12 94)
(12 14)	(12 93)	(12 16)	(14 93)	(16 29)	(16 80)
(15 26)	(16 88)	(18 34)	(18 75)	(19 2)	(19 106)
(21 3)	(21 109)	(21 29)	(21 80)	(24 31)	(25 78)
(21 13)	(25 96)	(26 26)	(26 83)	(28 19)	(28 90)
(32 16)	(27 93)	(32 101)	(30 8)	(34 32)	(34 77)
(36 47)	(36 61)	(36 52)	(36 57)	(36 105)	(38 4)
(37 23)	(40 87)	(43 16)	(43 94)	(46 45)	(37 23)

Table 2

ECC Domain Information and Its Public Key Components

Fingerprint	A	B	G	Public Key
FP 1	105	49	(54 , 70)	(54 , 13)
FP 2	70	23	(45 , 56)	(14 , 90)
FP 3	74	0	(52 , 80)	(54 , 26)
FP 4	52	24	(54 , 23)	(34 , 40)
FP 5	93	44	(59 , 25)	(99 , 56)
FP 6	75	60	(52 , 72)	(14 , 84)
FP 7	19	6	(46 , 99)	(64 , 65)
FP 8	105	87	(54 , 7)	(24 , 89)
FP 9	73	5	(61 , 43)	(80 , 63)
FP 10	95	65	(54 , 96)	(54 , 10)
FP 11	58	7	(54 , 21)	(14 , 61)
FP 12	105	52	(54 , 62)	(12 , 7)

This finding points out the effectiveness of the suggested algorithm, in that it preserves similarity to UNFingerprint support leeks even with malicious attacks. Figure 8(a) contains an original (freshly scanned fingerprint image), while in the case of Fig. 8(b), the recovered fingerprint image is displayed. Moreover, the 16 highest entropy blocks from HL (High-pass Horizontal) sub-band are chosen in the specific columns and rows where image iris codes have been embedded during transmission. The contribution of this work to the biometric security field is not trivial, especially in regard to devising a practical and secure method for overcoming some of its most pressing challenges. For high-security

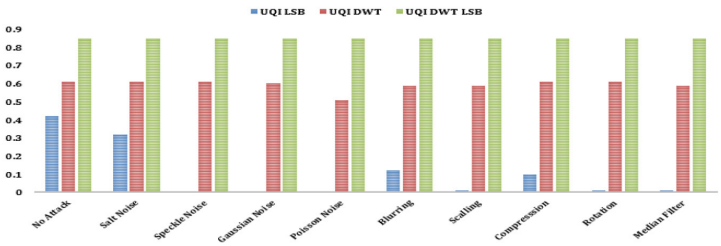

Figure 6

Fingerprint Quality Index Measurement (UQI)

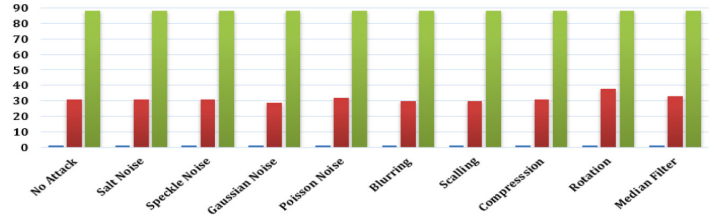

Figure 7

Measure of Fingerprint Similarity

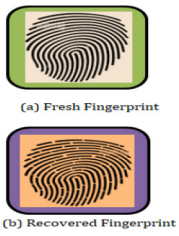

Figure 8

Fresh and Recovered Fingerprint

settings, such ECC with improved session keys may be crucial especially for financial sectors and governmental agencies.

6. Conclusion

In conclusion, this work has managed to bring about and analyze a new biometric security method by combining ECC with revised session keys. The main results show that such an integration is highly conducive toward the reinforcement of biometric systems' security. ECC is a specialized encryption that makes it much harder for persons to hack biometric data, and the dynamic nature of Enhanced session keys adds another layer of protection even better against attacks targeting static information. This research has numerous practical applications. That is why in highly security-related sectors such as banking, government services, and corporate access control, the proposed system proves to be a more reliable and convenient solution than those traditional biometric systems which are used today. High biometric identification accuracy and improved security features of this solution make it a suitable option for these conditions.

References

[1] G. Zhao,W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks," 2010 2nd International Conference on Signal Processing Systems, Dalian, China, pp. V2-640-V2-643 (2010).

[2] Guiliang Zhu, Mengmeng Wang, "Digital image encryption algorithm based on pixels," 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems, Xiamen, pp. 769-772 (2010).

[3] S P Ravi and L Dhanalakshmi, "DWT and Modified AES based Secure Image Steganography on ARM A8 Processor", *International Journal of Engineering Research & Technology* (IJERT) (2015).

[4] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[5] P. Karthika and P. Vidhya Saraswathi, "Image Security Performance Analysis for SVM and ANN Classification Techniques" in In: *Interna-*

tional Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 4, pp. 436-442 (2019).

[6] Shabana Urooj, S Kalathil, Cryptographic Data Security for Reliable Wireless Sensor Network, *Alexandria Engineering Journal*, Volume 72, Pages 37-50 (2023).

[7] P. Ramadevi, S. Vijayakumar, R. Sudha, Security for wireless sensor networks using cryptography, *Measurement: Sensors,*Volume 29, 100874 (2023).

[8] Sadashiva V. Chakrasali, Azhagu Jaisudhan Pazhani, Computer vision based healthcare system for identification of diabetes & its types using AI, *Measurement: Sensors,* Volume 27, 10075 (2023).

[9] Naidu, P. Ramesh, Parth M. & Gupta, Anand Kumar. Development of object identification model with deep reinforcement learning algorithm, *Journal of Information aHarnessing intelligent systems for water managementnd Optimization Sciences*, 44:3, 355–367 (2023).

[10] Ghazaala Yasmin, Jaisudhan Pazhani, A novel method of data compression using ROI for biomedical 2D images, *Measurement: Sensors,* Volume 24, 100439 (2022), ISSN 2665-9174.

[11] Ravi Shankar, Naziya Hussain, Industrial quality healthcare services using Internet of Things and fog computing approach, *Measurement: Sensors,* Volume 24, 100517 (2022), ISSN 2665-9174.

[12] Pullela SVVSR Kumar, B. Ashreetha, Performance Analysis of Energy Efficiency and Security Solutions of Internet of Things Protocols. IJEER 11(2), 442-450 (2023).

[13] N. Hussain, A. K. . N, "A Novel Method of Enhancing Security Solutions and Energy Efficiency of IoT Protocols ", *IJRITCC*, vol. 11, no. 4s, pp. 325–335 (May 2023).

[14] N. S. Reddy and B. Ashreetha, "Technologies for Comprehensive Information Security in the IoT," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, pp. 1-5 (2023), doi: 10.1109/ICONAT57137.2023.10080332.

[15] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.

[16] K. N. V. Srinivas and P. K. Lakineni, "Development of a Real-time Location Monitoring App with Emergency Alert Features for Android

Devices," *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, pp. 1-8 (2023).

[17] Sharma, Kumar & Gupta, Anand Kumar. A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm, *Journal of Interdisciplinary Mathematics*, 26:3, 519-530 (2023).

[18] Prasad, K.D.V. , Veera Sivakumar. A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 861-873 (2023).

[19] Kumar, Abhay. Securing networked image transmission using public-key cryptography and identity authentication, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 779-791 (2023).

[20] M. Nagabushanam, Raghavendra. Vector space modelling-based intelligent binary image encryption for secure communication, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1157-1171 (2022).