Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2025.00164

Review Article

Recent and significant advances in crypto-biometrics: A detailed review

Priyanka BHATTACHARYYA[1], G.S.G.N. ANJANEYULU[1,*]

[1]*Department of Mathematics, SAS, Vellore Institute of Technology, Vellore, Tamil Nadu, 632014, India*

ARTICLE INFO

Article history
Received: 22 April 2024
Revised: 03 August 2024
Accepted: 11 September 2024

Keywords:
Biometric; Cancelable Biometric; DNA; Fingerprint; Iris; Multi-Modal Biometric

ABSTRACT

In the field of information security, Crypto-Biometrics is an advanced technology. Data protection and its secure transmission remain a topmost priority in the current digital era. In recent times, data breaches have become a major issue which affects the organizations across various industrial sectors. In this context, this review on crypto biometrics aims to provide an extensive overview of recent developments in the field of crypto biometrics especially in the area of fingerprints, iris and DNA technologies. The survey provides a comprehensive analysis of the latest development in crypto-biometrics that further focuses on integrating biometrics technology with various cryptographic methods to improve security and privacy. Compared to biometric template, Various algorithms such as advanced encryption standard (AES), triple data encryption standard (3DES), Twofish, Elliptic Curve Cryptography (ECC), Elgamal cryptosystem and Diffie-Hellman key exchange are commonly utilized for encryption, decryption and key generation with enhanced security and privacy. Additionally this review reports various methods and algorithms to improve biometric recognition under various constraints. The study emphasizes the effectiveness and summarises those algorithms with their limitations. Major developments in cancelable biometrics, multi model biometric systems and cypto-bio keys generation are also reviewed in the study. The Survey also addresses several challenges related to biometric template protection, revocability and privacy concern while proposes possible solutions that linked biometrics to cryptography. This comprehensive survey outlines the importance of crypto biometrics for securing sensitive information in the modern digital era. This review also identifies potential areas for further exploration by the researcher.

Cite this article as: Bhattacharyya P, Anjaneyulu GSGN. Recent and significant advances in crypto-biometrics: A detailed review. Sigma J Eng Nat Sci 2025;43(5):1807–1836.

INTRODUCTION

In our era, dominated by information and communication technologies, safeguarding data and ensuring secure transmission have become paramount. Extensive research has been devoted to fortifying data during both storage and transmission phases. With the rapid evolution of these technologies, it's imperative to shield electronic data from interception and exploitation as it traverses communication channels. The potential for eavesdropping poses a

***Corresponding author.**
*E-mail address: anjaneyulu.gsgn@vit.ac.in

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

significant threat, allowing unauthorized individuals to intercept or pilfer sensitive information from computer systems. To mitigate such risks, it's recommended to employ encryption techniques to safeguard data integrity and confidentiality.

Cryptography emerges as a pivotal discipline in meeting these security imperatives. Modern cryptography not only serves to encode messages but also plays a pivotal role in guaranteeing that transmitted information remains accessible exclusively to authorized recipients. Consequently, employing advanced cryptographic methods ensures that any attempt to exploit vulnerabilities in communication channels for unauthorized access to data is thwarted, thereby safeguarding the integrity and confidentiality of information.

Symmetric key cryptography and asymmetric key cryptography are two types in securing the data. In symmetric cryptography such as AES, and DES, the encryption method $C = Enc_k(P)$ and the decryption method $P = Dec_k(C)$ both employ the same key ($k_e = k_d = k$). Two separate keys ($k_e \neq k_d$) are employed in asymmetric cryptosystem (such as the RSA technique), the public key is utilized for encoding a message $C = Enc_k(P)$, while the private key is used to convert the cipher to plaintext $P = Dec_k(C)$.

Ensuring the goals of information security necessitates maintaining the confidentiality of keys, which ultimately relies on the ethical conduct of the individuals involved. The security of the cryptographic technique depends on the reliability of the keys used in the algorithm. If a key is difficult to figure out and impossible to crack [1] in a reasonable amount of time, then it is said to be strong. In this field, constructing hard mathematical problems and generating keys on them are really challenging issues forever. It is highly difficult for a user to remember a key that is particularly large (128, 192, or 256 bits, for instance in the AES method). Additionally, a password-based authentication method is utilized to secure the token or smart-card and limit access to the successful completion of the operation. Conventionally, cryptographic techniques are relied on knowledge-based authentication, such as passwords, or possession-based authentication, such as tokens. However, a password can be misplaced or discovered by brute-force attacks. The non-repudiation property of standard cryptography cannot be ensured by possession or knowledge based authentication schemes.

There is another kind of user authentication system, known as biometrics, which is described as the instinctive identification of individuals based on physiological or behavioral traits. The phrase 'biometrics', which describes the statistical examination of biological data and occurrences, is acquired from the term 'biometry'. An individual's distinctive physical characteristics or other characteristics can be recognized through the procedure of biometrics and computerized devices that record all the characteristics, which is used to verify the individual. Unlike knowledge- or token-based approaches, like passwords or identity cards, biometric attributes are (specific to each particular) more trustworthy at confirming identity. The physical characteristic of a person is reflected in physiological biometric identifiers, which involved fingerprint, iris, DNA, facial, odor/scent, palm print recognition etc. Voice recognition, keystroke dynamics, signature analysis etc. are examples of behavioral trains that are connected to a person's pattern of activity. Some of the physiological and behavioral characteristics of a person are shown in Figure 1.

A general biometric system is depicted in block diagram in the following Figure 2. The methods of 'Biometric technology' are created with the intention of using biometric information obtained through biometric attributes. The biometric system is automatically processed through a mechanism with a set of steps, which includes, (i) Biometric data is to be fabricated in terms of iris, facial image, palm vein, fingerprints etc., (ii) Data extraction from the stored samples, (iii) Comparison of the real-time data with the source database, (iv) If verification reaches the predefined threshold, then authentication will be successful.

Biometric technology is composed of both hardware and software. Hardware for assembling, studying, and matching biometric information is known as a biometric recognition device. Biometric information is a specimen of a person that is specific to that individual. A biometric engine is a part of the software integrated into biometric technology that processes the biometric information that has been collected. The software often takes place in conjunction with the hardware to run the capturing procedure of the biometric data, extract data, and perform indistinguishability, regarding data matching. An image capture module gathers an individual's fresh biometric information with the use of a sensor during the process of capturing biometric data.

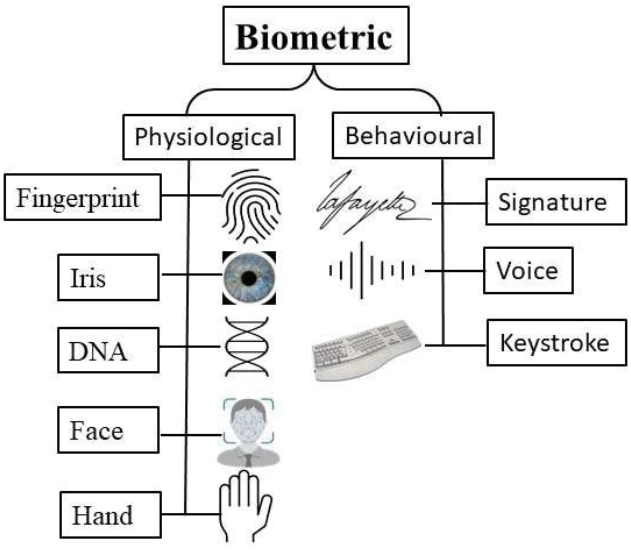

Figure 1. General classification of biometric schemes.

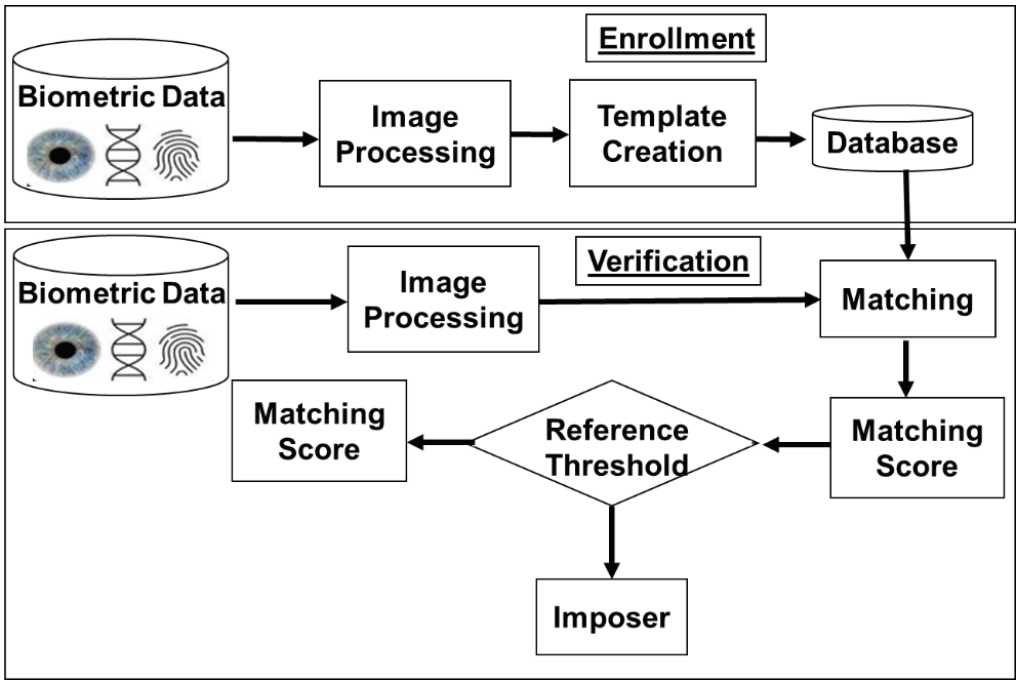

Figure 2. Systematic representation of generic biometric system.

Biometric identification enables a persistent connection between the user's identification and the verifier. In the event of a breach, the biometric information cannot be restored because it is inextricably linked to the user. Furthermore, the usage of biometrics poses a threat to privacy. The personal information of a user may be stolen by connecting the biometric information recorded in several databases.

There are approaches to address the issues that arise from the use of both cryptography and biometrics by integrating both. This composite system, also known as crypto-biometric systems, combines the capacity of biometric technology for individual authentication to boost the safety of cryptographic techniques. Together, these two methods can improve and strengthen the configuration of the system since they have supplementary qualities.

The necessary confidence for encryption can be provided by utilizing the high correlation between the biometric traits and user's identification. Additionally, biometric information can be protected using cryptographic methods while maintaining security. The most straightforward approach is to verify each user using their biometrics and once the verification is successful, free the confidential key relating to the user to the system. Biometric technology can verify only one bit at a time. To achieve a key, a hacker could replace the bit with a relevant outcome (like a Trojan house). The limitation of this method lies in poor setup between cryptographic techniques and biometrics. However, there are certain issues with the crypto-biometric scheme.

A biometric system must include the protection of biometric template to guarantee the confidentiality and the secrecy of biometric information [2]. Biometric systems have their own issues, including the inability to be revoked, a lack of diversity, and potential privacy breaches. The user authentication system is revocable in nature, which implies that if the validator (e.g., Password) is hacked, a new authenticator can be used instead. In this system, it is not possible for the previous validator to authenticate. Here the user is totally linked to their biometrics characteristics. This makes the biometrics data unchangeable because the biometric qualities are innate and immutable [3]. The templates created in different biometrics systems are remarkably similar under consideration of the identical biometric traits. If a template in a system got compromised, it poses a significant security risk in the system. This is because, biometric traits are permanently associated with specific systems and cannot be replaced with new data. This indicates an inadequacy of variation in templates. As a result, it is possible to log into other systems using a hacked template from one system. The interconnection of templates could jeopardize user confidentiality.

To address the drawback such as irrevocability, non-diversity, and potential invasion of privacy, a new field of study as cancelable biometrics has developed [4–6]. The biometric data in these frameworks is altered by using a one-way transformation. In the altered domain, a matching process takes place between two sample readings from templates. A determination of authentication success or failure results in such a differentiation. Regrettably, because it functions like the traditional biometric authentication system, using it for cryptographic purposes leads to a poor connection between cryptography and biometrics. Furthermore,

biometric information must be transferred across insecure networking channels, to use remotely. Consequently, it is necessary to create a revoking, irreversible encryption key that can be generated from biometric of two independent people while maintaining their confidentiality and secrecy.

There are various methods [7,8] that can establish a solid connection among cryptography and biometrics. The aforementioned system endeavors to acquire biometric data containing encryption keys. These keys, which are achieved using biometric information, are alluded as crypto-bio keys. Key formation [9] and key re-generation are the two main strategies. The key formation system retrieves a reliable bit-sequence known as a crypto-bio key. Several authors on [10–12] provide several instances of key formation systems. Whereas key re-generation systems, which associate a randomly generated key to the source biometric information before regenerating it using a distinct biometric specimen [13–15]. A solitary biometric identifier-based biometric system cannot meet the severe accuracy requirements placed by high-level safety appliances and large-scale recognition systems. By compiling data from multiple biometric traits, multiple biometric systems get beyond this restriction. Multi-biometric systems are more accurate at identification and have a wider community coverage than systems that just use one biometric feature. To make a trustworthy identification determination, the data from diverse resources might be combined at different levels. While discussing several biometric methods, four considerations need to be taken into account which includes the source of the data, the method of operation, the degree of fusion, and the fusion strategy. The different subcategories of multi-biometric systems are multi sample, multi sensor, multi instance, multi algorithm, and multi modal. The verification for the initial four situations is acquired from single biometric attributes, whereas the confirmation for the fifth situation comes from numerous biometric qualities [16]. The combination of multiple biometrics shows that the system's confidentiality and dependability have improved. Different degrees of combination in multiple biometric systems is provided as follows:

- **Sensor level fusion:** Prior to feature extraction, the verification provided by the raw data from many resources of information is combined at this level.
- **Feature level fusion:** Combining data from two independent sets of the same person's biometric attributes.
- **Score level fusion:** Integrating the result of the match scores issued by several biometric matchers to reach a final authentication,
- **Rank level fusion:** The process of combining all the ranks produced by various biometric sub- system to create a consent rank for every identity.
- **Decision level fusion:** When just the person biometric matcher's decision outputs are available, combination is done at the decision level.

These levels in actual execution will be implemented in biometric technology as given in Figure 3.

It is important to choose biometric traits carefully such that at least one of them is exceedingly challenging to take a picture. A secure biometric cryptosystem will be provided by two or more biometric traits combined with an improved cryptographic key generation process.

In the present scenario data secureness has become a big challenging issue in view of network security. Biometric cryptography plays an important role in overcoming the facing challenges. In the year 2019, Kaspersky researchers observed that one-third (37%) of the computers in the company's telemetry that gather, process, and store biometric information were the targets of malware attacks in the third quarter [17]. Recently in the first quarter of 2022, India faced around 18 million cyber- attacks, which are mostly happened during digital transactions as per the data reported by Google's Royal Hansen [18]. Data analysis of cipher shows that approximately 28000 cyber-attacks have come up during the COVID pandemic period [19].

The primary research gap in biometric cryptography is the lack of a thorough analysis that integrates advancements across fingerprint-based, iris-based, and DNA-based cryptography. Despite numerous studies reporting on each approach separately, there is a significant need for a comprehensive comparison and in-depth understanding of

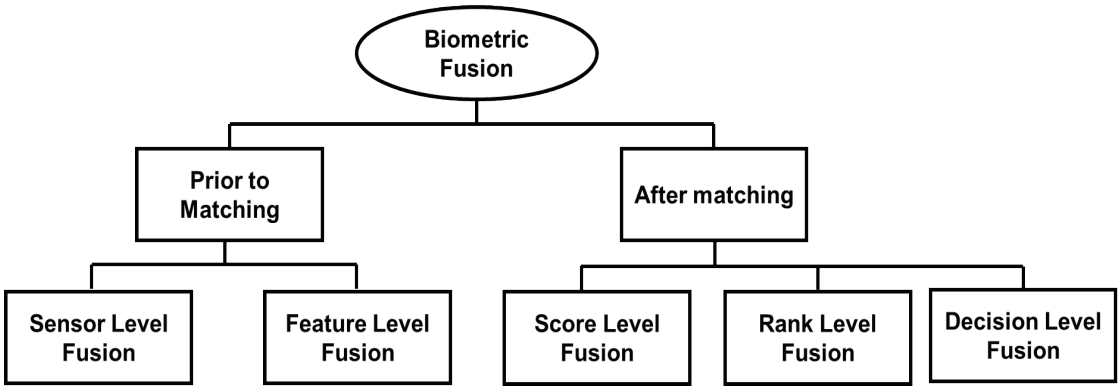

Figure 3. Various levels of fusion.

their performance, limitations, and integration potential. Previous studies have mainly explored biometric approaches in isolation. But they have failed to analyze the benefits and challenges of cross-modal systems and the complexity of scalability, efficiency, and privacy protection. In addition, various issues such as template protection standardization, error correction in fingerprint systems, and the real-time applicability of DNA cryptography are remained unsolved which hinder the progress of this field.

In this context, we present a comprehensive survey on biometric cryptography, which emphasizes the security, privacy, and technical aspects of biometric technologies. This review paper critically evaluates the recent literature by providing a clear overview of the current state of research and identifies its future directions. It also focuses to guide further advancements in biometric cryptography by addressing those overlooked topics. The present study focuses and analyzes the current research and developmental work on crypto- biometrics. In this review, the main attention has been given to fingerprints, iris and DNA-based cryptography.

The initial section of this review provides a comprehensive overview of biometric cryptography, where brief summary of the needs of this research is discussed. In the next section, the details survey focusing on latest advancements in fingerprint, iris, and DNA-based systems have been highlighted. This section qualitatively describes the critical role of integrating biometric data with cryptographic models to improve the security and efficiency of digital communication systems. Then a thorough analysis of various cryptographic models is provided where the performance and effectiveness of various model is compared with existing conventional methods. Finally the review concluded with a brief summary of the key findings and insights from the previous literatures. The conclusion thoroughly discusses the potential advancements in biometric cryptography, addressing current limitations, and an indicative future opportunity for researchers in this field.

DETAILED CURRENT SURVEY ON BIOMETRICS

Review on Fingerprint

Each person has a unique fingerprint, supported by a personal pattern and unique print set. To distinguish one fingerprint from another, it shares three key characteristics that are arch, loop, and whorl. These three characteristics are classified based on the direction of the ridges. Among three characteristics; Arch**:** has ridges that rise from the center to all directions; Loop**:** has ridges that have a circular pattern, which enter from one side, flow around the center, and exit on the other side. Whorl**:** have ridges that form a spiral pattern. The following Figure 4 describes the characteristics of fingerprints. These are the following reviews on fingerprints based on Cryptography.

This section summarizes a series of recently published articles in the area of fingerprints. The integration of fingerprint features into a biometric key-dependent cryptosystem represents an innovative strategy to enhance overall system security. By incorporating fingerprint characteristics as a key component, the system is strengthened against unauthorized access or breaches. The fingerprint-generated key coupled with the system's cryptographic key is shown in Figure 5. In this research, the authors suggested an effective method for extracting minutiae from biometric images to generate irreversible cryptographic keys using fingerprint biometrics. For segmentation, the picture is partitioned into blocks. The gray scale difference is determined for every block. It is relegated to the background if the value is less than the global threshold, otherwise it is allocated to the foreground. The variance threshold distinguishes the foreground and background regions. The ridge structures are present in the segmented foreground sections, while the remaining regions have not been touched. In terms of distinguishing the foreground and background regions, a variance threshold of roughly 100 has been shown to offer the best results. The Normalized image is represented by equation (1),

Figure 4. Characteristics of fingerprints.

$$N(i,j) = M_0 + \sqrt{V_0 \frac{(I(i,j)-M)^2}{V}} \quad if\ I(i,j) > M$$
$$= M_0 - \sqrt{V_0 \frac{(I(i,j)-M)^2}{V}} \quad otherwise \tag{1}$$

For a pixel I(i,j), the estimated mean and variance are denoted by M and V, respectively. M_0 and V_0 represent the intended mean and variance values. As a normalization method, histogram equalization is a mechanism for enhancing the contrast of images by altering their intensity values. The original image's histogram shows that all the intensity values are on the right side of the 0–255 scale and there are no pixels on the left. The normalized image's histogram reveals that the range of intensity values has been modified, resulting in a more equal distribution of dark and light pixels. The suggested approach generates a 128-bit cryptographic key from the system and a 128-bit biometric key from the fingerprint minutiae. A 256-bit secret key is formed by combining those two keys [20].

In conventional cryptosystems, managing and ensuring the confidentiality of keys poses challenges. The Key Distribution Center (KDC) is primarily used for key distribution, which is further secured through enhanced privacy through the integration of biometric data. The KDC facilitates secure communication in symmetric cryptography. In symmetric cryptography, which often uses a special key to share the session key [21].

The fingerprint biometrics of the communicating party serves as a solution, involving the distribution of the session key alongside the user's fingerprint-based key. There is no way to compromise the unique key because it is produced using the user's fingerprint. This eliminates the need for the communication party to memorize the unique key since it is linked to the user's biometric information. The knowledge-based authentication of KDC is converted to biometric authentication using this method. The user's identity is kept secret even if the KDC is compromised, which safeguards the privacy of fingerprint identity. The KDC is registered with user fingerprint information. Minutiae points are retrieved from the fingerprint image after pre-processing. The fingerprint data is converted into a cancelable template using a one-way Cartesian transformation function [4]. During this transformation process, minutiae points are separated into cells, and each cell can include one or more minutiae points. Minutiae points are moved in accordance with the location of their new cell after the cells are randomly shuffled (using a key as the transformation parameter). The cancelable template created using a user's fingerprint data is registered with the KDC. A Unique Id (UId) is given to the user, and the cancelable template that corresponds to the UId is kept in the KDC database. A user's cancellable fingerprint data may be enrolled in one of two methods. The cancelable template can be sent to the KDC over an encrypted channel. Alternately, a user can physically enroll his fingerprint data in a safe position using an offline enrolment method.

A modified minutiae point with (x, y) coordinates values is a component of a cancelable template. First, a minutiae point (let's say, M_i') is chosen, and then the distances (D_{ij}, where $i \neq j$ and $j = i + 1$, $i = 1$ to n) of this minutiae point from every other minutiae point (i.e., M_I', where $I = i + 1$ to n) are determined. Each distance can be recorded as a vector which is denoted as $D = (D_{1,j+1}, D_{1,j+2}, \ldots, D_{n-1,n})$, where $j = 1$ to n, n = the number of total minutiae in cancelable template. The average distance D_{avg} is calculated using the equation (2),

$$D_{avg} = \frac{2}{n*(n-1)} \sum_{i=1}^{n-1} D_{i,j} \tag{2}$$

The average distance D_{avg} in each distance D_{ij} is compared and matched, which results in a key in the binary form. If the distance exceeds the average, the bit is 1, and if

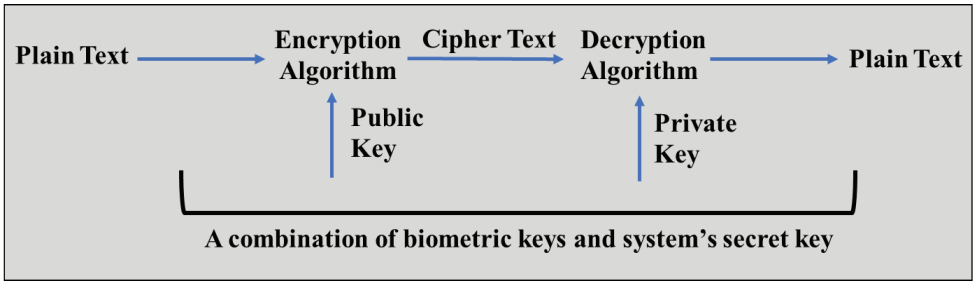

Figure 5. Generation of secret key combining biometric keys and system's secret key.

Table 1. Segment specific time

Execution	Extracting features	Creating cancelable template	Producing key	Overall time to produce a key
Time (sec)	0.05	0.006	0.003	0.059

not, it is 0. This results in the production of a binary vector K_p from all components of the distance vector D_{ij}. To create an everlasting key of N bits, the initial N bits of K_p are required. As a result, KDC creates the fixed keys K_{ps}, K_{pr} from the cancelable templates of the user S and R, respectively, and uses these keys to produce an encrypted communication link with the communication party. Then, for the pair of communicating parties mentioned above, the KDC chooses a confidential key at random. Messages between users S and R will be safely transmitted using this secret key.

For experiment purposes, one fingerprint is used as the input and a genuine key which is everlasting is created using that fingerprint image. The key to the impostor is created using the left fingerprints in the uniform database of fingerprints. In this suggested method, authors have contrasted the genuine key to impostor keys made from different fingerprints to assess the resilience of the genuine key. It is determined that the counterfeiters are unable to produce a key in a manner that is like the real key. The length of the impostor's key is half as long as a genuine key, on average, according to Hamming distance. As a result, to successfully crack the real permanent key, the impersonator must estimate at least half of the bits or 128 bits of the 256 bits. The overall time to construct a key from a fingerprint picture is calculated to assess the overhead time of the proposed method as reported in [21]. The implementation period considers the time spent extracting features, creating cancelable templates, and producing keys. The following Table 1 includes the segment-specific time.

Utilizing a key-pair generated from fingerprint impressions provides a more secure approach to encryption and decryption processes. The ability of the key generation technique to generate the key from the retrieved minutiae points of the fingerprint biometrics is an efficient technique for ensuring the privacy and security of the key creation process. A matrix is used for representing the scanned picture of the fingerprint in the minutiae point extraction procedure. A set of number of furrows and ridges in a small section is represented by the matrix consisting of data regarding the number of ridges and the furrows. In the method proposed by Ankit et al., minutiae points are extracted in a three-step process, and the scanned image is then converted into machine-readable data to analyze the pixel values. In the ridge thinning technique, repetitive erosion is used to identify the ridges of pixel of width one and then the suggested system, which is based on the minutiae point method [22], creates both public and private keys from an individual's fingerprint minutiae points. The time taken for every process is calculated in this work. The suggested method offers the advantage of not requiring the asymmetric key to be kept in a secure location, which drastically reduces security risks. The economic growth of this kind of biometric cryptosystem would be the main emphasis for future development, which would guarantee that any communication channel or network is secure [23].

When two parties communicate over an unsecured channel without prior acquaintance, the main limitation of the Elgamal cryptosystem is the necessity for a pair of encoded messages. The recipient's public key and the sender's private key are used in this computation to encode the message. For highly secret data exchange across the system, instead of using a random number as a private key in the calculation, employing a specific fingerprint ensures better security. The system's data exchange is made more secure by the organizations that uses a specific finger impression as a framework for confirmation [24]. The rough edges of a finger leave a distinctive mark. They are always unique since they are created in person during their final development prior to birth. In the field of criminological study, fingerprints play a significant role. Techniques for coordinating distinctive marks are categorized into three kinds. It consists of edge include based, details based, and connection-based coordinating. The idea put out by Sergey Tulyakov [25] is to protect biometric systems by using symmetric hash capabilities.

Since the user's fingerprint is saved in a database and only pulled out upon authentication, no one may pretend to be the sender using this Elgamal encryption system. By adding a random exponent k, Elgamal makes the Diffie-Hellman key exchange procedure simpler. This exponent takes the place of the receiving party's private exponent. This makes the technique easier to use and allows for one-way encryption without the involvement of the second party. The ability of the algorithm to encrypt electronic messages that are sent via public store and forward services represents a significant advancement of the algorithm in this case. A key component of the encryption process is the randomness of the random exponent k selection, as the ability to guess the random exponent provides the attacker with a large portion of the information needed to decrypt the message. Following the decryption procedure, sender A will select a number arbitrarily and generate a fresh public key, each time A wants to convey a message to the receiver B. In the suggested approach, the sender's (A) produced random number (k) and the receiver's (B) private key serves as each party's unique fingerprint. The decimal values of each fingerprint are obtained. The fingerprint's decimal value was collected through a biometric authentication appliance. With this proposed approach, the sender and the recipient can encode and decode the data while ensuring non-repudiation and verification. It is more safe to communicate information through a system with high confidentiality when a particular finger impression is used as the private key in the computation rather than a random integer.

Integrating fingerprint recognition with cryptographic methods, particularly through the Secure Hash Algorithm SHA-512, combines advanced image processing with SHA-512 to enhance the efficiency and security of fingerprint-based authentication. The study creates a robust identity verification system by extracting distinctive identity

verification system through SHA-512. The hashin process gets optimized through the use of SHA-512 loop unrolling resulting in improved performances along with maintained security feature. This approach reduces the resource allocation and thereby makes the standalone device economical and power efficient. The Look-Up Table (LUT) utillization is reported to be reduced from 63% to 33.07% along with Flip-Flop (FF) utilization decreased from 36% to 13% and Clock Buffer Resources (BUFG) utilization rate stands notably low at 3.13%. This results showcased the improved efficiency in budget allocation, lesser time consumption in hashing. This feature makes the process suitable for time sensitive applications. Future studies can explore the integration of Field Programmable Gate Arrays (FPGA) for further optimization of resource expenditure towards the improvement of system efficiency [26].

Generating symmetric cryptographic key by using fingerprint biometrics offer a unique system in securing communication technology. The system uses a combination of Diffie-Hellman key exchange and fingerprint authentication to create a secure communication channel to encrypt and decrypt between two party's sender and receiver. This system is more secure, convenient and scalable against several attacks, man-in-the-middle attacks, and impersonation attacks. The workflow of the system is as follows: Initially, by using Diffie-Hellman key exchange, the sender and reciever exchange their public keys. Then a figerprint template is generated by the corresponding sender from their fingerprint images, followed by an encryption of the template with the use of public key of the recipient. After recieving the encrypted template from the sender, the reciever uses their private key to decrypt it. Then both the decrypted template and original fingerprint is compared. If the fingerprint matches, the reciever gets to know that the message is sent by the intended sender.

The system is then examined by using four fingerprint image datasets refer to FVC2002 databases (FVC2002DB1, FVC2002DB2, FVC2002DB3, and FVC2002DB4). Each of this dataset contains 100 subjects, consisting 8 impressions per subject. Performance was assessed based on the FVC protocol, which dictates that all unique impression pairs from the same subjects are used to generate genuine cryptographic keys. The results demonstrated that the system achieved a high level of accuracy [27].

Biometric security is enhanced by integrating Elliptic Curve Cryptography (ECC) with advanced session keys, improving protection against sophisticated cyber threats. By combining ECC with dynamically generated session keys, the approach adds an additional layer of protection, which significantly enhances the security of biometric systems against various cyber threats. The study demonstrates that this innovative method remarkably improves resistance to common cryptographic attacks, such as those targeting static information, by incorporating dynamic session keys. Compared to the traditional static key mechanism, this dynamic session key makes the system more secure and prevent the attackers from exploiting the system. The simulation results in the proposed system substantially resticts the data breaches and subsequent security threats, resulting in increasing security parameters. Moreover, the approach maintains high system performance while strengthening security, as indicated by the successful simulations that highlight its effectiveness without compromising operational efficiency [28].

Elliptic Curve Cryptography (ECC) parameters for fingerprints are generated through several key processes, including fingerprint preprocessing, ECC parameter extraction, and public key computation [29]. The literature outlines various thresholding methods, such as Global Thresholding and Thresholding with Iterative Application of the Laplacian Operator [30]. Among them, particularly adaptive thresholding is suggested due to its speed and reliability in fingerprint analysis [31,32]. In the complex patterns of fingerprints, where it is important to preserve intricate details, this procedure is effectively adapted.

This work notably highlights the recent advancements in biometric security carried out with the integration of Elliptic Curve Cryptography (ECC) and effectively protects the sensitive dataset as reported in [32]. Through incorporating upgraded session key introduces dynamic features to the biometric security and thereby overcome various limitations as discussed in [33]. This study shows that apart from the parameters 'A', 'B', 'G' and the public key associated to each fingerprint are distinct and stable. This feature reveals the novelty of the ECC parameters derived from a single fingerprint. Fingerprint Quality İndex analysis shows that the recovered image after the attack is qualitatively protected. This method potentially tackle the practical challenges indicating its effectiveness against potential threats. The integration of ECC in enhanced session key is found to be advantageous in high security environment including financial sector, defence agencies due to its improved identifications accuracy and security.

An encrypted security model integrating OTP, cryptography, and fingerprint sensor technology was devised to enhance the security of biometric systems. Within this network an OTP generator that can be changed intermittently with variations of inputs. The architecture of this methodology is furnished in Figure 6. The whole system can be implemented through an application in android mobile. The potentiality of the system extended to a pattern identification scheme, where a set of template-based features can be obtained for the enrolled personnel [34].

The system will be accessible after first logging in by the administrator and then by the user. Here admin has the authority to carry out the registration process of a user by taking the fingerprint as well as identification documents of the user. Registered customers can retrieve their own data through biometric as well as OTP verification. The system algorithm consists of (i) Advanced Encryption Standard (AES) Algorithm and (ii) Time-Based One-Time Password (TOTP). The AES algorithm constitutes by three

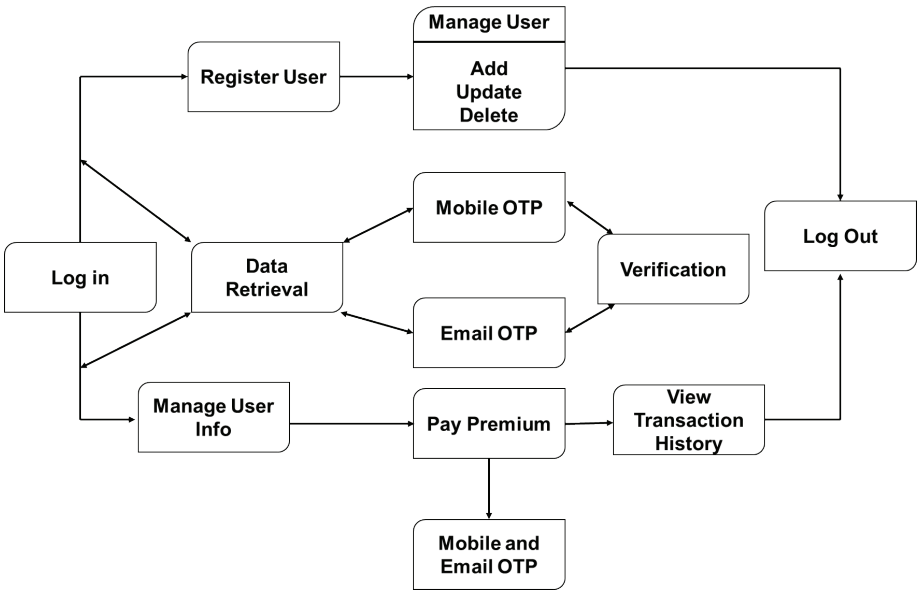

Figure 6. Architecture of the proposed methodology [From Pawar et al. [34], with Permission from Solaris Publication].

block ciphers. By using 128-bit, 192-bit and 256-bit cryptographic keys, all ciphers perform to encrypt and decrypt the block data. Whereas TOTP algorithm executes the OTP in the android-based application in a definite time interval.

As reported in [35], it is not practically possible to generate the same key from an interferer's fingerprint. Neither the user's fingerprint nor the encryption key needs to be stored. This improves the scheme's security. The proposed solution guarantees the confidentiality of a user's biometric data while also addressing the issue of encrypted key storage. Inside the same region of all the fingerprint photos of the same person, a collection of minutiae points is carefully chosen. This assures that all the images of fingerprint of the same person use the same collection of minutiae points. The suggested method only examines ridge ending and ridge bifurcation points. The local pattern of pixels where the ridge terminates or divides is distinguished by analyzing the depleted binary image. Feature points were extracted from the fingerprint image using NIST's NBIS software tool FpMV (Fingerprint Minutiae Viewer) [36]. A fingerprint image is taken by this tool and it outputs minutiae points with x and y coordinates, angles, qualities, and types of minutiae. The keys are generated using x and y coordinate values in the suggested method. Gray coding is an essential component of the presented method since it reduces inconsistencies between keys generated from numerous instances of the same fingerprint. The gray code representation lowers the mistake caused by minor differences in the distances between two minutiae spots in two distinct fingerprints. The practicability of the presented scheme is investigated by calculating the specified difference between the key strings, as a key created using an impostor's fingerprint differs significantly compared to one created from another occurrence of the same person's fingerprint. The Hamming distance is employed to quantify the difference between two key strings extracted from identical fingerprint images. It calculates the number of differing bits between two binary strings. In the case of legitimate fingerprint, the highest Hamming distance is 20, whereas the average Hamming distance is 12. The impostor fingerprint has maximum and average Hamming distances of 81 and 65 respectively. In this suggested technique, error correction codes are used to fix tiny variations in keys of the same person's fingerprint. The stated scheme becomes much more intriguing as a result of this.

A novel Biometric Cryptosystem is introduced based on fingerprint identification, utilizing an Eigen space algorithm instead of traditional geometric methods. It organizes Eigen space and computes Eigen values and vectors from fingerprint images taken at various angles. In this method (Figure 7), the authors first analyzed fingerprint images from different positions and computed an average image for the training set. Each image $I(x, y)$ in an $N * N$ array is transformed into a $N^2 * 1$ vector. Let $I = [p_1, p_2, p_3, p_4, \ldots, p_N]$ represent the pixel values. After normalizing each image, the normalized image is calculated using $\emptyset_p = \frac{1}{N}\sum_{n=1}^{N} \emptyset_n$, resulting in a normalized image $I' = [p_1', p_2', p_3', p_4', \ldots, p_N']$. After that average image is calculated by, $A = \frac{1}{p}\sum_{i=1}^{p} I_i'$. Finally, projecting all images onto this eigen space, h_i is calculated by equation (3),

$$[e_1, e_2, e_3, e_4, \ldots, e_p]^T \; \frac{1}{p}\sum_{i=1}^{p}(I_i' - A)^2 \qquad (3)$$

where, e_1, e_2, e_3, e_4, …, e_p represent the eigen space vectors, each of which is N-dimensional. In the next step, an unknown input image is projected onto the eigen space

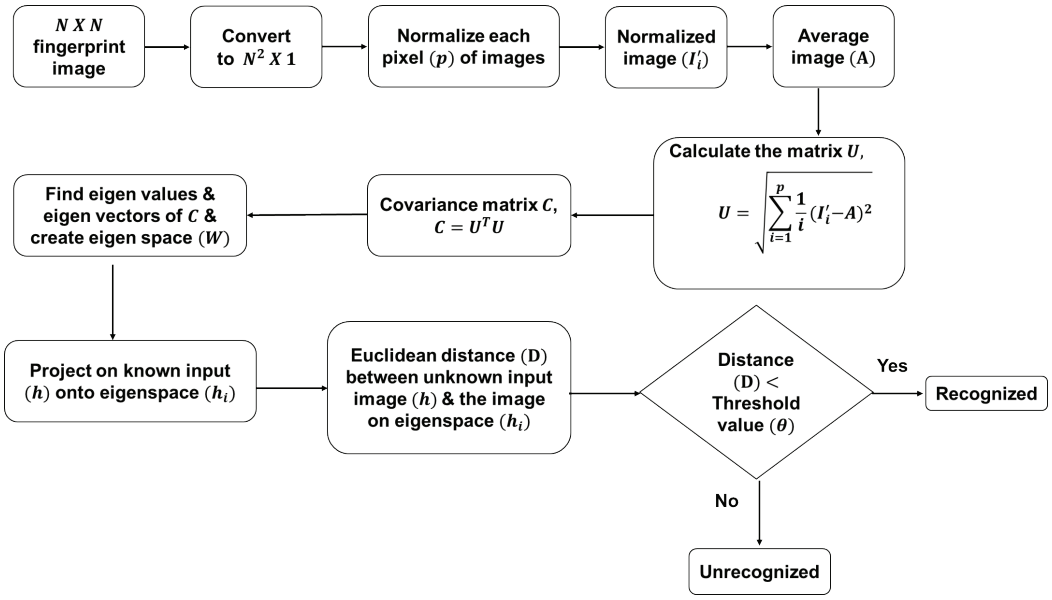

Figure 7. Schematic block diagram of fingerprint recognition model as demonstrated in [37] [Drawn by the author].

which results in a p -dimensional point labelled as h. The Euclidean distance between point h and eigen space image h_i is then calculated. If this distance falls below a predetermined threshold, the image is identified; if not, it is considered as unknown.

The effectiveness of this methods across diverse subjects is validated by experimental results. The practical recognition systems customize the precision and efficiency of the system by considering limited sample sizes. This further forms an universal Eigen space through averaging the image and standardizing the pixel value. The time complexity of this method is estimated as $0(p^{3/2})$, demonstrate the simplicity, speed and reliability of the system compared to other methods. This research lacks efforts to improve success rates, especially for larger databases, and to assess real-time applications across different programming languages and hardware platforms [37].

A study aims to demonstrate a prototype of a password-less authentication system integrating cryptographic methods, steganography, and physiological and behavioral biometrics. It shows that the password-less authentication is scalable and can be acheiviable while balancing both security and usability. This model integrates threat modeling techniques to identify security requirements and appropriately select the proper security protocols. The comparative analysis also shows that the system works as effectively as other password based systems with reasonable authentication time-frames without any additional hardware costs. The system effectively eliminates the risk of data breaches by avoiding the password storage and their hashes. This techniques presents the password-less system as a potential alternative which addresses various user related challenges [38]. Table 2 summarizes some important results from the recently published articles based on fingerprint.

Review on Iris

Unique Iris pattern recognition can be used in cryptography to create secure passwords and encryption keys and a digital representation of the eye that can be used to authenticate users and encrypt data. The four main regions of the iris, shown in Figure 8, that are used for iris recognition are,

Internal region: Pupil, is the most stable and least susceptible to changes in lighting.

External region: Sclera (the white of the eye), contains many unique features to identify individuals.

Lower region: The region below the pupil which is less susceptible to occlusion by eyelids and eyelashes.

Upper region: The region above the pupil which contains many unique features to identify individuals.

This section summarizes the recently reported articles in the area of Iris.

In 2008, a ground breaking biometric cryptosystem using iris recognition was introduced. It involves during

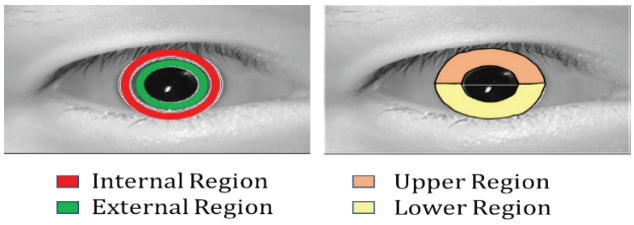

Figure 8. Different regions used for Iris Recognition [39] [Drawn by the author].

Table 2. Significant contributions based on fingerprint

Datasets Used During Performance Analysis	Method	Processor	Advantage	Ref.
-	Generating secret key by combining the fingerprint characteristics as a key and Cryptographic key	-	Fingerprint for enhance security of data	[20]
FVC2004	MINDTCT tools of NBIS software The traditional key distribution center (KDC) is strengthened by the integration of user's fingerprint data, this allows parties who want to connect with one another to share a secret key using fingerprint data.	-	Fingerprint for key distribution center	[21]
http://www.academia.edu/4814389/D01211622. http://www.yaldex.com/tcpip/0672325659_ch20lev1sec1. html.	An encryption and decryption technique that leverages a key-pair derived from fingerprint impressions.	-	Fingerprint for Network Security	[23]
-	To enhance network security and support this analysis, the ElGamal algorithm has been implemented.	-	Fingerprint for Enhanced Security Mechanism	[24]
FVC2002 databases (i.e., FVC2002DB1, FVC2002DB2, FVC2002DB3and FVC2002DB4)	A combination of Diffie Hellman key exchange and fingerprint authentication to create a secure communication channel to encrypt and decrypt between two party's sender and receiver.	Commercial software VeriFinger SDK	Fingerprint for Secure communication	[27]
INSURANCE COMPANY's data	Retrieval of data and cryptography AES algorithms and non-repudiation and verification while allowing for encoding and decoding between the sender and the receiver.	TOTP (Time-Based One-Time Password): TOTP in RFC 6238	Fingerprint for Insurance Data Retrieval with Additional OTP Generation and Verification.	[34]
Fingerprint Verification Competition (FVC) 2002 Database DB1	To derive a cryptographic key directly from the unique features obtained from a user's fingerprint.	NIST'sNBIS software tool FpMV(Fingerprint MinutiaeViewer)	Fingerprint for Cryptographic Key Generation.	[35]
-	Eigen space approaches is used. The identity of the individual is known if there is a minimal distance between Eigen space and the unknown picture.	R-software	Fingerprint for user recognition	[37]
-	Combination of cryptographic methods, steganography, fingerprint for password-less authentication. Threat modelling approaches to identify the system's security requirements and choose the best cryptographic protocols.	JAVA	Fingerprint for password less authentication	[38]

encryption process by utilizing a 256-dimensional textural feature vector extracted from the iris image through 2-D Gabor Filters. Reed-Solomon Code generates an Error Correction Code (ECC) simultaneously. Then the feature vector is transformed into an encryption key via a Hash function. This cipher key is employed by encryption algorithms to secure sensitive data. ECC rectified the feature vector obtained from the input iris in the decryption process. The Hash function converts it to the cipher key. Finally, the data is decrypted using standard decryption techniques with the key [40].

Another study proposes that a unique iris cryptosystem is developed using a modified fuzzy vault algorithm and iris texture features, effective in fingerprint cryptography [41,42]. CRC codes are generated and mixed with the original message, then encoded using Reed-Solomon to produce RS codes of length 256. Grids B and C, each 256 *X* 3, are created as vaults [43]. RS codes are placed in Grid C

with remaining rows filled with random integers for data obscure. Grid B is filled to minimize dissimilarity between vectors from identical iris images. During decryption, the modified fuzzy vault unlocking algorithm retrieves the feature vector from the decryption iris. RS decoding recovers the message and CRC codes, which are then used to check decryption success. The variations between most of their corresponding elements of two vectors taken from the identical images of the same iris are smaller than the vault tolerance. This difference can be eliminated by determining the order of Grid B by choosing the elements in every row that is closest to the corresponding elements of decryption vector. FAR, FRR, and MC code lengths are 0, 4.6296%, and 128 respectively.

Error-correcting code and Hashing algorithms have been proposed by several authors as the foundations for the iris cryptography system [12,44]. This method assumed that the maximum error rate of the iris templates utilized for encrypting and decrypting is not exceeded 10%. The biometric data is exposed through the secured error-correcting code. Hao [14] rectified the disparities between the encoding and decoding of iris codes using Hadamard and Reed-Solomon code. The weakness in the system lies in its low level of security (Breaking ratio= 2^{-44}). In this paper, an innovative cryptosystem based on the production of iris keys is suggested to address these shortcomings and enhance security. Iris distortion, CCD camera pixel noise, eyelashes, among the other factors, create differences in features retrieved from different images of the same iris. As a result, the iris features cannot be employed as a cipher key directly. This paper employs an error correcting method to eliminate the difference to tackle this challenge. The iris textural feature vector is translated using the Hash function and the Reed- Solomon error-correcting algorithm.

John G Daugman [45] uses the preprocessing procedure to locate and normalize the iris. The inner 3/4 of the bottom half of an iris is defined as a region of interesting (ROI). The ROI is then converted into a (256 * 64) pixels rectangular block. A set of 2-D Gabor filters are applied to the normalized iris image. By converting each iris vector's component to an integer between [0, 15] the feature vector is obtained. The public database CASIA 1.0 [46] is used to test the practicality of the proposed system. Selecting three images of each iris for picture blurriness, occlusion, and other different issues, author conducted (108 * 107) imposter decryptions and (108 * 1) genuine decryptions. After completing all of the decryptions, the result of FAR and FRR are 0% and 5.5556% respectively. The value of FAR is ideal for preventing data from being effectively decrypted by an imposter. The probability of accessing the message from the vault without the real iris can be determined using the equation (4),

$$p = \frac{\sum_{i=0}^{64}(2^i * C_{256}^i)}{3^{256}} \approx 2^{-137} \quad (4)$$

In other words, the security of this system is equivalent to that of a 137-bit cipher key, which is significantly stronger compared to Hao's method, which has a security level of 44 bits. This method has a FRR of roughly 6%, which indicates that 6% of real users will have to present their iris more than once for decryption, which can still be accepted. For this cryptosystem, a more fruitful technique of extraction can be developed, and the suggested system can be tested on a big database.

A unique and highly secure cryptographic key is created from an iris template by employing AES for encrypting and decrypting identification data. For the genuine identification test, this study utilizes two distance metrics—Hamming distance and Euclidean distance. The Log-Gabor technique is used for feature extraction. The authors evaluate the FAR and FRR at various thresholds using both distance metrics, finding that a threshold of 0.4 yields the optimal FAR and FRR. Additionally, the authors analyze the Equal Error Rate (EER) and Total Success Rate (TSR). The TSR, which measures the verification performance of the iris cryptography system, is calculated as shown in the following equation (5),

$$TSR = \left(1 - \frac{FAR + FRR}{Total\ no.of\ accesses}\right) X\ 100\% \quad (5)$$

In this case, the Equal Error Rate (EER) is 3.68%, while the computed Total Success Rate is 89%. The comparison results of using Hamming distance and Euclidean distance, are given in Table 3, which we collected from available literature [47].

When compared to the result of the Hamming distance, the result of the measurement of Euclidean distance is substantially weaker and ineffective for the application of iris recognition. Because of its efficiency and simplicity,

Table 3. Comparison Results Using Hamming Distance and Euclidean Distance

Threshold Value (0.4)	Hamming Distance	Euclidean Distance
FAR (%)	0.02	20.5
FRR (%)	11	41.51
FAR (%)	3.68	28.7
FAR (%)	89	56.41

Hamming distance is an appropriate distance metric for computing the difference between one iris template and several templates. But Euclidean distance metric is inadequate for iris template matching. The efficiency of this iris cryptography system can be enhanced by researching and using a hybrid of several error-correcting code techniques to address the burst and backdrop of an iris picture error.

The phase correlation technique is another efficient technique to establish a novel iris recognition system [48]. The iris boundaries in the digital image of the eye are identified using a Canny Edge Detection technique and a Circular Hough Transform. Circle Houghman Detection technique is utilized to build up the speed of the suggested system. In the normalization module, the proposed system employs the Image Registration technique to align a newly acquired picture, $I_a(x, y)$, with a database image, $I_d(x, y)$. The intensity of the new image has been created to be close to points to the reference image, when a mapping function $u((x, y), v(x, y))$ is used to convert the original coordinates. The mapping function at equation (6) must be selected to minimize,

$$\iint (I_d(x,y) - I_a(x-u, y-v))^2 \, dxdy \tag{6}$$

while being limited in capturing an image coordinate similarity transition from (x,y) to (x',y'), meaning,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} - sR(\emptyset) \begin{pmatrix} x \\ y \end{pmatrix} \tag{7}$$

In this scenario, *'s'* acts as the scaling factor, while $R(\emptyset)$ is a matrix that corresponds to a rotation by $\emptyset$. When implemented, for a specific pair of iris images I_a and I_d, the warping parameters *'s'* and '$\emptyset$' are obtained through an iterative process of minimization. For this iris picture registration, a phase correlation base approach is applied. The efficiency of the result offered by the phase correlation method is considerably high.

The normalized iris region is convolved with a 2D Gabor filter to encode the iris region's features. The encoding method creates a bitwise template that contains a lot of bit data, as well as a noise mask that is consistent with the contaminated area of the iris pattern and identifies the template's bits as corrupt. For comparing the quantified vectors and verifying users, Hamming distance measurement is utilized. To enhance security, the Reed-Solomon method is used to encrypt and decrypt data directly. By applying proposed Hadamard and Reed Solomon error correction algorithms, authors were able to reach a 60 percent accuracy rate for a single accurate capture between two different photographs of the same iris. The appropriate acceptance ratio could increase to 93.6% if multiple photos for a single iris are saved for matching and comparison.

By employing visual cryptography, the method [49,50] offers dual-layer security to the biometric template, ensuring the preservation of the iris template's extracted image within the proposed approach. In addition, each template is given a distinctive number that is encrypted by employing Visual Cryptography. CASIA eye image database [51] has eye images of 756 grayscale with 108 unique eyes or types and seven various images for each individual eye. In this paper, JAVA platform is used to execute the system for the improvement of the security.

The primary flaw with traditional cryptography is that it is incapable of identifying legitimate users. Traditional methods rely on the presence of a token or on knowledge. It is possible to crack them. The human iris is a distinctive structure that can be used for non-invasive biometric analysis. It is reported that encryption keys in software-based cryptography are lengthy bit strings. It is difficult to remember such a big list of random numbers. It is also vulnerable to brute-force attacks or other techniques. Biometric cryptography was introduced to improve the security of encrypted data. For the experiments, the Casia iris database was used to obtain iris images for feature extraction process. A 128-bit secret key is chosen from an iris image which is used as the key in AES encryption. In this paper, Radial edge suppression is used for extracting the image after segmentation. For Normalization process, Dougman's rubber sheet model is applied. Five tests are carried out to ensure that the key is random [52].

Visual Cryptography method is a key tool to create unique key with the use of the iris template for security improvement [53]. Employing the VC module for storing the extracted iris image in the database with the use of random number generator algorithm has proven to be an innovative technique to keep iris templates safe. Visual information (images, texts, etc.) can be encrypted using the cryptographic technique in visual cryptography which enables decryption to be done entirely by sight. Visual cryptography transforms encrypted images based on the principles of human visual perception. The whole system is working based on the two phases: (i) Enrollment, & (ii) Authentication. SNF module is used for segmentation, normalization, and feature extraction process in the enrollment phase. The author employed the VC module for storing the extracted iris image in the database by using the random number generator algorithm. The author has proposed an automatic segmentation algorithm using Circular Hough Transform to analyze the boundary of the iris and the pupil. Daugman's rubber sheet model is used for normalization process. In the authentication phase, a comparison is made between the iris template and the extracted image by sending the image of the eye to the SNF process. In this paper, shares are generated by using the generated random number as input to the VC module only for the monochrome images. The colored eye image will be the focus of future development with the use of color visual cryptography for generating the shares. The proposed visual cryptography method in this paper will solve the problem of the existing method by generating high quality shares [54].

The iris image database pictures are first trained by utilizing segmentation, normalization, Hough transform and feature extraction processes respectively. The text picture is then used to extract the features of the database's matching iris image. The size of the database determines the time it takes to train and text the image [51,55]. For feature extraction, the normalized iris pattern is converted into a 1-D Gabor wavelet. The obtained information is generated and quantized into bit-wise templates that are in adequate sizes for both the real and fictitious responses. The working procedure of the proposed algorithm is described by the following flow chart below (Figure 9). This method is used for the iris template to make it safer from attacks in addition to providing a centralized database to the users [56].

About 10-20 iris database images are used in the suggested technique. Each of the databases has about 20 images of it. This work was carried out by using the MATLAB and the summarized result is given in Table 4, which we collected from [56].

The time of implementation is dependent on the size of the database. As much as the number of images increases, the execution time is also increased.

To develop an efficient method for iris recognition, a study is done by employing advanced techniques such as Hough transform, Daugman rubber-sheet model for iris segmentation, normalization. The equation (8) refers to Log Gabor filter used for iris feature extraction,

$$G(f) = \exp\left[\frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^2}{2log\left(\frac{a}{f_0}\right)^2}\right] \quad (8)$$

In addition, this equation utilizes 3DES and Twofish algorithms to improve the privacy through the encryption of iris template. It is then concealed within a cover image using a least significant bit technique using steganography, which ultimately creates a stego image. This process makes the changes in master file to be undetectable which addresses the template security in biometric recognition. Twofish, Triple Data Encryption System, and LSB steganography are utilized to emphasize the security Iris template. This technique primarily executes two operations: securing and retrieving. In first operation, Iris template and cover image are taken as inputs whereas stego image along with cover image in the second operation. Over successful operations, the outputs of stego image and iris template assert the strength of the system in the steganography algorithm. This process highly secure the iris template and reducing the risks in information technology environments [57]. The generation of iris biometrics based encryption keys through the extraction and normalization of iris data effectively identify consistent regions within the iris structure. This methods creates feature vectors from local space filling curve descriptors. This encryption keys are generated from the features vectors created from local space. Hybrid feature selection, neighborhood component analysis along with interval-based encoding scheme are combined to express these keys as a distinct feature vector. As shown in Figure 10, the dynamic biometric key generation system is tested with various iris datasets using illumination and rotation invariant descriptors. This results demonstrate that keys in the range of 333 to 1120 bits exhibit high randomness, unlinkability, revocability. This system is reported to be secure against brute-force and JPEG compression attacks. The key generation rate of this system has been achieved up

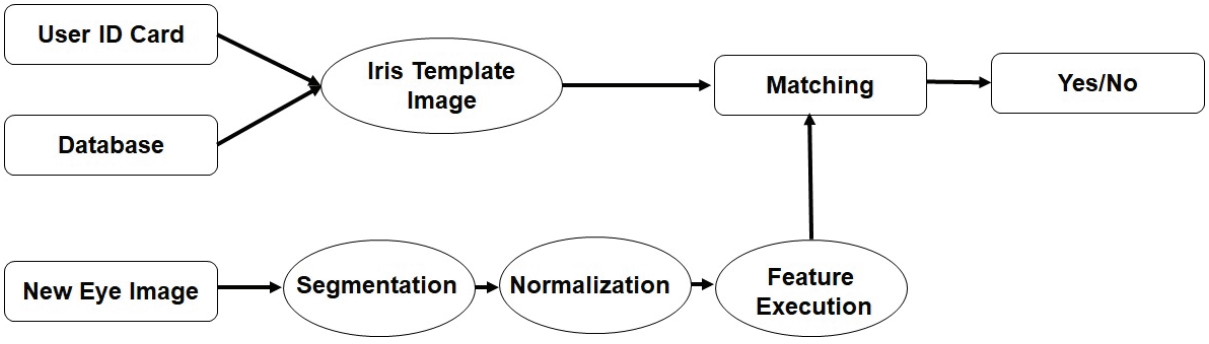

Figure 9. Working Procedure of the proposed algorithm [From Udayini et al. [56], with permission from Blue Eyes Intelligence Engineering and Sciences Publication].

Table 4. Implementation Time

Images in the database (No.)	10	20	30	40	50
Implementation time (sec)	~ 0.602	~ 0.699	~ 0.735	~ 0.806	~ 0.832

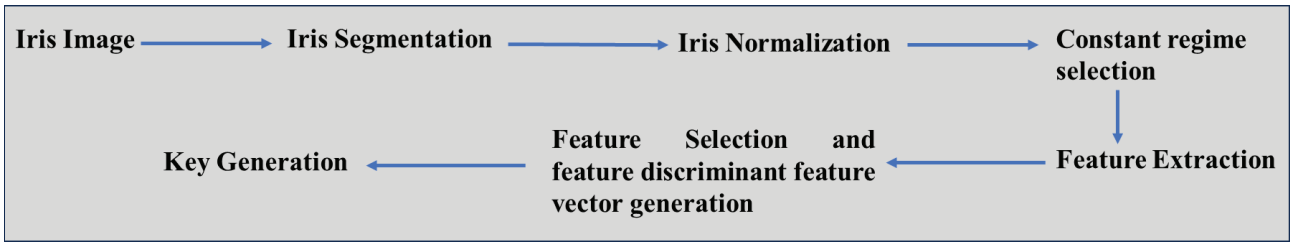

Figure 10. Schematic model for iris-based key generation process as proposed in [58] [Drawn by the author].

to 95.50%, which outperforms existing methods in terms of false acceptance rate (FAR), false rejection rate (FRR), and true acceptance rate (GAR). This results make the system suitable for cryptographic applications in cyber-physical security, IoT, and cloud computing. Future research could explore improving key generation speed and testing with other biometric modalities [58].

The unique iris texture can effectively use to generate secure encryption keys. This provides a secure method for protecting sensitive informations. Using the Histogram of Oriented Gradients (HOG) algorithm, keys of varying lengths (64 to 1024 bits) were produced. The security and reliability of the keys are rigorously tested using chi-square, ENT, and GAP tests. Multiple implementations were performed using high-resolution iris images which shows that the keys consistently maintains high randomness across different samples. The study also suggests that biometric features such as fingerprints can generate similarly secure encryption keys, which offers a wide range of applications for improving cryptographic systems [59].

Firdous Kausar [60] proposed an iris-based cancelable biometric cryptosystem that provides authenticity to the user and safety encryption of user healthcare data which is secured and authenticated. Symmetric key-cryptography is used for encrypting that data and in the encrypted form keeping it on the smart card. The secret encryption key is bound to the patient's cancelable iris template using the fuzzy commitment approach. Using the owner's iris template of the healthcare smart card, the suggested approach allows user verification as well as decryption of healthcare data as needed. The main beneficiation of this paper is the effective combination of a cancelable biometric system with the Fuzzy commitment scheme-based key-binding technique for verifying and safely reserving patient healthcare data on a smart card. The helper data is created with the integration of the secret key's Reed Solomon (RS) encoding and a cancelable transformation of the patient's iris biometric template. The author used symmetric key-cryptography methods to overcome the crucial issue of key-management by authorizing healthcare professionals and patients to share the encoded key, preserving it nowhere. It can be accessed at the running time once the user has successfully completed iris-based biometric authentication. To tie the cancelable iris template with the secret key, author use Reed-Solomon codes. In comparison to [61], where the maximum key length is 63-bits with FAR of 0% and FRR of 63%, the exploratory findings demonstrate that it can be successfully acquired a key of maximum 252-bits with FAR of 0% and FRR of 7% from the input iris template. According to the security analysis, the adversary is unable to extract the secure key from the stored data on the smart healthcare card. Before applying a secret key to the iris template, a non-invertible cancelable transform function prohibits the attacker from performing a cross-matching attack or obtaining a secret key from the user's stolen iris template.

The One-Time İris Code (OTIC) encoding scheme effectively addresses the security concerns related to transmitting Iris Codes between clients and servers. As depicted in Figure 11, the model converts the iris code into an 8 X 8 binary matrix and distorts it by rotating the matrix in one of five possible directions. Thus the security of the original code is enhanced. In the next step, the distorted matrix is linearized into a 64-bit sequence, then a 33-bit timestamp is embedded at random positions using four random numbers. This results in 97-bit encoded iris code which is then combined with 3-bit rotation parameter which forms a 100 bit OTIC. This data is then transmitted to the server which decodes this OTIC by reversing the rotations and extracting the embedded timestamp and reconstruct 64-bit Iris Code. The method minimized the risk of the compromisation of the Iris code [62].

The histogram processing of iris images, along with FAR vs. FRR and time complexity analyses, showed that the proposed Iris Recognition System (PIRS) offers greater security and efficiency compared to conventional systems (CIRS). The Equal Error Rate (EER) of PIRS is 0.44, which is nearly similar to CIRS (0.2 to 0.5). PIRS exhibits higher resistance to common security attacks such as MITM, brute-force, and replay attack. The time complexity of PIRS is O(log n) which is lowered than the time complexity of CIRS (O(n)). This leads to faster execution, enhances overall security and minimizes the risk of original iris code compromise.

Cloud storage is relatively economical and flexible business models, but security breaches remain a major concern in various threat landscapes. To enhance data protection in public cloud environments, a biometric-based authentication approach is proposed in the study [63]. The study improves cloud security by combining biometric authentication, encryption, and data placement methods that protects the sensitive information from unauthorized

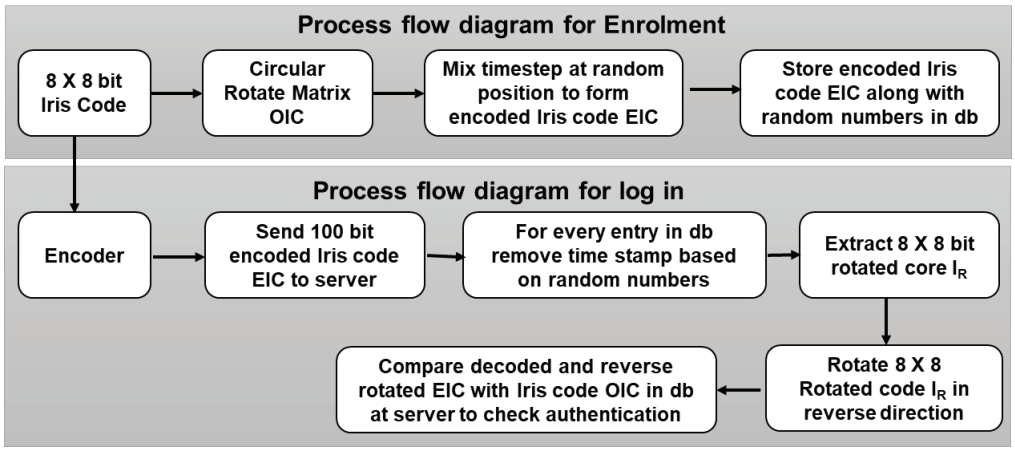

Figure 11. Enrollment and login process [Harikrishnan ei al. [62], with permisstion from Elsevier].

access and potential misuse within cloud environments. This study introduces an integrated crypto-biometric system (ICBS) for secure data access. In addition to this, a data-placement method is introduced which is based on splitting and merging the data into multiple storage containers. This approach ensures accountability, privacy and protection against unauthorised access. This approach further enhances storage efficiency and provides safety assurance even in dispersed across a public cloud environment. Integrated Crypto-Biometric System (ICBS) improves overall data security in cloud environments. This results in strong authentication and secure access control. Furthermore, This approach reduces potential vulnerabilities through the distribution of data pieces across different locations and thereby reducing the chance of a data breach or unauthorized access to the entire dataset.

This study introduces an efficient data placement strategy, alongside supplementary techniques for data partitioning and merging. The cloud storage system utilizes data partitioning [64] and distributes the divided data across multiple object storage containers within the IBM Bluemix cloud.

To improve performance during the classification process, a more sophisticated learning model like Support Vector Machine (SVM) can be applied. A schematic flowchart of Iris based recognition in cloud processing is displayed in the Figure 12. The use of the suggested biometric authentication approach helps minimize latency, prevent data loss, and optimize packet handling while processing

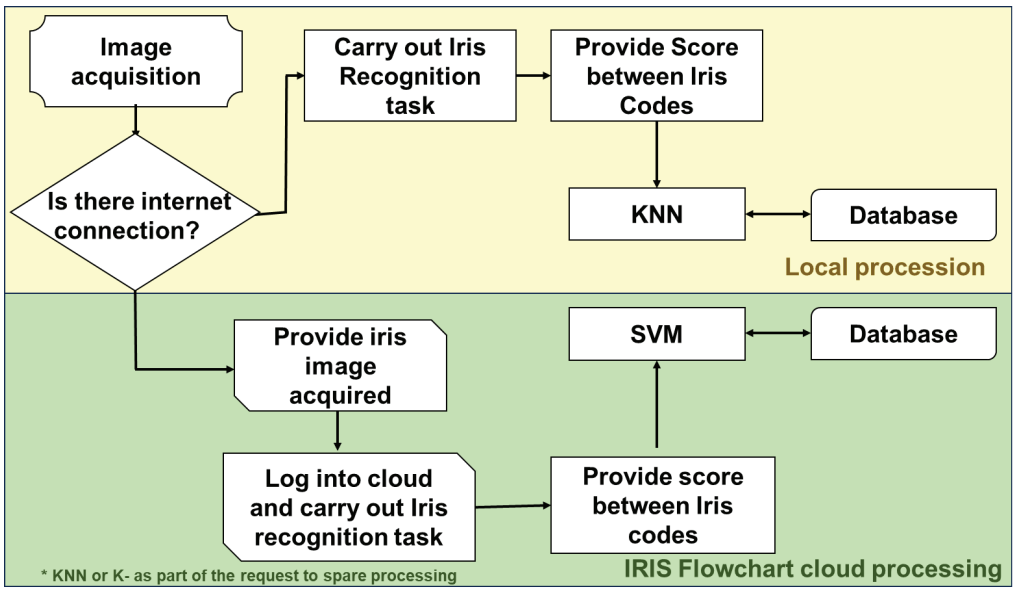

Figure 12. Schematic flowchart of Iris based recognition in cloud processing.

Table 5. Significant contributions based on Iris

Datasets Used During Performance Analysis	Method	Processor	Advantages	Ref
Database CASIA 1.0	To remove the differences caused by iris distortion, eyelashes, eyelids occlusion etc., Reed-Solomon error correcting code is used. The iris textural feature vector is converted to a cipher key for encryption and decryption using the error correcting code and hash functions.	-	Iris Key Generation	[40]
Database CASIA 1.0	The system derived vector features from the iris and utilized an altered fuzzy vault algorithm for encrypting and decrypting messages.	-	Iris for Information Security	[43]
Database CASIA 1.0	To derive a distinctive and reliable cryptographic key from an iris template. The AES cryptography algorithm is utilized for encrypting and decrypting iris image data. The identification process for template matching uses distance metrics like Hamming distance and Euclidean distance.	MATLAB 7.0	Iris for Identity Document	[47]
CASIA 1000 Iris Image Database	A technique for image registration based on phase correlation that converts the iris texture from cartesian to polar coordinates.	-	Iris for Normalization Process	[48]
Database CASIA 1.0	To provide two-fold security to the iris template using Visual Cryptography.	MATLAB & JAVA	Iris for Visual Cryptography	[49]
Database CASIA 1.0	AES is used for both encryption and decryption and some different tests are done to check the randomness of the key.	-	Iris for security improves	[52]
-	To create a distinct robust key using iris template.	-	Iris for Security Purpose	[53]
IIT Delhi Iris Database (Version 1.0)	A proposed algorithm can be used for hiding different types of data and to secure the iris template in data base by using visual cryptography.	MATLAB	Iris for Visual Cryptography	[56]
CASIA- database V3.0	Generation of iris template using cryptography and steganography. To address the issue of exploiting a biometric template hack or assault for malicious reasons.	MATLAB 2013A	Iris template generation	[57]
CASIA-IrisV3-Lamp database	A cancellable biometric cryptosystem utilizing iris recognition is designed to securely store patient healthcare data on a smart card. It uses symmetric key cryptography to encrypt this data before saving it in encrypted form on the smart card.	-	Iris to secure healthcare smart card	[60]

multiple user requests on a single server. Additionally, the data is securely stored using a data placement strategy, with authentication and access control managed through Crypto-Biometric Systems (CBS) in cloud computing, providing strong protection against unauthorized data access. Table 5 summarizes some published articles based on Iris.

Review on DNA

In the recent scenario, DNA cryptography utilizes DNA's encryptic features to address data security challenges. Due to their stability and variability, various segments of DNA are selected for encoding. This approach offers highly secure data storage and transmission solutions. This unique feature of DNA makes it a promising way to increase information security against cyber threats.

An enhanced key generation proposal based on the concepts of DNA was reported, with reformed encryption and decryption processes. The proposed methods were developed and examined, demonstrating their efficiency in computing, storage, and transmission. Throughout the decryption process, a noticeable increase in dynamism was observed [65]. This study builds upon prior suggested work

Table 6. Datasets during performance analysis

TESTS	.doc	.pdf	.zip	.txt	.gif	.jpeg
File size (kb)	370	524	210	89	2750	3930
Cipher text size (kb)	370	524	210	89	2750	3930
Encrypting time (sec)	7	9	4	3	44	62
Decrypting time (sec)	8	9	4	1	54	62

by incorporating techniques such as key creation, encryption, and decryption.

An algorithm proposed by Roy et al. based on DNA encoding genetic information in codons [66] or symmetric key encryption, along with transmitter and receiver side calculations, is efficiently introduced in this study. The reported key distribution systems presented in the literatures [67–70] are considered to address this issue. In this method, two-level keys are employed, with the first-level key used for converting plaintext to ciphertext, and the second level enhancing the security of the method. This approach proves resilient against brute force attacks due to the utilization of two levels of keys. Based on the datasets in Table 6, the result suggests that the cipher text size is nearly identical in all test situations. It demonstrates that decryption takes substantially less time than encryption. It can also be deduced that even if the file size grows significantly, the encryption and decryption times do not change dramatically.

DNA technology is found to be a source of biometric authentication. Biometrics based on deoxyribonucleic acid (DNA) may be the most precise method of identifying a person [71]. Every human being has their own unique map (blueprint) for every cell they create. Since DNA determines both the physical and mental attributes of humans, it is unlikely that anyone will possess the exact same collection of genes, except in the case of identical twins. Human DNA is shared in 99.7% of cases and 0.3% (1 million nucleotides [72]) are varying. Because this variability is inherited and is consequently particular to every individual. These changeable regions are known as Short Tandem Repeats (or STRs) that may be tested to differentiate one man or woman from another. Extracting, Amplifying, and Sequencing are the three main steps to crack the DNA code. In just a few hours, PCR has enabled the production of hundreds of millions of copies of a single DNA sequence. PCR is an enzyme process that replicates a particular section of DNA over and over again to produce multiple copies of a sequence. This molecular technique comprises heating and cooling samples for 30 cycles in a specific thermal cycling pattern. Every molecule bearing the target sequence receives a copy of the target DNA sequence throughout each cycle. In recent years, it has become possible to PCR amplify 16 STRs in one tube, including the 'amelogenin', gender assignment locus. DNA can be amplified in about 20 minutes using some commercially available devices, such as the Miniature Analytical Thermal Cycling Instrument (MATCI) and on-chip PCR. The suggested DNA cryptography method using XOR techniques is proven to be a user friendly and time saving approach towards network security. In these methods, plain text is chosen to be encrypted, after which a random key is generated. Also, a randomised codon list is generated, which is XORed with the random key. The encrypted message is created using the swap complement procedure. Biotechnology and DNA features are used to create the key. This approach is quick because of the XOR operation, and the time complexity is O (logN). However, space complexity may improve in the future [73].

A novel DNA cryptography approach was introduced, incorporating the XOR operation and the One-Time Pad for secure data transmission. This approach integrates an arithmetic operation or XOR operation, a One-Time Pad, and a DNA complementary rule, thus providing three layers of security [74]. This method is simple to use and secure against random OTP generation. OTPs are difficult for hackers to guess. Due to several prerequisites being used, this method is not that convenient, therefore, when choosing the OTP, care must be taken to consider the prerequisites.

A pseudo-biological DNA encryption approach was proposed, inspired by the central dogmas of biology. Unlike traditional DNA encryption, this method employs DNA idioms and techniques. Encryption and decryption are executed through transcription, splicing, and translation processes (Figure 13). These encryption steps significantly bolster security measures. Randomly generated keys are utilized to maximize confusion and diffusion, rendering decryption of encrypted text challenging. Robustness analysis is conducted to validate the method's resilience against attacks. This approach advocates the utilization of advanced Biocomputing systems [75].

In DNA-based cryptography, keys can be secured by using hamming code and a block cipher. The use of symmetric cryptography is important for optimizing DNA-based approaches. It compensates for the original algorithm's shortcoming of requiring a match between the length of the plaintext and the length of the secure key. This approach employs an improved matching mechanism with unexpected length to guarantee confusion of the ciphered result. The maximum length matching method has also

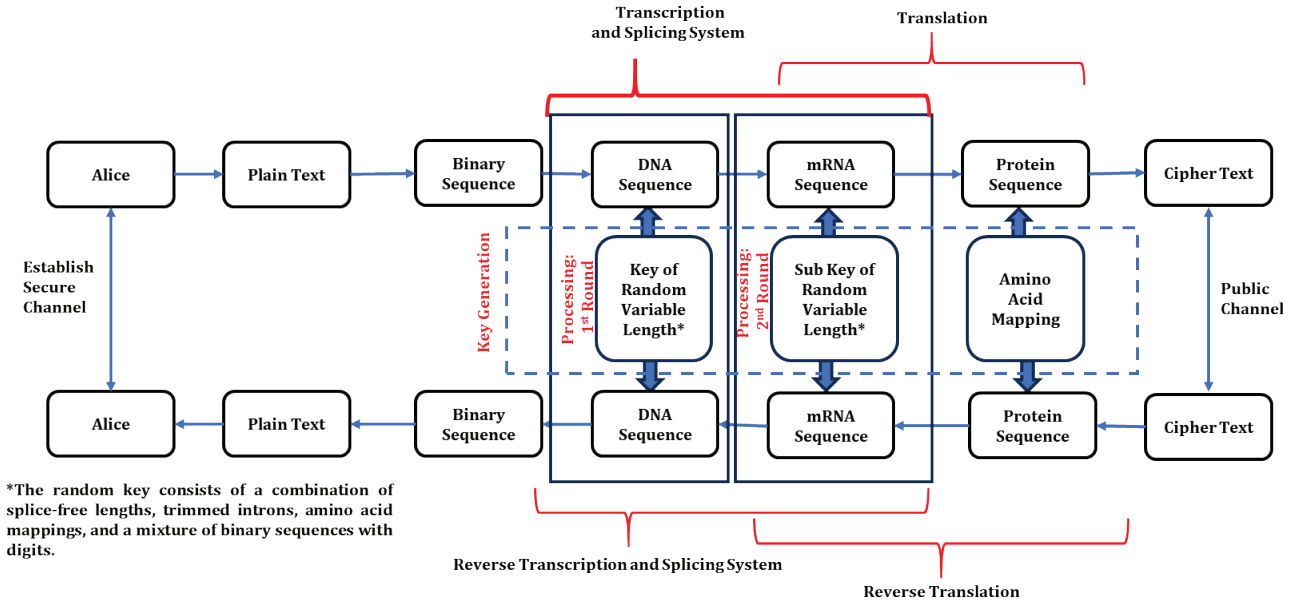

Figure 13. Biotic DNA-based cryptosystem proposed in [75] [Drawn by the author].

been developed in this technique to protect against various attacks. The length restriction of the secret key illustrated by DNA strands is eliminated by the proposed DNA-cryptographic method [76].

The approach of encrypting client-side data before saving in the cloud is an innovative technique based on cryptography methodology. This is a symmetric-key cryptography scheme based on DNA cryptography. The suggested system employs random dynamic encoding tables, resulting in increased security. The proposed method is CPA-secure, according to the security study. In addition to providing a comprehensive architecture of this methodology (Figure 14) and comparing it to current symmetric-key algorithms (DNA, DES, AES, and Blowfish), the experimental findings show that this method beats the earlier one in terms of cipher text size, encryption time, and throughput. As a result, this new technique is far more efficient and effective than the old one [77].

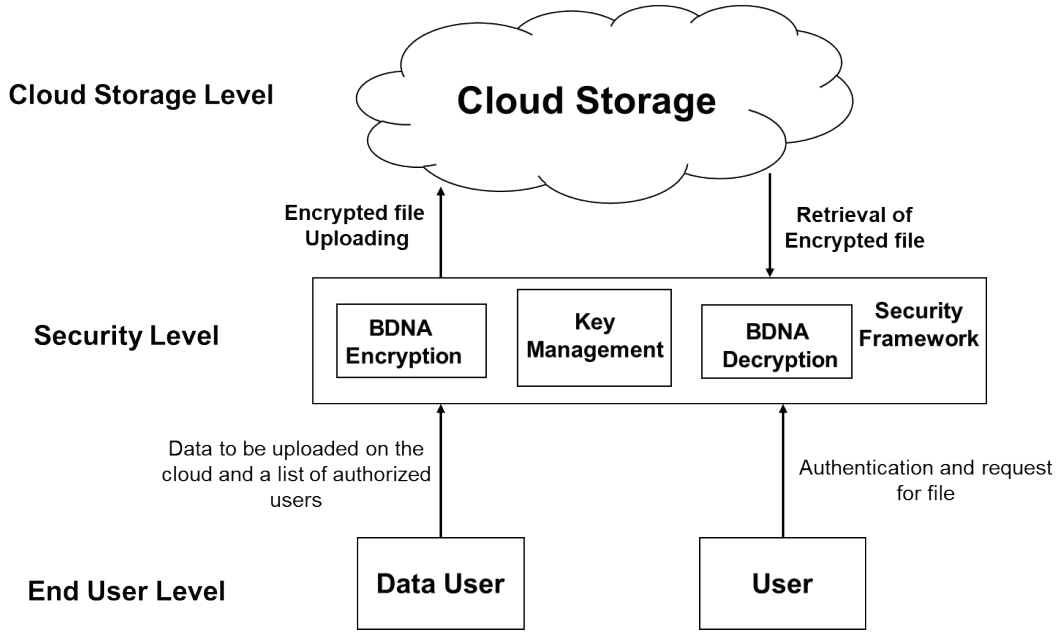

Figure 14. DNA-based methodology to secure cloud computing [From Sohal et al. [77], with permission from Springer].

The strategy for ECC assisted DNA mapping technique generates random DNA codes and the alphabets are assigned to non-repetitive subdivisions. The alphabets are then employed at both ends for encryption and decryption. Standard elliptical curve parameters and techniques were selected for the DNA elliptical cryptography. The robustness of elliptical cryptography against time and simple power analysis attacks (SPA) [77–80] has been validated by existing research. Without needing for a valid authentication key, elliptical cryptography randomly generates data after decoding. Finding the authentication key is the primary goal of attacks against cryptosystems. When useful information is discovered during decryption while utilizing a random key, these attacks are successful. The overall cryptosystem is much more secure from attacks if the encrypted data is itself encoded using a nonrepeating pattern. DNA mapping prior to encoding and DNA remapping after decoding is not a challenging computations according to the linear relation between time consumed and inputs in the described system. Due to the DNA mapping and remapping in the suggested approach, the energy usage is marginally higher compared to the other system. The current elliptical cryptography approach is made more secure by DNA mapping before encryption. This technique is appropriate for real-time IoT applications that have limited resources because of their low timing consumption and high CPU usage. This suggested strategy was tested in an IoT setting utilizing a Raspberry Pi3. According to the security study of the suggested scheme, the existing cryptosystems are far more resistant to SPA attacks and timings when used with the suggested DNA mapping. The referred technology has great capability in cloud-based implementations and mobile applications. The proposed solution holds many promises for future IoT technologies that demand a more compact but effective security framework. The suggested DNA mapping, encryption, decryption, and DNA remapping takes a linear amount of time in relation to the length of the input data. As a result, the suggested DNA mapping and remapping system (Figure 15) enhances the security of existing elliptical cryptosystems while consuming time [81].

Feature extraction is used to process the fingerprint template, and the features are then encrypted using the DNA cryptographic technique. For the second level of authentication, an XOR technique is used. The feature vector that matches the input feature vector throughout the decryption process is obtained and for the final output the user input image is recovered. There are certain concerns with the algorithms such as AES, DES, IDEA, they've chosen to implement. It is difficult to integrate AES with software. When using DES, the cost of execution rises. The IDEA method is a challenging decision due to the enormous number of weak keys, and management has become complicated. The optical fingerprint imaging technique is utilized here. For capturing fingerprint input, this operates similarly to a digital camera. This study uses a U. are. U 4500 sensor to capture a digital image of a fingerprint. The use of visible light is used to capture this specialized image. MATLAB software is used to process the fingerprints that have been obtained. The safety of the fundamental DNA codon usage is improved by the random generation of DNA sequences that are never used again. It is feasible to authenticate fingerprint templates effectively and safely by integrating DNA cryptographic techniques and a chaotic algorithm. The suggested technique encrypts human fingerprints and iris utilizing DNA characteristics and chaotic algorithms, ensuring that the template's privacy is preserved [82].

As the volume of digital data generated globally continues to grow exponentially, traditional storage mediums are reaching their limits in terms of capacity, durability, and efficiency. DNA storage meets a critical need for more efficient storage solutions with the ability to archive vast amounts of data in an extremely compact form. DNA storage technology represents a groundbreaking advancement in data storage, leveraging artificially synthesized deoxyribonucleic acid (DNA) as a medium for storing information.

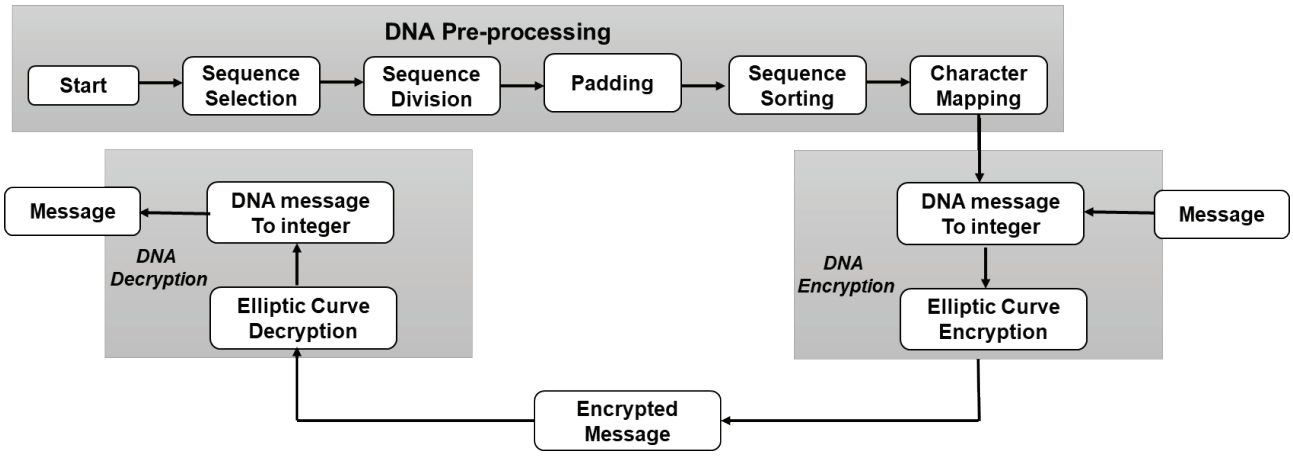

Figure 15. DNA-based elliptic curve cryptosystem for IoT devices.

This technology, characterized by its exceptionally high information density at the molecular scale, offers significant advantages such as enormous storage capacity, long-term durability, ease of access, and maintenance-free operation. Overcoming the current bottlenecks of cost and sequencing speed would propel DNA storage to the forefront of future information technologies, offering a sustainable and scalable solution to the world's growing data storage needs [83].

Encoding data in the hybridization states of DNA oligonucleotides, rather than relying solely on their sequence, has proven to be an advantageous approach for DNA information storage. This method allows for the creation of a metastable information solution that remains stable for long periods at room temperature but can be rapidly and permanently erased by brief heating. The authors demonstrated the effectiveness of this method using eight bitmap images of famous artwork, showing that after over two months of storage at 25 °C, more than 99% of the encoded pixels could be accurately restored, indicating a potential information half-life of at least 15 years. Importantly, the encoded information can be rapidly and permanently erased by heating the solution to 95 °C for just 5 minutes, which disrupts the truth marker pairing, rendering the data unrecoverable. Here bitmap artwork images are used to demonstrate the approach in a visually clear way. However, the method does not depend on long-range patterns within the data. The authors predicted that this approach will be particularly useful for compressed information files with high K-complexity. The approach not only enhances the potential of DNA as a storage medium but also addresses the challenge of securely erasing stored information, which traditional methods struggle to achieve without leaving traces [84].

Another study showed a secure storage scheme that integrates biometric authentication based on the user's genomic short tandem repeat (STR) profile which explore the potential of DNA as a digital data storage medium. The study further combines natural and synthetic DNA for secure data storage. The cryptographic keys of at least 80 bits of entropy is generated by using STR profiles, a form of personal genetic information. With the combination of AES-256 encryption and Reed-Solomon error correction, these keys enables secure and long-term storage of sensitive data in synthetic DNA. This main advantage of this method is that both the encryption key and the encrypted data are stored in the same DNA medium. The encrypted data can be read simultaneously using sequencing technology. This integration makes the decryption process simple and ensure that the encrypted data can only be deciphered with the correct STR marker data. The analysis confirms that STRs provide sufficient entropy to be used as cryptographic keys and thereby preventing brute-force attacks. The study experimentally generated an 80-bit strong key from human DNA and encrypted 17 kB of information in synthetic DNA. This data is then successfully decrypted which shows the efficacy of the methods in security applications [85].

The use of highly specific, stimuli-responsive DNA materials in DNA cryptography plays a crucial role in information encryption [86]. Leveraging their high information density, low maintenance cost, vast computational parallelism, and ease of synthesis, user-defined DNA materials have been developed for cryptographic applications, including encryption, authentication, and digital signatures [87,88]. DNA based tools are widely used in developing cryptographic methods and biosensors. However, conventional DNA based methods have typically used in controlling enthalpy, which provides unpredictable responses to stimuli and less accurate outcomes due to significant energy fluctuations. Programmable pH-responsive DNA motifs objectively overcome this problem by simultaneously controlling both enthalpy and entropy, which has proven to be an effective method for data storage. These advanced DNA motifs were successfully applied to glucose biosensing and crypto-steganography systems. This technique demonstrates their significant potential in both biosensing technologies and secure information encryption [89].

DNA data storage by combining bioinformatics with the Diffie–Hellman Key exchange method enhances data protection during communication. The study demonstrates a novel cryptosystem that leverages the entire Central Dogma of Molecular Biology (CDMB), encompassing the process by which DNA is translated into proteins (Figure 16).

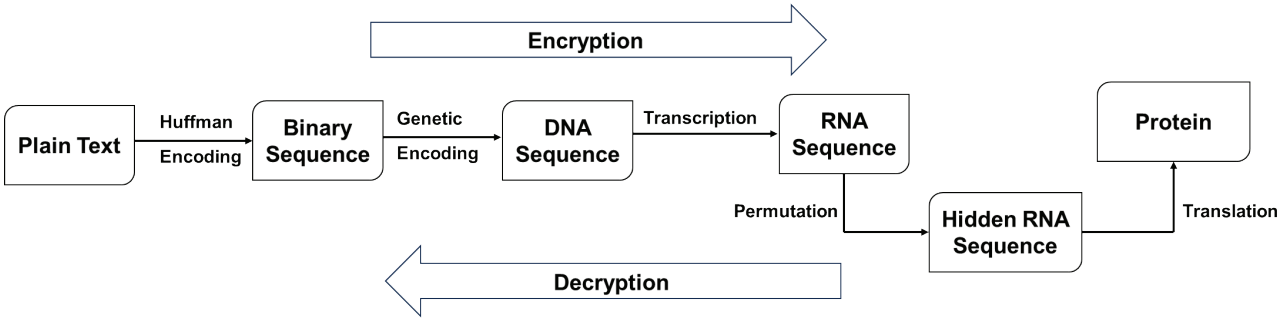

Figure 16. Schematic block diagram of encryption & decryption process of the methodology as reported in [90] [Drawn by the author].

Table 7. Significant contributions based on DNA

Biometric	Method	Processor	Advantage	Ref.
DNA	An enhanced key generation method is proposed using DNA synthesis principles, with improvements made to optimize the encryption and decryption processes.	JAVA	DNA for Enhanced key Generation	[66]
DNA	DNA as a source of biometric authentication	Miniature Analytical Thermal Cycling Instrument (MATCI) and on- chip PCR	DNA for Biometric Authentication	[71]
DNA	XOR encryption for providing DNA based encryption systems.	MATLAB	DNA for Enhancing Asymmetric Encryption	[73]
DNA	A cryptographic mechanism using secret keys derived from biotic DNA.	Pseudo–Biotic DNA cryptography method in C++ and conducted a series of experiments in a network simulator [NS2] to evaluate its effectiveness.	DNA for Adaptive Cryptographic Attacks	[75]
DNA	Study of existing DNA cryptography methods and then proposed a new pseudo-DNA	MATLAB	DNA for Secure Data Transfer.	[74]
DNA	A Hamming code combined with a block cipher mechanism to guarantee the secure transmission of a cryptographic key.	A simulation program, created in C language with VC6.0, has been developed for assessing the algorithm.	DNA for enforced secure key distribution	[76]
DNA	A novel cryptographic method has been proposed that utilizes client-side encryption to secure data before it is uploaded to the cloud. This technique features a multi-faceted symmetric-key encryption approach based on DNA cryptography.	MATLAB	DNA for secure cloud computing	[77]
DNA	A novel hybrid ECC scheme encoded with DNA that offers multiple levels of security.	C and Cortex-A8 running at 200 MHz.	DNA-Based Elliptic Curve Cryptography (ECC) for IoT Devices	[81]
DNA	A fingerprint template encryption scheme, leveraging DNA encoding and genetic algorithms, has been suggested to enhance the security of fingerprint templates.	MATLAB	DNA for Fingerprint Authentication	[82]

To generate key, this approach combines DNA cryptography with Diffie–Hellman Key exchange and includes additional modifications to strengthen the system. The proposed bio-inspired cryptosystem is designed to offer higher cryptographic efficiency and robustness even with large datasets, which provides effective protection against various online threats [90]

Table 7 summarizes a recently published article based on DNA.

PERFORMANCE ANALYSIS

This section offers a comparative analysis of existing Fingerprint, Iris and DNA based cryptographic models, summarizing their performance metrics, results, and effectiveness compared to existing methods.

Fingerprint-Based Cryptographic Model

A comparative analysis of existing fingerprint-based cryptographic models is summarized in Table 8.

Table 8. Performance analysis of existing fingerprint-based cryptographic models

Existing Models	Performance Metric	Performance/ Result Analysis	Comparison Analysis
A New Approach to Symmetric Key Generation Using Combination of Biometrics Key and Cryptographic Key to Enhance Security Of Data [20]	Storage, Security	Generation of 256-bit secret key by combining a 128-bit biometric key from fingerprint minutiae with a 128-bit system-generated key, enhancing security.	Cryptographic key generation process is unique, such key ensures the enhancement of the security and effectiveness.
An approach to cryptographic key distribution through fingerprint based key distribution center [21]	Hamming distance, Time for key generation	Time computed for feature extraction, cancelable template generation, key generation are 0.05 sec, 0.006 sec, 0.003 sec.	• The comparison shows impostors must guess at least half of the bits to break the key due to a 50% average Hamming distance. • Traditional cryptosystems face key sharing and privacy issues. The proposed KDC method addresses these by improving distribution and using biometric data to enhance security and simplify privacy.
Biometrics as a cryptographic method for network security [23]	Time for key generation	• Time calculated for Feature extraction of biometric template, template generation, template encoding and decoding, cryptographic key generation are 0.05 sec, 0.002 sec, 0.15 sec, 0.002 sec respectively • The amount of time needed for the entire process = 0.204 sec	Stronger and offers an improved level of security for methods of encryption and decryption through the employing of a pair of keys generated from fingerprint imprints.
Biometric Based Cryptography for Enhanced Security Mechanism [24]	FAR, FRR, GAR, EER	• The average matching percentage for genuine fingerprint pairs= 89.99%, • Range of Matching percentages= 81.37% to 99.83%, with a standard deviation of 0.043, showing that genuine pairs consistently have a high number of matchable bits for cryptographic keys. • The average Hamming distance is 49.94%, which means there is an average difference of 128 bits between genuine and imposter keys. • Hamming distances range from 37.89% to 61.72%, with a standard deviation of 0.031. Genuine keys differ by 40% to 60% of bits from 99.89% of imposter keys. Only 0.04% of imposter keys have unmatched bits below 40%. An imposter cannot match more than 128 bits out of a 256-bit cryptographic key.	• GAR for the FVC2002 database= 96.49% and GAR for the NIST special databases= 95.89%, indicating proposed method surpasses existing ones. • It effectively counters various attacks, including network, host, replay, and Man-in-the-Middle attacks. • This approach provides an effective solution to secure the session-based communication over unsecured channels.
Designing an Efficient Fingerprint Authentication Algorithm using SHA-512 and its Implementation [26]	Look-Up Table (LUT), Flip-Flop(FF), Clock Buffer Resources (BUFG)	• The reduction of LUT utilization from 63% to 33.07%, results in 47.62% improvement which indicates more efficient resource allocation. • FF utilization dropped from 36% to 13%, reflecting more efficient resource use and speeding up the hashing process, which is especially advantageous for time-sensitive applications. • Utilization rate of BUFG is 3.13% which demonstrates effective clock use. This promotes system reliability and synchronized operation.	• This system uses a secure binary representation and efficient feature extraction, and thereby improving the security and dependability of systems. • Methods like loop unrolling for SHA-512 minimizes the resource usage. This makes the system ideal for cost-effective and low-power standalone electronics.
Fingerprint Based Cryptographic Key Generation [35]	Hamming distance (HD)	• The maximum HD for a genuine case is 20 and the minimum HD is 4; The maximum HD for an impostor case is 81 and the minimum HD is 40. • Impostors cause more mismatches than natural variations in fingerprint images, indicating they cannot replicate an authentic key.	The distinct separation in Hamming distances between genuine and impostor keys demonstrates the effectiveness the proposed algorithm, as impostor-generated keys differ significantly from another fingerprint of the same person.
Finger print recognition based on biometric cryptosystem [37]	Euclidean Distance	• The Euclidean distance of the random image and Eigen space= 43.99. • Time complexity of the proposed method is $0(p^{3/2})$, which ensures the algorithm is efficient, rapid and reliable.	Compared to other approaches, this one is simple, trustworthy and fast.

Table 9. Comparative analysis of existing iris-based cryptographic model

Existing Models	Performance Metric	Performance/Result Analysis	Comparison Analysis
An effective authentication scheme for a secured IRIS recognition system based on a novel encoding technique [62]	Time Complexity, Execution Speed	• Time complexity of proposed iris recognition system (PIRS) is O(logn), leading to faster execution speeds compared to conventional systems. • The EER for PIRS is 0.44, which comparable to conventional Iris recognition system (CIRS).	• Compared to CIRS (having a time complexity of O(n)), PIRS delivers superior security. In addition, it reduces the vulnerability and provides better protection against common threats. • The EER of PIRS is stable and comparable to traditional systems. The system further offer similar accuracy along with improved security features.
Efficient private key generation from iris data for privacy and security applications [58]	Distinctiveness, dissimilarity, randomness, security analysis, segmentation accuracy.	• Key sizes of the system is of 333 to 1120 bits which makes the technique suitable for various cryptographic applications. • The iris key generation rate of the system is 95.50%. This makes the proposed scheme more efficient than other key generation methods in terms of GAR, FAR, and FRR. • Provides high uniqueness, strong inconsistency, passes random tests, resists attacks, supports dynamic and revocable keys, maintains a low mean error rate (MER) under various conditions.	This work outperforms traditional static methods, other biometric modalities like fingerprints, and other dynamic key generation approaches especially in noisy or diverse environments.
Generate and Evaluate Encryption Keys Obtained From Iris Biometric Data [59]	Randomness of generated keys (Chi-square test, ENT test, Block Metric, Gab Metric)	For a 64-bit random key (thresholds: GAB = 3.84, Block = 3.841), the Chi-square test shows the key is random, with entropy of 3.875 bits per byte, GAB and Block metric value 3.781125 and 22 respectively.	-
Iris based cancelable biometric cryptosystem for secure healthcare smart card [60]	False Acceptance Rate (FAR), False Rejection Rate (FRR)	FAR=0%, FRR= 7%, with the ability to generate a robust 252-bit encryption key, indicating high accuracy and security.	• Compare to [61][54], which yields a key length of 63 bits, with a FAR of 0% and an FRR of 63%, proposed model gives better FAR, FRR values. • Compared to traditional encryption methods, the proposed model enhances security by eliminating the need for secure key storage and significantly outperforms in terms of FAR and FRR, making it a superior choice for secure healthcare applications.
A safe and secured iris template using steganography and cryptography [57]	GAR, FAR	GAR=98.70%, FAR=0%	• The proposed approach improves other existing approaches in terms of GAR, FAR values. • Combining 3DES and Steganography enhances performance by improving revocability and distinguishing between genuine and imposter distributions, while reducing sensitivity to outliers compared to existing methods.
Iris image authentication using visual cryptograph [56]	Execution time	As the database size grows, execution time also increases, and conversely, a smaller database size reduces execution time.	Compared to existing methods, proposed visual cryptography method offers greater security by adding an extra layer of authenticity and a centralized user database.
Iris biometric cryptography for identity document [47]	FAR, FRR, EER, TSR	• (At threshold value=0.04 using Hamming Distance) FAR=0.02%, FRR=11%, EER=3.68%, TSR=89% • (At threshold value=0.04 using Euclidean Distance) FAR=20.5%, FRR=41.51%, EER=28.7%, TSR=56.41%	Comparing to Hamming distance, Euclidean distance is much weaker and not sufficient for the use of iris identification.

Table 10. Comparative analysis of existing DNA-based cryptographic model

Existing Models	Performance Metric	Performance Analysis / Result Analysis	Comparison Analysis
An improved Symmetric key cryptography with DNA based strong cipher [66]	Length of text size, Time.	• The ciphertext size nearly doubles in all test cases, making the process ideal to encrypt a huge file. • Decryption time is much shorter than encryption time, and both encryption and decryption times remain stable even with significantly larger file sizes.	Though this method is efficient and powerful against specific attacks, the partial information contained in the ciphertext makes the method more powerful.
Advancement In DNA As Source of Biometric Authentication [71]	Time	• Time required for extracting DNA= less than 30 seconds • Time required for amplifying DNA=approximately 20 minutes • Time required for sequencing DNA=less than 30 seconds	The high throughput microchips can provide outcomes up to 5 times faster than the existing machinery.
Enhancing Asymmetric Encryption using DNA Based Cryptography [73]	Speed, Time complexity	• The encryption speed of the XOR Cipher technique is extremely high. • A message can be encrypted in polynomial time (O (log n) time).	-
Pseudo DNA Cryptography Technique using OTP Key for Secure Data Transfer [74]	Computational complexity	Proposed algorithm ensures maximum security during data transfer while minimizing issues related to computational complexity.	Compared to traditional DNA-based cryptography algorithms, proposed pseudo-DNA cryptographic algorithm is much harder to crack due to the additional artificial features.
Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks [75]	Length of plaintexts and ciphertexts, Key length, Speed, Time, Storage	• Ciphertext length matches plaintext length and varies with key length. • It uses less storage space than plaintext, offering better storage efficiency. • With larger plaintext sizes, the random key length also increases, significantly minimizes the relative size of the key length. • The key and ciphertext transmit faster via safe and public channels, respectively, enhancing the storage and transmission efficiency of the method. • The adversary needs more chosen ciphertexts to obtain the key for a given plaintext, increasing the time required to recover it.	Proposed method is effective against chosen ciphertext and brute force attacks, and it also excels in computation, storage, and transmission efficiency than existing methods.
An optimized DNA based encryption scheme with enforced secure key distribution [76]	Length of the secure key	• Ciphertexts vary significantly because different secure keys are used for each encryption, showcasing the algorithm's effective diffusion property. • Matching positions are below 2%, and identical positions and lengths are under 1.5%, due to the algorithm's unpredictable matching length, satisfying the confusion theory.	The old DNA encryption technique achieves confusion theory but restricts its scope and applications. The proposed enhanced DNA computing, using block cipher symmetric cryptography, overcomes the original algorithm's need for matching plaintext and key lengths.
BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing [77]	Ciphertext size, Encryption time	• For plaintext size= 30 kb, ciphertext size= 35.0 • For plaintext size= 30 kb, encryption time= 0.149 • The throughput of BDNA is high.	• The proposed model encrypts plaintext more quickly than AES, DES, DNA, and Blowfish. • BDNA offers higher throughput in comparison to all other approaches. • The recommended approach generates smaller ciphertexts compared to existing encryption techniques.

Iris-Based Cryptographic Models

A summary of the comparative analysis of existing iris-based cryptographic models is provided in Table 9.

DNA-Based Cryptographic Model

A comparative analysis of existing DNA-based cryptographic models is furnished in Table 10.

CONCLUSION

In this paper, we presented recent research contributions in the field of Crypto-Biometrics specially in the areas of fingerprints, Iris, and DNA for cryptographic key generation, template protection. In comparison to conventional systems, the application of this kind of system, which combines biometrics and cryptographic methods, offers significantly greater confidentiality and security. This survey highlights significant advancements in fingerprint-based biometric cryptosystems, demonstrating their enhanced security capabilities through the integration of fingerprint features with cryptographic methods. By integrating biometric data with traditional Key Distribution Centers (KDCs), these systems achieve greater confidentiality and eliminate the need for key memorization. The development of cancelable biometric templates further improves security by transforming and shuffling minutiae to protect against unauthorized access. Performance metrics confirm the system's effectiveness in distinguishing genuine keys from impostor ones, while advanced cryptographic methods such as Secure Hash Algorithm (SHA-512) and Elliptic Curve Cryptography (ECC) contribute to enhanced efficiency and protection. Practical implementation, including mobile applications and encryption algorithms like Advanced Encryption Standard (AES) and Time-Based-One-Time-Password (TOTP), underscores the usability and effectiveness of these systems. The survey covers recent developments and innovations in iris recognition for generating secure key and thereby protecting the data. Methods such as 2-D Gabor filtering, fuzzy vault algorithms and error-correcting codes like Reed-Solomon and Hadamard codes have reported to be a promising approach to enhance the security of biometric cryptosystems. Numerous studies reported the advantage of using visual cryptography and phase correlation to improve security and mitigating potential threats. In Iris recognition, the superiority of Hamming distance over Euclidean distance has been emphasized through the comparison of different distance metrics and encryption algorithms. The combination of steganography, cancelable biometrics, and advanced data placement in cloud environment has made significant progress in this field. The DNA integration improves the security in cryptographic systems while provides a novel solutions for key generation, authentication, encryption and data storage. It is relatively a secure method for encoding data using XOR operations, one-time pads, and symmetric encryption. This methods adopts the stability and variability of DNA.

The current fingerprint-based biometric cryptosystems faces several limitations such as high false rejection rates, issues in practical implications and challenges in integrating fingerprint data with traditional cryptographic methods. System performances and efficiency is affected by the variability in fingerprint quality, computational overhead, and privacy concerns. The main challenges in iris-based cryptography are to maintain image consistence, reduce processing time and ensure key security. It is important to balance false acceptance and rejection rates to improve practical usability. Key length and randomness are the critical parameters. For instance, some methods produce shorter keys with attack vulnerabilities. Commercial implementation is only possible if the system demonstrates a user-friendly, cost-effective solution and ensures robustness against spoofing and attacks. DNA-based cryptography faces various concerns due to its high cost, low scalability and its high complexity. This is mainly due to slow processing and over-reliance on specialized equipment. The practical integration and efficiency is further restricted by several security concerns like vulnerabilities in key management and sequencing exposure along with its high power consumption. For broader adoption in practical, it is important to address these issues.

There is significant potential for several important areas of future research on biometric cryptography. Future work should explore various error correction techniques to increase accuracy in key generation processes. Handling instance-to-instance fluctuations in biometric data such as fingerprints is one of the potential areas that can be explored. In addition, integrating multi-parameter security techniques such as hybrid pairings of DNA with fingerprint or iris could significantly improve protection against highly secure attacks. The use of complex OTPs and consistent fine-point selection can improve the system security. Future works should also be focused on developing more efficient feature extraction methods for iris cryptosystems and the use of color visual cryptography for eye images. Furthermore, incorporating diverse distance metrics and segmentation methods could improve processing outcomes and efficiency. The scope of biometric cryptography can be broadened by exploring multimodal fusion of various biometrics to increase accuracy and key length, as well as optimizing memory usage and execution time across different smartcard types. Implementing advanced encryption techniques like AES and minimizing DNA space complexity present promising paths for future research, supporting the ongoing advancement and improved efficacy of biometric cryptography.

ACKNOWLEDGEMENTS

This research work is supported by Vellore Institute of Technology, Vellore, India.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence was not used in the preparation of the article.

REFERENCES

[1] Şolt N, Çalkavur S, Güzeltepe M. Secure encryption over the ring F2 + uF2 + vF2 + uvF2. Sigma J Eng Nat Sci 2024;42:529–533. [CrossRef]

[2] Jain AK, Nandakumar K, Nagar A. Fingerprint template protection: from theory to practice. In: Campisi P, editor. Security and Privacy in Biometrics. London: Springer; 2013. [CrossRef]

[3] Jain AK, Flynn P, Ross AA. Handbook of Biometrics. New York: Springer; 2007. 564 p. [CrossRef]

[4] Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 2007;29:561–572. [CrossRef]

[5] Boult TE, Scheirer WJ, Woodworth R. Revocable fingerprint biotokens: accuracy and security analysis. In: IEEE Conf Comput Vis Pattern Recognit 2007;1–8. [CrossRef]

[6] Kanade S, Petrovska-Delacretaz D, Dorizzi B. Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data. In: *IEEE Conf Comput Vis Pattern Recognit* 2009;120–127. [CrossRef]

[7] Kaur P, Kumar N, Singh M. Biometric cryptosystems: a comprehensive survey. Multimed Tools Appl 2023;82:16635–16690. [CrossRef]

[8] Sharma S, Saini A, Chaudhury S. A survey on biometric cryptosystems and their applications. Comput Secur 2023;134. [CrossRef]

[9] Hashem MI, Alibraheemi K. Literature survey: biometric cryptosystems based on fingerprint processing techniques. In: 2022 Int Conf Data Sci Intell Comput (ICDSIC) 2022;198–201. [CrossRef]

[10] Argyropoulos S, Tzovaras D, Ioannidis D, Strintzis MG. A channel coding approach for human. IEEE Trans Inf Forensics Secur 2009;4:428–440. [CrossRef]

[11] Monrose F, Reiter MK, Wetzel S. Password hardening based on keystroke dynamics. CCS '99: Proceedings of the 6th ACM conference on Computer and communications security. 1999.

[12] Davida GI, Frankel Y, Matt BJ. On enabling secure applications through off-line biometric identification. In: *1998 IEEE Symp Secur Priv (Cat No 98CB36186)* 1998;148–157. [CrossRef]

[13] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: *Advances in Cryptology – EUROCRYPT 2004*. Berlin: Springer; 2004. p. 523–540. [CrossRef]

[14] Hao F, Anderson R, Daugman J. Combining cryptography with biometrics effectively. Available at: https://www.cl.cam.ac.uk/techreports/ Accessed on Sep 01, 2025.

[15] Kanade S, Camara D, Krichen E, Petrovska-Delacretaz D, Dorizzi B. Three factor scheme for biometric-based cryptographic key regeneration using iris. In: 2008 Biometrics Symp 2008;59–64. [CrossRef]

[16] Jain AK, Ross AA, Nandakumar K. Introduction to Biometrics. New York Dordrecht Heidelberg London: Springer; 2011. [CrossRef]

[17] Seals T. ThreatList: a third of biometric systems targeted by malware in Q3. Threat Post. Available at: https://threatpost.com/threatlist-a-third-of-biometric-systems-targeted-by-malware-in-q3/150778/ Accessed on Sep 01, 2025.

[18] Sur A. India saw 18 million cyber attacks in first quarter of 2022: Google's Royal Hansen. Available at: https://www.moneycontrol.com/europe/?url=https://www.moneycontrol.com/news/business/india-saw-18-million-cyber-attacks-in-first-quarter-of-2022-google-executive-royal-hansen-9084911.html Accessed on Sep 01, 2025.

[19] Mascellino A. Japan government websites hit by cyber-attacks, Killnet suspected. Whats Hot On. Available at: https://www.infosecurity-magazine.com/news/japan-govt-websites-killnet/ Accessed on Sep 01, 2025.

[20] Solanki KH, Sahayak A. A new approach to symmetric key generation using combination of biometrics key and cryptographic key to enhance security of data. Int J Eng Res Technol 2013;2:1-7.

[21] Barman S, Chattopadhyay S, Samanta D. An approach to cryptographic key distribution through fingerprint based key distribution center. In: 2014 Int Conf Adv Comput Commun Informatics (ICACCI) 2014;1629–1635. [CrossRef]

[22] Balakumar P, Venkatesan R. Secure biometric key generation scheme for cryptography using combined biometric features of fingerprint and iris. Int J Comput Sci 2011;8:349–356.

[23] Ankit K, Rekha J. Biometrics as a cryptographic method for network security. Indian J Sci Technol 2016;9. [CrossRef]
[24] Prasanthi KS, Krishna HV, Saranya S. Biometric based cryptography for enhanced security mechanism. Int J Pure Appl Math 2017;117:779–787.
[25] Tulyakov S, Farooq F, Mansukhani P, Govindaraju V. Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognit Lett 2007;28:2427–2436. [CrossRef]
[26] Gupta A, Banakar N, Chetan NK, Aryan M, Purushotham U. Design and implementation of an efficient fingerprint authentication algorithm using SHA-512. In: 2024 Third Int Conf Distrib Comput Electr Circuits Electron (ICDCECE) 2024;1–7. [CrossRef]
[27] Dwivedi R, Dey S, Sharma MA, Goel A. A fingerprint based crypto-biometric system for secure communication. J Ambient Intell Humaniz Comput 2020;11:1495–1509. [CrossRef]
[28] Gowda VD, Gite P, Rahman M, Kadam KR, Manivasagam G, Prasad KDV. Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography. J Discrete Math Sci Cryptogr 2024;27:477–488. [CrossRef]
[29] Gowda VD, Prasad K, Shekhar R, Srinivas R, Srinivas KNV, Lakineni PK. Development of a real-time location monitoring app with emergency alert features for Android devices. In: 2023 4th IEEE Glob Conf Adv Technol 2023;1–8. [CrossRef]
[30] Gowda VD, Sharma A, Kumaraswamy S, Sarma P, Hussain N, Dixit SK, et al. A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm. J Interdiscip Math 2023;26:519–530. [CrossRef]
[31] Gowda VD, Prasad KDV, Gite P, Premkumar S, Hussain N, Chinamuttevi VS. A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks. J Discrete Math Sci Cryptogr 2023;26:861–873. [CrossRef]
[32] Gowda VD, Kumar PSVVS, Latha J, Selvakumar C, Shekhar R, Chaturvedi A. Securing networked image transmission using public-key cryptography and identity authentication. J Discrete Math Sci Cryptogr 2023;26:779–791. [CrossRef]
[33] Gowda VD, Sharma A, Raghavendra K, Nagabushanam M, Reddy HGG. Vector space modelling-based intelligent binary image encryption for secure communication. J Discrete Math Sci Cryptogr 2022;25:1157–1171. [CrossRef]
[34] Pawar P, Datar S, Ranade N, Thorat K, Gharu AN. Biometric security using cryptography for insurance data retrieval with additional OTP generation and verification. Int J Innov Res Technol 2019;5.
[35] Suresh K, Pal R, Balasundaram SR. Fingerprint based cryptographic key generation. In: *Intelligent Data Communication Technologies and Internet of Things*. Cham: Springer International Publishing; 2020. p. 704–713. [CrossRef]
[36] Salamon WJ, Ko K. Fingerprint Minutiae Viewer (FpMV). Available at: https://www.nist.gov/services-resources/software/fingerprint-minutiae-viewer-fpmv Accessed on Sep 01, 2025.
[37] Jalaja V, Gsgn A, Mohan LN. Finger print recognition based on biometric cryptosystem. J Integr Sci Technol 2024;763. [CrossRef]
[38] Oduguwa T, Arabo A. Passwordless authentication using a combination of cryptography, steganography, and biometrics. J Cybersecur Privacy 2024;4:278–297. [CrossRef]
[39] Murugan A, Savithiri G. Feature extraction on half iris for personal identification. In: 2010 Int Conf Signal Image Process 2010;197–200. [CrossRef]
[40] Wu X, Qi N, Wang K, Zhang D. A novel cryptosystem based on iris key generation. In: Proc 4th Int Conf Nat Comput (ICNC 2008) 2008;53–56. [CrossRef]
[41] Nagar A, Chaudhury S. Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme. In: 18th Int Conf Pattern Recognit (ICPR'06) 2006;537–540. [CrossRef]
[42] Juels A, Sudan M. A fuzzy vault scheme. Des Codes Cryptogr 2006;38:237–257. [CrossRef]
[43] Wu X, Qi N, Wang K, Zhang D. An iris cryptosystem for information security. In: 2008 Int Conf Intell Inf Hiding Multimed Signal Process 2008;1533–1536. [CrossRef]
[44] Davida G, Frankel Y, Matt B, Peralta RE. On the relation of error correction and cryptography to an off line biometric based identification scheme. In: Proc WCC99 Workshop Coding Cryptogr 1999;129–138.
[45] Daugman J. High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Pattern Anal Mach Intell 1993;15. [CrossRef]
[46] Service note on CASIA iris image databases. 2012. Available at: https://www.yumpu.com/en/document/view/3796486/service-note-on-casia-iris-image-databases Accesed on Sep 01, 2025.
[47] Moi SH, Rahim NBA, Saad P, Sim PL, Zakaria Z, Ibrahim S. Iris biometric cryptography for identity document. In: 2009 Int Conf Soft Comput Pattern Recognit 2009;736–741. [CrossRef]
[48] Nithyanandam S, Gayathri KS. A new IRIS normalization process for recognition system with cryptographic techniques. Int J Comput Sci 2011;8:342–348.
[49] Hajare N, Borage A, Kamble N, Shinde S. Biometric template security using visual cryptography. J Eng Res Appl 2013;3:1320–1323.
[50] Ehuil BB, Chen C, Wang S, Guo H, Liu J. A secure mutual authentication protocol based on visual cryptography technique for IoT-cloud. Chin J Electron 2024;33:43–57. [CrossRef]

[51] Kezheng L, Bo F, Hong Z. Visual cryptographic scheme with high image quality. In: 2008 Int Conf Comput Intell Secur 2008;366–370. [CrossRef]
[52] Asok SB, Karthigaikumar P, Mangai S. Iris based cryptography. Int J Adv Res Comput Commun Eng 2013;2:1310–1313.
[53] Ajith S, Balaji Ganesh Kumar M, Latha S, Samiappan D, Muthu P. Iris cryptography for security purpose. J Phys Conf Ser 2018;1000:012111. [CrossRef]
[54] Pawar A, Kumbhare T, Murkute P, Kallapur S. Enhancing iris scanning using visual cryptography. IOSR J Comput Eng 2015;17:54–57.
[55] Zhang H, Wang X, Cao W, Huang Y. Visual cryptography for general access structure by multi-pixel encoding with variable block size. In: Proc 2008 Int Symp Knowl Acquis Model (KAM) 2008;340–344. [CrossRef]
[56] Udayini V, Bindu CH, Malleswari PN. Iris image authentication using visual cryptograph. Int J Recent Technol Eng 2019;8:288–291.
[57] Abikoye OC, Ojo UA, Awotunde JB, Ogundokun RO. A safe and secured iris template using steganography and cryptography. Multimed Tools Appl 2020;79:23483–23506. [CrossRef]
[58] Dash P, Pandey F, Sarma M, Samanta D. Efficient private key generation from iris data for privacy and security applications. J Inf Secur Appl 2023;75. [CrossRef]
[59] Abdulraheem AA, Hasso SA. Generate and evaluate encryption keys obtained from iris biometric data. In: 21st Int Multi-Conf Syst Signals Devices (SSD 2024). IEEE; 2024. p. 321–328. [CrossRef]
[60] Kausar F. Iris based cancelable biometric cryptosystem for secure healthcare smart card. Egypt Inform J 2021;22:447–453. [CrossRef]
[61] Yang W, Wang S, Hu J, Zheng G, Chaudhry J, Adi E, Valli C. Securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. IEEE Access 2018;6:36939–36947. [CrossRef]
[62] Harikrishnan D, Sunilkumar N, Shelby J, Kishor N, Remya G. An effective authentication scheme for a secured iris recognition system based on a novel encoding technique. Meas Sens 2022;25. [CrossRef]
[63] Shaleen. A study on integrated crypto-biometric system to protect the unauthorized access of data. J Interdiscip Multidiscip Res 2024;19:593–610.
[64] Prabu S, Ganapathy G. Secured data storage in public cloud environment through crypto-biometric system. Int J Comput Sci Eng Technol 2017;7:10–14.
[65] Roy B, Rakshit G, Chakraborty R. Enhanced key generation scheme based cryptography with DNA logic. Comput Sci 2011. Prepint. https://api.semanticscholar.org/CorpusID:18906078
[66] Roy B, Rakshit G, Singha P, Majumder A, Datta D. An improved symmetric key cryptography with DNA based strong cipher. In: Int Conf Devices Commun (ICDeCom-2011) 2011;1–5. [CrossRef]
[67] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proc 9th ACM Conf Comput Commun Secur 2002;41–47. [CrossRef]
[68] Zhu S, Xu S, Setia S, Jajodia S. Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach. In: 11th IEEE Int Conf Netw Protocols 2003;326–335.
[69] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks. ACM Trans Inf Syst Secur 2005;8:41–77. [CrossRef]
[70] Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. A pairwise key predistribution scheme for wireless sensor networks. ACM Trans Inf Syst Secur 2005;8:228–258. [CrossRef]
[71] Qaseem IAQM, Asif SAW, Armeen ZF. Advancement in DNA as source of biometric authentication. Int J Eng Res Technol 2013;2:1–8.
[72] Delibaş E, Arslan A. A new feature vector model for alignment-free DNA sequence similarity analysis. Sigma J Eng Nat Sci 2022;40:610–619. [CrossRef]
[73] Rani M, Jain S. Enhancing asymmetric encryption using DNA based cryptography. Int J Comput Sci Trends Technol 2014;2:7–11.
[74] Kalyani S, Gulati N. Pseudo DNA cryptography technique using OTP key for secure data transfer. Int J Eng Sci Comput 2016;5657.
[75] Suresh Babu E, Naga Raju C, Munaga HM, Prasad K. Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks. Int J Netw Secur 2016;18:291–303.
[76] Zhang Y, Liu X, Ma Y, Cheng LC. An optimized DNA based encryption scheme with enforced secure key distribution. Cluster Comput 2017;20:3119–3130. [CrossRef]
[77] Sohal M, Sharma S. BDNA—a DNA inspired symmetric key cryptographic technique to secure cloud computing. J King Saud Univ Comput Inf Sci 2022;34:1417–1425. [CrossRef]
[78] Odelu V, Das AK, Choo KKR, Kumar N, Park Y. Efficient and secure time-key based single sign-on authentication for mobile devices. IEEE Access 2017;5:27707–27721. [CrossRef]
[79] Cheng C, Lu R, Petzoldt A, Takagi T. Securing the Internet of Things in a quantum world. IEEE Commun Mag 2017;55:116–120. [CrossRef]
[80] Reddy AG, Yoon EJ, Das AK, Odelu V, Yoo KY. Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment. IEEE Access 2017;5:3622–3639. [CrossRef]
[81] Tiwari HD, Kim JH. Novel method for DNA-based elliptic curve cryptography for IoT devices. ETRI J 2018;40:396–409. [CrossRef]
[82] Vijayakumar S, Jansi M, Lavanya D, Lavanya Sree V. Delay efficient genetic algorithm with DNA based cryptography for fingerprint authentication. Eur J Mol Clin Med 2020;7:2077–2080.

[83] Zhang Z, Zhang Z. DNA information storage and cryptography system. Acad J Sci Technol 2024;10:243–249. [CrossRef]

[84] Kim J, Bae JH, Baym M, Zhang DY. Metastable hybridization-based DNA information storage to allow rapid and permanent erasure. Nat Commun 2020;11. [CrossRef]

[85] Grass RN, Heckel R, Dessimoz C, Stark WJ. Genomic encryption of digital data stored in synthetic DNA. Angew Chem Int Ed Engl 2020;59:8476–8480. [CrossRef]

[86] Zhang C, Ma X, Zheng X, Ke Y, Chen K, Liu D, et al. Programmable allosteric DNA regulations for molecular networks and nanomachines. Sci Adv 2022;8. [CrossRef]

[87] Zhang Y, Wang F, Chao J, Xie M, Liu H, Pan M, et al. DNA origami cryptography for secure communication. Nat Commun 2019;10. [CrossRef]

[88] Fan HJ, Li J, Wang LH, Fan CH, Liu HJ. Constructions of iron atoms arrays based on DNA origami templates for cryptography applications. Wuli Xuebao Acta Phys Sin 2021;70. [CrossRef]

[89] Zheng LL, Li JZ, Wen M, Xi D, Zhu Y, Wei Q, et al. Enthalpy and entropy synergistic regulation-based programmable DNA motifs for biosensing and information encryption. Sci Adv 2023;9. [CrossRef]

[90] Vaishali R, Naik SM. A DNA cryptosystem using Diffie–Hellman key exchange. SN Comput Sci 2024;5. [CrossRef]