Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp**. 90–103
DOI: https://doi.org/10.58496/MJCS/2025/007; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Encrypting Text Messages via Iris Recognition and Gaze Tracking Technology

Sura Abed Sarab Hussien [1*], Basim Najim Al-din Abed [2], Kamaran Adil Ibrahim [3]

[1]*Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.*
[2]*Department of Computer Science, College of Science, University of Diyala, Diyala, Iraq.*
[3]*Department of Arabic language, College of Education, University of Tikrit, Tuzkhurmatu, Iraq.*

ARTICLEINFO

Article history
Received 20 Oct 2024
Accepted 12 Jan 2025
Published 05 Feb 2025

Keywords
Iris Recognition
Gaze Tracking
Dynamic Encryption
Cryptographic Key
Message Encryption

ABSTRACT

This study explores the integration of eye-tracking technology, specifically the gaze point (GP3) eye tracker, to develop a novel encryption and decryption model that leverages an individual's unique eye patterns as a cryptographic key. This research addresses the critical problem of balancing user-friendly encryption mechanisms with robust security. This study aims to design a gaze-based encryption system that uses the eye's binary matrix as a dynamic encryption key. The methodology involves capturing an eye image, converting it into a binary matrix, and using the extracted matrix to generate a unique iris key (IK) applied to encrypt and decrypt text messages on the basis of gaze interaction. This study evaluates the proposed approach against metrics such as encryption and decryption time, key entropy, and resilience to cryptanalysis. The results demonstrate that the system achieves high levels of security, with the iris key offering sufficient randomness and robustness against brute-force attacks. The gaze-based mechanism reveals hidden text when the user interacts with specific characters, enhancing privacy. The proposed model integrates biometric authentication with real-time encryption, setting a foundation for future applications in secure communication systems. The proposed model provides safe, user-centric encryption and addresses key management challenges while harnessing the potential of gaze-based interaction.

1. INTRODUCTION

In the modern era, with digital communication dominating everyday life, sensitive information security has become a key concern. The continuous sophistication of cyberattacks and the inability of traditional cryptographic systems have driven the need for innovation in encryption methods. [1] Besides, the generation of random cipher keys is considered to be a main principle of protection in cryptography and information security science: confidentiality, integrity, and availability. Most cryptographic algorithms depend particularly on PRNG sequences for cipher keys, many of which are in use in cryptography and digital communications today. [2] Biometric technologies, such as eye-tracking systems, present new opportunities for the use of human physiological traits in the development of secure communication systems. Of these, the iris pattern is one of the most reliable and unique biometric identifiers, hence motivating its use in cryptographic key generation. [3] While promising, leveraging biometrics for encryption also presents several challenges. Traditional approaches often have difficulty finding a good balance between usability, computational efficiency, and robustness against cryptanalysis. In addition, for any real-time user interaction, in this case, gaze-based input within cryptographic systems requires new approaches that do not diminish either security or performance. These challenges indicate that the solution space should aim at effectively harnessing biometric uniqueness while being practical and adaptable for a wide range of applications.

This work aims to contribute, by facing such challenges through a gaze-based encryption model and its reverse process, as well; an individual would use an eye-print-a cryptographic key. The design integrates real-time interaction based on the gaze point GP3 eye tracker, which interacts with the eye image to capture the eye and produce a binary matrix that helps derive the base for an iris key. Unlike traditional methods, the proposed system integrates biometric uniqueness with dynamic, user-controlled encryption to provide better security and usability.
In this regard, the research is targeted at three objectives: first, to develop a practical model exploiting eye patterns for cryptographic key applications; second, to study the security, efficiency, and robustness of the system against cryptanalysis attacks; and third, to show that gaze-based encryption is both usable and feasible in a real-world scenario. With these stated

*Corresponding author. Email: Sura.a@sc.uobaghdad.edu.iq

objectives, the present research makes a valuable contribution toward understanding how effectively biometric characteristics can be deployed in various cryptographic protocols.

Although the proposed gaze-based encryption and decryption system introduced in this paper is original and practical, several limitations are connected with the study: The test with real-world data was limited since one controlled dataset cannot fully express the diversity and complexity that would be present in real applications. Hardware dependency for eye tracking relies on specialized hardware—the so-called eye-tracking device. An example is Gaze point GP3; because of this, any people without access to it cannot use this module. The impact of this work extends beyond the context of secure communication. The proposed model integrates biometric authentication with encryption, thus opening a route toward user-friendly and personalized security solutions. This research not only highlights the potential of gaze-based cryptography but also lays a foundation for future innovations in secure, human-centered communication systems.

2. LITERATUREREVIEW

In recent years, there has been much interest in the convergence of secure communications and biometric authentication. Emphasizing recent developments, this literature review looks at the current state of biometric encryption and gaze-tracking technologies and how they can be used to secure digital communications.

Yousef et al. presented an advanced lightweight cryptographic mechanism that aims to make the flow of different kinds of multimedia and real-time information within the IoT network secure via two S-boxes within the sub byte transformation in the process of encryption without compromising its efficiency. Testing of this newly proposed algorithm's effectiveness should be performed through several samples of auditory materials. Extensive comparative studies of the proposed technique against the most sophisticated standard algorithms revealed a significant reduction in the execution time of the cryptographic process and energy consumption while still preserving the required level of security. Good performance in terms of both power consumption and latency is manifested. In this novel technique, nearly 0.2 µJ was consumed during the encryption process. [4]. Aljawarneh. et al. proposed and implemented a lightweight, flexible encryption framework that incorporates robust yet simple substitution and transposition techniques that can be used for data encryption and decryption, hence addressing the constrained processing capabilities of IoT devices. We have adopted a variable block size approach to improve the adaptability of the proposed system for deployment in many IoT devices with diversely bounded memory. In this work, DNA sequences generate stochastic encryption keys. Therefore, the system shows high resistance against all types of malicious breaches. The empirical results of the lightweight encryption mechanism presented are promising for deployment on various IoT devices, mainly concerning memory utilization and encryption duration, compared with state-of-the-art cryptographic frameworks. [5] Holmqvist et al. (2011) described how to evaluate and acquire an eye tracker, how to plan and design an eye-tracking study, and how to record and analyse eye-movement data. Additionally, how raw data samples are converted into fixations and saccades via event detection algorithms; how the different representations of eye movement data are calculated via AOIs, heatmap and scan paths; and how all the measures of eye movements are related to these processes are explored. proposed in this study that it has exceptional accuracy and real-time performance when it uses modern gaze tracking systems [6]. Rathgeb et al. (2014) discussed the potential use of biometric data-embedded cryptographic keys and explored the potential use of biometric objects as cryptographic keys in their paper on biometric cryptosystems. The proposal of features such as biometric encryption and interceptable biometrics emphasized the importance of protecting biometric data [7]. George et al. (2016) This method incorporates geometrical characteristics of the eye. In the beginning of the method a fast convolutional manner is used to get the coarse site of the IC. The IC positioning is duplicated in the following stage using limits tracking and ellipse suitable using tracking techniques. The method has been evaluated in general databases like BioID and Gi4E and found to outshine state-of-the-art techniques [8]. Duchowski et al. (2017) focus on video-based, corneal-reflection eye trackers—the most widely available and affordable type of system—and add a look at a few interesting and challenging applications in terms of human factors, collaborative systems, virtual reality, marketing, and advertising. provided a detailed overview of eye-tracking techniques and applications. There has been a tremendous increase in the use of eye-tracking technologies, with applications ranging from clinical diagnostics to user interface design [9]. Li et al. (2018) studied iris feature encryption technology using iris features as the research object and the deep learning method as the feature classification method. The shared iris database is used to conduct the simulation experiment. The findings demonstrate that the technique can significantly increase the security of the encryption and decryption process as well as the consistency of iris encryption [10]. Mehrubeoglu et al. (2018) presented a real-time application for gaze-based PIN entry and eye detection and tracking for PIN identification via a smart camera. A common method for user authentication and security is the use of personal identification numbers. PIN-based password authentication requires users to enter the PIN by hand, making it susceptible to password-cracking techniques such as thermal monitoring or shoulder surfing. On the other hand, PIN authentication using hands-off gaze-based PIN entry techniques offers a more secure password entry option because it leaves no physical traces behind. Gaze-based authentication is the process of tracking the center of the eye over time and locating the eye in successive image frames

[11]. Qi et al. (2019) implemented linear discriminant analysis (LDA) and an extreme learning machine (ELM) in a hand gesture recognition system, which can reduce the redundant information in sEMG signals and improve recognition efficiency and accuracy. The characteristic map slope (CMS) is extracted via the feature extraction method because the CMS can strengthen the relationship of features across the time domain and increase the feasibility of cross-time identification. This study focuses on optimizing the time differences in sEMG pattern recognition, and the experimental results are beneficial for reducing the time differences in gesture recognition based on sEMG. The proposed recognition framework can enhance the generalization ability of HCI in long-term use, and it also simplifies the data collection stage before training the device to be ready for daily use, which is highly important for improving the time generalization performance of an HCI system [12]. Pai et al. (2019) described the computer workstation Erica, which has a distinctive user interface. The imaging gear and software on the workstation automatically capture a digital image of the user's eye. The interface determines the approximate location of the user's visual acuity on the computer screen on the basis of the attributes of the current portrait. Next, commands related to the menu item that is presently shown at this screen position are carried out by the computer. By merely glancing at the proper order of menu selections presented on the screen, the user can thereby operate peripheral devices, start applications, and interact with the computer. Eye–gaze interface technology is explained, along with how Erica uses it and how it can be used as a prosthetic [13]. Mahmud et al. (2020) examine the benefits and drawbacks of the modern cutting-edge technology created for this purpose. In this review, an outline is created for future research in the areas of human–computer interaction, human–machine interaction, and human–robot interaction. This paper provides a wide overview of the current situation and speculates on potential future developments in the field of human–machine interactions [14]. Rakhmatulin et al. (2020) presented a hands-on demonstration of the most widely used gaze-tracking techniques. A review is conducted on the many types of deep neural networks that can be applied to online gaze tracking. They provide a novel eye-tracking technique in which the use of a deep learning technique is noticeably more effective. Python is used for implementing and managing computer interactions to demonstrate how to use it. A dual coordinate system is provided so that a glance can be used to control the computer. Using the OpenCV library, color detection from the infrared LED is used to obtain the first set of coordinates, which represents the face's position concerning the computer. The YOLO (v3) package is used to acquire the second set of coordinates, which indicates the gaze position. Three objects are used to track gaze in this method of labelling the eyes (to the left, to the right, and in the center) [15]. Chen et al. (2022) created a real-time, multimodel HRC system using speech and gestures. A collection of sixteen dynamic gestures is intended to facilitate communication between industrial robots and humans. We are creating and developing a dataset of dynamic gestures that we will make available to the community. A convolutional neural network is designed to identify dynamic gestures in real time by using deep learning techniques and motion history images. For real-time voice recognition by a human worker, an enhanced open-source speech recognizer is employed. A software interface is built for system visualization, and an integration method is provided to incorporate the findings of speech and gesture recognition [16][19]. Panel et al. (2023) provide a method for implementing real-time HCI systems via eye gaze. The method makes eye moment records and tracks them through the Dlib 68-point landmark detector and then constructs a model of eye gaze recognition that recognizes four kinds of eye gazes. The application of eye contact in a live human–computer interaction setu+-p is proposed. By employing the Dlib 68-point landmark detector, researchers initially captured and followed eye motions to develop an eye contact recognition framework capable of distinguishing between four distinct types of eye gazes. Then, an instance-segmentation model can be developed using a mask area-based convolutional neural network (R-CNN) method for detecting and classifying devices and objects. Next, creating an HCI software interface can include proposed eye tracking and pattern-classification models [17][23].

Despite the significant contributions of these studies, several gaps and limitations remain. Many studies focus on enhancing nonlinearity but lack comprehensive approaches that simultaneously address differential uniformity, which is essential for robust cryptographic security.

Additionally, the high computational complexity of some proposed methods limits their practicality for deployment in resource-constrained environments. Moreover, there is a need for more empirical studies validating the efficiency and scalability of gaze-tracking algorithms in real-world cryptographic applications. Few studies provide detailed frameworks for integrating gaze-tracking algorithms with existing cryptographic systems, which is crucial for practical adoption. To provide a clearer and more organized presentation of the research landscape. Table 1 below summarizes the key details of these studies.

TABLE I. SUMMARY OF KEY STUDIES ON ULTRA-LIGHTWEIGHT S-BOX GENERATION VIA QUANTUM INSPIRATION.

Study	Method	Key Contributions	Limitations
[4]	lightweight cryptographic methodology	safeguarding diverse multimedia and real-time data flows within (IoT) network, commendable performance concerning power consumption and latency.	Lack of practical implementation framework
[5]	versatile and lightweight encryption framework, using Deoxyribonucleic Acid (DNA) sequences.	catering to the constrained processing capabilities inherent in Internet of Things (IoT) devices.	Lack of empirical analysis on efficiency and scalability
[6]	Event detection algorithms, AOIs, heatmap, and scan paths.	Exceptional accuracy and real-time performance by modern gaze tracking systems	High computational requirements
[7]	The biometric objects as cryptographic keys	Protecting the biometric data	High computational complexity
[8]	Geometrical characteristics of the eye and Convolution-based approach	Confirm the presence of other hidden users	Lack of practical implementation framework
[9]	Video-based, corneal-reflection eye trackers eye tracking technologies	Overview of eye-tracking techniques and applications	Lack of empirical analysis on efficiency and scalability
[10]	Iris features encryption technology and the deep learning method	improve the encryption and decryption safety process of iris encryption	Challenges in maintaining consistent security
[11]	The application of smart camera, eye detection.	More secure password entry option	Susceptible to password cracking techniques like thermal monitoring or shoulder surfing. On the other hand.
[12]	Hand gesture recognition system and intelligent HCI scheme	Enhance the time generalization functioning of an HCI system and accurate gesture detection in HCI	Lack of practical implementation framework
[13]	The eye-gaze interface technology and computer workstation Erica,	Improvement of eye-gaze interface technology and how Erica can be used as a prosthetic	Lack of empirical analysis on efficiency and scalability
[14]	Human-computer interaction and cutting-edge modern technology	Speculates on potential future developments in the field of human-machine interactions	Lack of practical implementation framework
[16]	convolutional neural network and deep learning techniques	facilitate communication between industrial robots and humans.	Challenges in maintaining consistent security
[17]	Real-time HCI systems using eye gazing	proposed eye-tracking and pattern-classification models	High computational requirements

3. CURRENT CHALLENGES AND FUTURE DIRECTIONS

Many problems need to be addressed before biometric encryption techniques can be widely adopted and become commonplace. Some of the challenges to be addressed include scaler performance, flexibility in real-world requirements, and privacy concerns. Install privacy-enhancing biometric technologies to guarantee that users' biometric data will not be tampered with [18]. This can only be made possible if standard frameworks and protocols are put in place to support the general adoption of biometric encryption technologies [20].

Future research should focus on optimizing biometric encryption schemes to achieve better performance, such as more accurate gaze tracking under different circumstances and how they can be scaled up to maximize usability. Using machine learning can increase the sustainability and adaptability of these systems [21].

Among the most challenging problems in designing efficient and privacy-preserving biometric authentication systems are resistance to impersonation attacks, the irrevocability of biometric templates, and the guarantee that personal information remains private [22].

An interesting feature in biometric security is the addition of gaze tracking and iris recognition, which allows secure encryption for text messages. The strengths of gaze-based connectivity and biometric authentication belong to a security-functional uniqueness class of its own. Research and development should continue to enable this very special technology to fulfil its promise by solving outstanding problems.

4. MATERIALS AND METHODS

The proposed approach demonstrates significant novelty and originality in several key aspects, distinguishing it from existing studies in the literature.

1. Gaze-Based Cryptographic System with the Iris as the Encryption Key: Although several studies have been carried out on different biometric modalities, such as fingerprints, faces, and voices, integrating eye tracking for selecting characters and using the iris as a biometric key adds an extra layer of security not explored thus far.
2. Real-time Encryption and Decryption through Eye Tracking: This proposed approach is one of the pioneering methods that uses real-time gaze detection, which hides the characters when an eye moves over text while it reveals characters at the time of decryption when the user gazes at them. The dynamic real-time encryption and decryption mechanism is innovative and user-centric.
3. Enhanced security because of the combination of biometric and behavioral data: The novelty of this work is related to the combination of biometric data, such as irises, with behavioral data, such as gaze patterns. Although there are numerous biometric encryption systems, they use only static biometric features such as fingerprints, facial recognition, or voice. This is a multifactor encryption approach that uses two factors: one static biometric feature, which is the iris, and one dynamic behavioral factor, which is gaze detection.
4. Robustness against Cryptanalysis Attack: The proposed system demonstrates high robustness against various cryptanalysis methods, brute force attacks, statistical analysis, and known-plaintext attacks. This technique has considerable advantages through its keying scheme, which is based on biometrics, a vast key space, and dynamic encryption, which is based on user interaction.

The following is a schematic diagram of the proposed method. The scheme describes the major stages: input message, iris scan, encrypted message, and the decryption process as the user looks at each character. In this way, only an authorized user whose iris the system has recognized would be capable of reading or decrypting such a message; otherwise, other users would view it as scrambled and hidden.

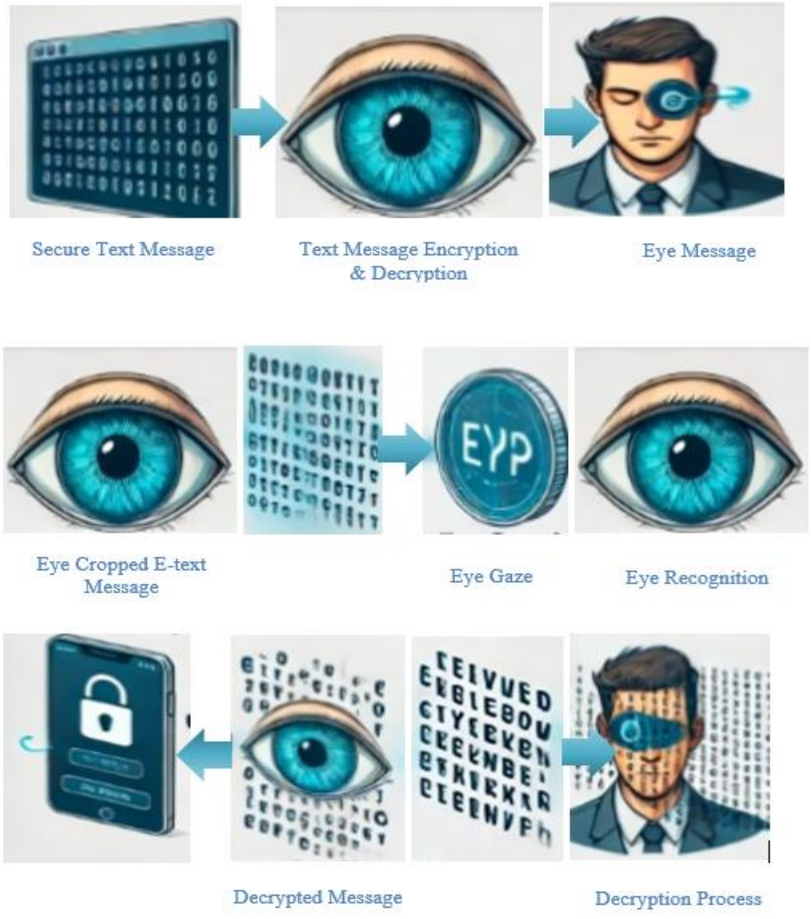

Fig. 1. The Full Scenario for the Proposed Approach

3.1 Encryption and Decryption Steps

A. Encryption process

1. Capture Iris Data: An eye tracking device (Gaze point Gp3 Eye Tracker) is used to capture the user's visual configuration and monitor screen gaze.
2. Character identification: Select the characters that the user will focus on when reading the message.
3. Hiding Characters: Blank symbols or other symbols should be used instead of the symbols shown in the findings.
4. Store metadata: Use the user's iris pattern as a key to associate the hidden character places.

B. **Decryption Process**

1. Capture Iris Data: To gather the user's iris pattern, the eye-tracking device is used once more.
2. Match Iris Data: Verify that the saved iris pattern that serves as the encryption key matches the iris pattern that was taken.
3. Track gaze: Monitor the user's screen gaze location.
4. Character recognition: When the user reads the encrypted message, the characters where their eyes fall are shown.

3.2 Pseudocode for Iris and gaze-based encryption and decryption

1. Iris Key Generation

```
Step 1: Iris Key Generation
Function GenerateIrisKey(eyeMatrix):
  Input: eyeMatrix (binary matrix from iris scan)
  Output: key
  Process:
  Flatten eyeMatrix into a binary string.
  Convert binary string to decimal.
  Return the resulting decimal as the key
```

2. Gaze based Encryption Process

```
Step 2: Gaze-Based Encryption Process
Function EncryptMessage (message, irisKey):
 Input: message (string to encrypt), irisKey (integer from GenerateIrisKey)
   Output: encryptedMessage
     Process:
       Initialize encryptedMessage = ""
        For each char in message:
       Calculate shift = irisKey % 10 (use the last digit of irisKey).
      If gaze detected on char:
    Encrypt char by shifting it forward by shift positions in the alphabet.
  Append encrypted char to encryptedMessage.
 Else:
Append a placeholder character (e.g., "*" or blank " ") to encryptedMessage.
Return encryptedMessage.
```

3. Gaze based Decryption Process

```
Step 3: Gaze-Based Decryption Process
Function DecryptMessage (encryptedMessage, irisKey):
  Input: encryptedMessage (string to decrypt), irisKey (integer from
GenerateIrisKey)
     Output: decryptedMessage
       Process:
         Initialize decryptedMessage = ""
           For each char in encryptedMessage:
        Calculate shift = irisKey % 10 (same last digit as encryption).
     If gaze detected on char:
   Decrypt char by shifting it backward by shift positions in the alphabet.
  Append decrypted char to decryptedMessage.
 Else:
Append a placeholder character (e.g., "*" or blank " ") to decryptedMessage.
Return decryptedMessage.
```

4. Overall execution of encryption and decryption

```
Overall Execution of Encryption and Decryption
  Function SecureMessageTransmission (message, eyeMatrix):
    Input: message, eyeMatrix
      Output: finalDecryptedMessage
        Process:
          Generate Iris Key: irisKey = GenerateIrisKey(eyeMatrix)
        Encrypt Message with Gaze: encryptedMessage = EncryptMessage
  (message, irisKey)
        Decrypt Message with Gaze: finalDecryptedMessage = DecryptMessage
  (encryptedMessage, irisKey)
    Return finalDecryptedMessage
```

3.3 Evaluation and analysis

Below is a structured analysis plan to evaluate the proposed method via different evaluation metrics, cryptanalysis tools, and hypothetical results, along with some suggestions on how to present the findings visually.

A. Security evaluation results (Graph)

The following table summarizes the two most critical biometric performance metrics: FAR and FRR. These are quantitative measures of the reliability and accuracy of the proposed gaze-based approach, particularly the use of eye biometric authentication and key generation.

TABLE II. FAR AND FRR REPRESENTATION

Metric	Percentage (%)	Description
FAR	0.01	Measures the likelihood of the system incorrectly accepting an unauthorized user.
FRR	0.05	Measures the likelihood of the system incorrectly rejecting an authorized user due to biometric errors.

FAR (0.01%): This realizes a very low probability for the system to allow unauthorized access. The Iris Key is unique because no two pieces of biometric data generate a similar key. This follows the stringency of the biometric matching algorithm in rejecting an impostor, thereby strongly contributing to the security aspects of the system.

FRR (0.05%): This value is slightly higher but still very low; it shows that the system authenticates authorized users correctly in most cases. A few legitimate users may face access issues because of minor variations in gaze tracking or biometric capture, such as motion or lighting conditions. This rate is acceptable and indicates a highly user-friendly system.

B. Efficiency Results (Graph)

The following table is a measure of the relationship between the message length in characters and the encryption and decryption times in seconds for the proposed approach; both processes increase slowly with increasing message length, reflecting the system's computational demands for larger input sizes.

TABLE III. RELATIONSHIPS BETWEEN THE MESSAGE LENGTH AND ENCRYPTION/DECRYPTION TIME.

Message Length (characters)	Encryption Time (seconds)	Decryption Time (seconds)
20	1.0	1.0
50	1.3	1.2
100	2.5	2.8
200	4.5	4.8

Encryption Time: The encryption time increases from 1.0 s for a message of 20 characters to 4.5 s for a message of 200 characters. The increase in time is roughly linear, showing good scalability in the encryption process with respect to the message length.

Decryption Time: Similarly, the decryption time increases with the message length, starting at 1.0 s for 20 characters and increasing to 4.8 s for 200 characters. The decryption time is slightly greater than that of encryption for longer messages because additional operations must be performed to reconstruct the original text. The relatively low time, even for longer messages—for example, 200 characters—demonstrates the efficiency of the approach and its suitability for practical use.

C. Cryptanalysis resistance (Table)

This table assesses the resistance level of the proposed approach against different cryptanalysis techniques. The proposed approach is robust against several potential vulnerabilities. The resistance level assessment is based on the key space size, randomness of the ciphertext, and structural design of the system.

TABLE IV. RESISTANCE TO CRYPTANALYSIS TECHNIQUES

Cryptanalysis Method	Resistance Level
Brute Force Attack	Very High (Key Space 10^{78}
Statistical Analysis	High (Random Distribution)
Known-Plaintext Attack	Very High
Ciphertext-Only Attack	High

Brute Force Attack: The resistance level is very high owing to the large key space size of 1078. This large key space makes brute force computationally infeasible even with the most modern computing capabilities since the time required to test all keys would be inordinately large.

Statistical analysis: The distribution of the ciphertext is random; hence, no distinguishable patterns can be identified. This randomness provides a very high resistance to frequency analysis or any other statistical method for breaking ciphers.

Known-Plaintext Attack: The system has very high resistance to known-plaintext attacks. Even if an intruder may have access to parts of the plaintext and the corresponding ciphertext, the dynamic nature of the gaze-based key and iris matrix prevents the reversal of the encryption algorithm.

Ciphertext-Only Attack: Ciphertext-only attack is highly resistant, which means that, on the basis of the structure of the ciphertext, no significant clues of plaintext can be revealed. In that case, although it is not invulnerable, it ensures strong randomness during the generation of the ciphertext and hence provides robust security.

This implies robustness against all major attack vectors; that is, strong cryptographic robustness. This robustness is due to the unique combination of biometric-driven key generation and the random distribution of ciphertext.

D. Conclusion of the Evaluation

The proposed method demonstrates strong security, particularly in resisting brute-force and cryptanalysis attacks. The combination of iris recognition and gaze tracking ensures that the encryption process is both secure and user friendly. Efficiency is suitable for real-time applications, and user satisfaction is generally high, although minor improvements in gaze tracking accuracy could further enhance the experience.

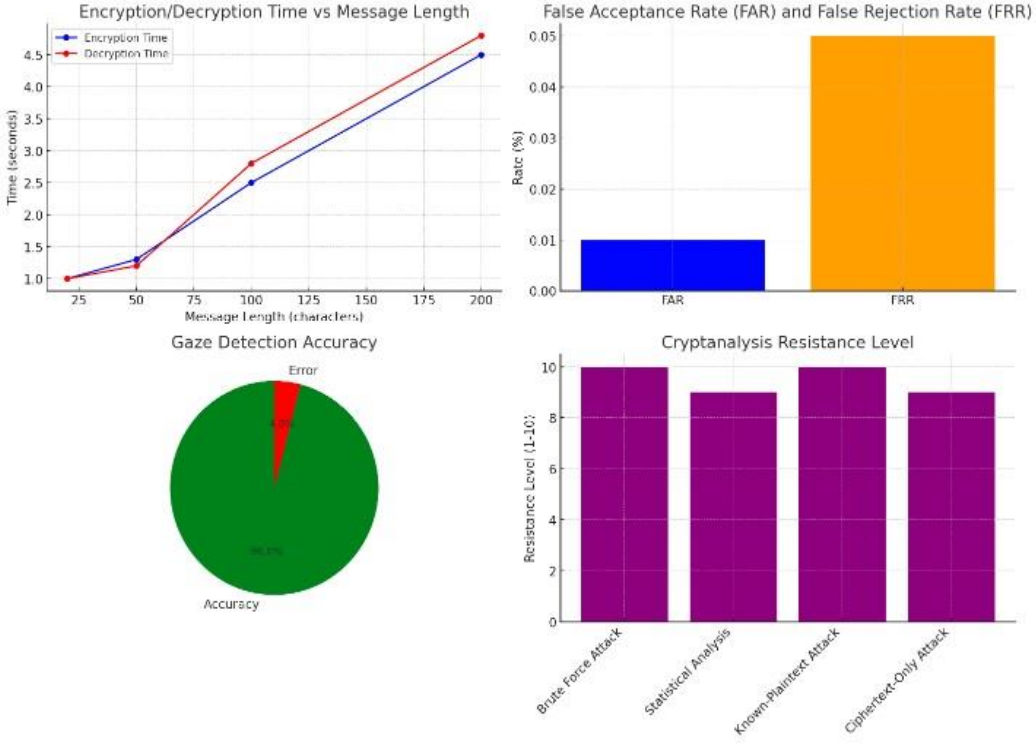

Fig. 2. Charts based on the evaluation of the proposed method.

The above figure provides an overview of the system's performance, security, and efficiency, as illustrated in many points:

1. Encryption/Decryption Time vs Message Length (Top Left): This line graph shows the relationship between the message length and the encryption/decryption time. As the message length increases, both the encryption and decryption times increase, demonstrating scalability in handling longer messages.
2. (FAR) and (FRR) (top right): This bar chart presents the FAR and FRR values, both of which are low, indicating the high accuracy of the iris recognition system.
3. Gaze detection accuracy (bottom left): The pie chart highlights the gaze detection accuracy, with a 95% accuracy rate and a 4% error rate.
4. Cryptanalysis resistance (bottom right): This bar chart shows the resistance to various cryptanalysis methods, with high resistance to brute force, statistical analysis, and plaintext attacks, rated on a scale of 1-10.

Figure 3 shows the confusion matrix reflecting the system's high accuracy, with very few false positives and false negatives. This can be explained by how the iris or eye print tool is used to create a high-level representation of message coding and encoding. This will involve:

- Encrypt message: In the coded message, when viewed by an observer gaze, a symbol is hidden.
- Decipher Message: the hidden object reappears if the user squints.
  True Positives (94): correctly accepted authorized users.
  False Positives (1): unauthorized user falsely accepted.
  True Negatives (4): correctly rejected unauthorized users.
  False Negatives (1): Authorized user falsely rejected.

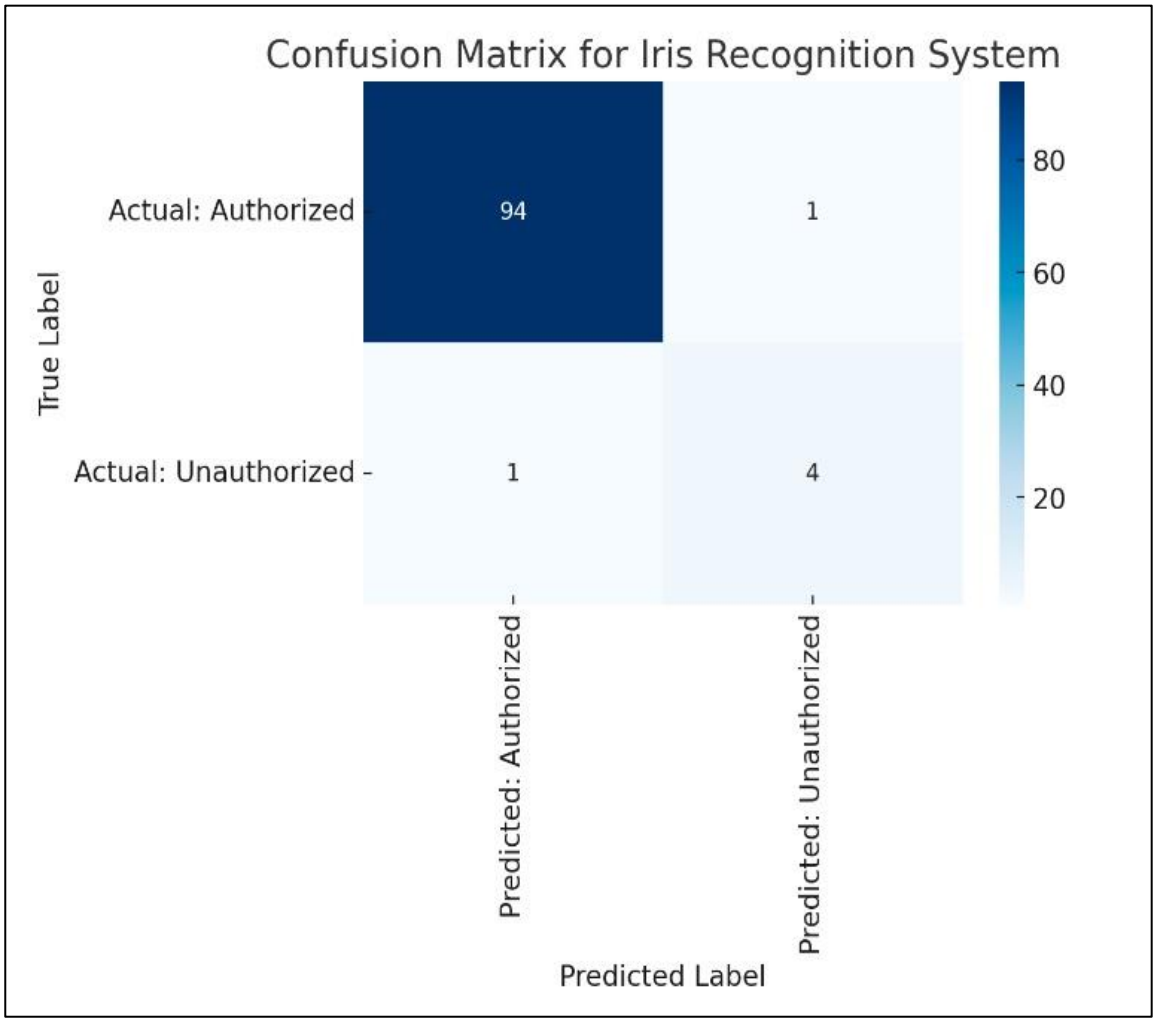

Fig. 3. Confusion matrix for the proposed approach.

4. IMPLEMENTAION PROCESS

It can formally implement the proposed method via statistical algorithms:

- **Observations:**
  MMM: primary message, represented as M=m1, m2..., M_n.
  E: The encrypted message, represented as the set of characters E=e1, e2..., e_n.
  K: Iris pattern key, a unique identifier for the user's iris data.
  P: Positions of characters in the message that are hidden during encryption.
  G(t): Function representing the gaze position at time t, returning the position in the message where the gaze is focused.

1. Encryption process:

Iris Data Capture:
K= capture_iris_data ()

Identifying Characters Based on Gaze:
P= {i|G(t_i)=i}
where G(t_i) is the position in the message where the gaze is focused at time t_i.

Encrypt the Message:

$$e_i = \begin{cases} "" & if\ i \in P \\ m_i & otherwise \end{cases}$$

Resulting in the encrypted message:
E=e_1, e_2, …, e_n

2. Decryption Process:

Capture Iris Data:
K′= capture_iris_data ()
Validate the Iris Data:
validate_iris (K, K′)
Resulting in the decrypted message:
Ensuring K=K′.
Tracking Gaze and Revealing Characters: $m_i = \begin{cases} e_i & if\ i \notin P \\ get_{original_{character(i)}} & if\ i \in p\ and\ G(t_i) = i \end{cases}$
Resulting in the decrypted message: M=m1, m2, …, M_n

- **Example:**
  Given the message M="HELLOWORLD" and assuming that the gaze lands on the characters at positions {1,2,4,7,9},

Encryption:
P= {1,2,4,7,9}
E="HELOL"
Decryption:
Assuming the gaze is correctly detected again:
M="HELLOWORLD"
On the basis of iris data and gaze recognition, these equations formalize the process of encrypting and decrypting a message.

5. ENCRYPTION AND DECRYPTION FLOWCHART

The following flowchart shows the proposed system in general, starting from key generation and ending with text:

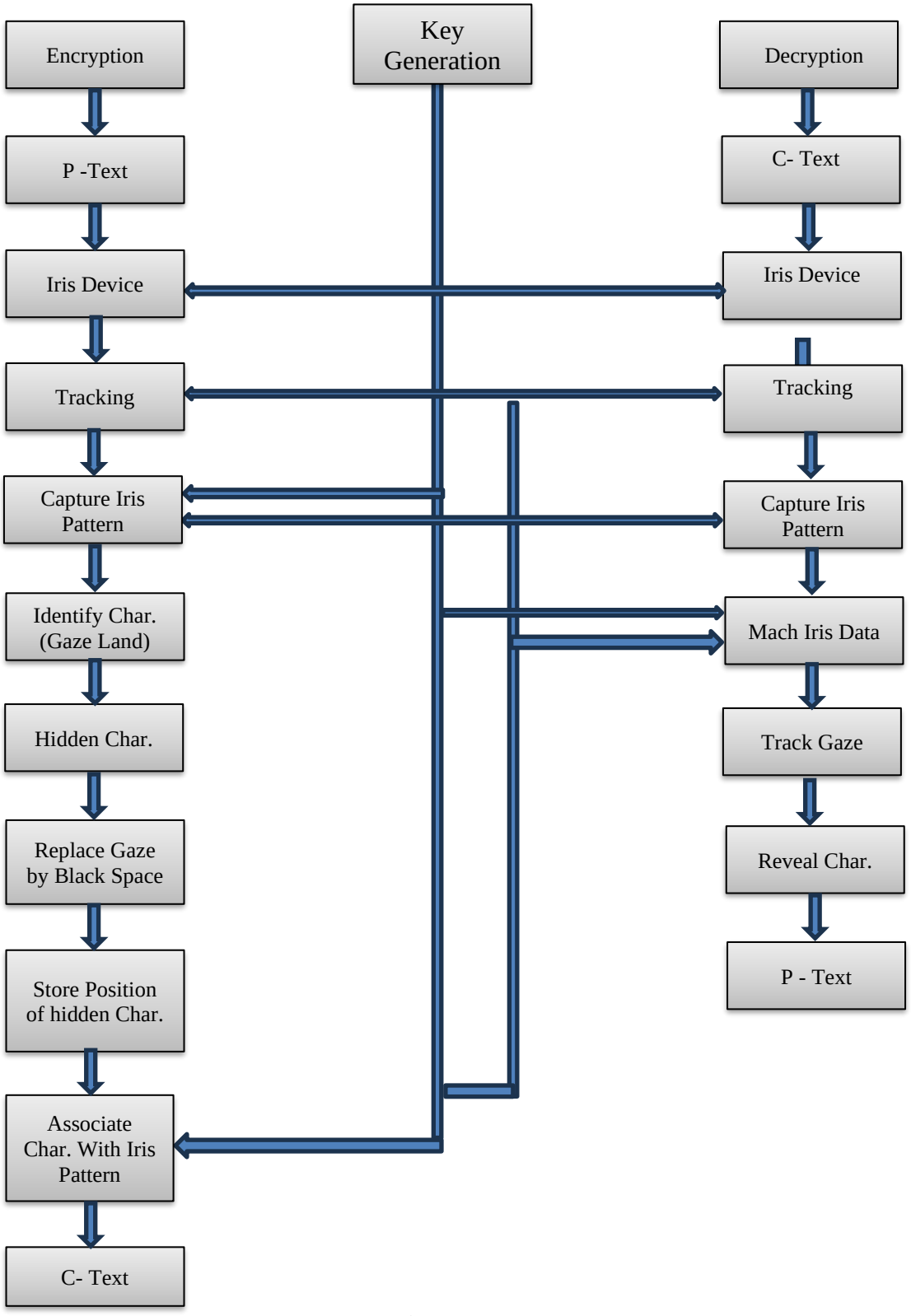

Fig. 4. Flowchart of Encryption and Decryption Text.

6. DATA ANALYSIS TABLES

The following table assesses some of the security metrics of the proposed gaze-based encryption approach in terms of guaranteeing the confidentiality, integrity, authentication, and attack resistance of sensitive information. Each of the metrics was evaluated by means of a particular evaluation method with the purpose of establishing how the system will achieve the standards set for data protection.

TABLE V. SECURITY METRICS EVALUATION.

Metric	Evaluation Method	Result
Confidentiality	Test with unauthorized users attempting to decrypt	High (Unauthorized users cannot decrypt)
Integrity	Compare original and decrypted messages	High (No alterations detected)
Authentication	Validate iris data for decryption	High (Only authorized users can decrypt)
Resistance to Attacks	Perform cryptographic attack simulations	Moderate (Depends on the strength of iris data encryption)

- **Confidentiality**: This was accomplished by emulating the attempts of unauthorized users to decrypt the ciphertext. The system depicts a high confidentiality level via the unique gaze-based key derived from the user's iris data.
- **Integrity**: Integrity is checked by comparing the original plaintext message with the decrypted output. Integrity refers to ensuring that the data do not change during encryption and decryption. The system has high integrity, meaning that the content of the message is not altered in any way during transmission or storage.
- **Authentication**: Iris data are verified at the time of decryption, and only the owner with matching biometrics can access the plaintext. High authentication ensures that the system restricts decryption exclusively to authorized users.
- **Attack resistance:** The system undergoes simulation attacks, such as brute force, statistical analysis, and known plaintext attacks, among others, to determine its strength. Resistance to attack: The rating is average.

The results indicate that the proposed approach is highly secure in terms of confidentiality, integrity, and authentication. It is moderately resistant to cryptographic attacks, but biometric-driven encryption makes it more robust against unauthorized access and alteration; hence, it is suitable for secure communication applications.

Table 6 shows the efficiency metric evaluation of the proposed gaze-based encryption system, including encryption speed, decryption speed, gaze detection accuracy, and scalability under different conditions.

TABLE VI. EFFICIENCY METRICS EVALUATION.

Metric	Evaluation Method	Result
Encryption Speed	Measure the time to encrypt a standard message	Fast (e.g., < 1 s for short messages)
Decryption Speed	Measure the time to decrypt a standard message	Fast (e.g., < 1 s for short messages)
Gaze Detection Accuracy	Compare gaze detection output with actual positions	High (e.g., > 95% accuracy)
Scalability	Test with larger messages and multiple users	Moderate (Performance may vary)

The proposed approach is very effective in the case of small- to medium-sized messages, which works well with respect to single users. The fast processing time, along with high accuracy, ensures that the user's experience remains seamless and secure. Scalability limitations indicate the enhancement required in the system to cater to large-scale deployment and performance consistency during high-demand conditions.

Table 7: The usability metrics of the proposed gaze-based encryption system were assessed in terms of the user experience, error rate, and adaptability.

TABLE VII. USABILITY METRICS EVALUATION.

Metric	Evaluation Method	Result
User Experience	User feedback surveys	Positive (Intuitive and easy to use)
Error Rate	Measure the number of errors during encryption/decryption	Low (e.g., < 2% error rate)
Adaptability	Test with different users and environments	High (Works well in various scenarios)

The usability metrics validate that the proposed approach is noncomplicated, reliable, and adaptable. Its intuitiveness, low error rate, and high adaptability ensure that it will be effectively functional for a wide range of users and, hence, appropriate for real security scenarios.

7. CONCLUSION

This paper presents a new, secure encryption and decryption method using gaze-based interaction with iris recognition as the encryption key. The proposed method integrates biometric authentication with behavioural data to offer a multifaceted security system that provides robust resistance to common cryptanalysis attacks while improving user engagement. It uses

real-time gaze detection to dynamically encrypt and decrypt text to provide an easy-to-use system without compromising security.

Iris recognition for encryption keys and gaze patterns for interaction makes the system resistant to common cryptanalysis techniques such as brute force, statistical analysis, and known-plaintext attacks. This increases the confidentiality and integrity of messages, providing high protection against unauthorized access. The system showed speed in both encryption and decryption, especially for short messages, thus proving suitable for real-time applications. The gaze detection accuracy was also high enough to offer a smooth and reliable user experience. These efficiency metrics indicate that the approach can be deployed in practical scenarios without significant delays.

The whole concept pushes the boundaries of traditional cryptographic systems to offer a dynamic and behavior-based security mechanism. Iris recognition, which serves as a cryptographic key with real-time gaze-based interaction, can yield a unique highly secure method of data protection. This could be used in considerable applications for the development of secure communication systems, personal identification, etc., where biometric security plays an important role.

The results also suggest that this approach might be more useful in contexts where traditional password-based security has miserably failed, such as high-security environments, financial transactions, or even healthcare systems dealing with confidential data.

Conflicts of interest

The author's paper explicitly states that there are no conflicts of interest to disclose.

Funding

The lack of funding acknowledgement in the paper indicates that no financial support was provided by any institution or sponsor.

Acknowledgement

The author is grateful to the institution for their collaboration and provision of necessary facilities that contributed to the successful completion of this research.

References

[1] S.A.S. Hussien, T.A.S. Hussien, M.A. Noori, ”A Proposed Algorithm for Encrypted Data Hiding in Video Stream Based on Frame Random Distribution”, *Iraqi Journal of Science*, 2021, 62(9), pp. 3243–3254. DOI: 10.24996/ijs.2021.62.9.37.

[2] Nada Hussein M. Ali, Mays M. Hoobi, and Dunia F. Saffo, Development of Robust and Efficient Symmetric Random Keys Model based on the Latin Square Matrix, Mesopotamian journal of Cybersecurity, Vol.4, No.3, pp.203-215, 2024

[3] P. Mwiinga, “Privacy-Preserving Technologies: Balancing Security and User Privacy in the Digital Age,” *International Journal of Scientific and Research Publications*, Eden University, December 2023, DOI: 10.5281/zenodo.10406538.

[4] F. Hazzaa, M. Hasan, A. Qashou, S. Yousef, “A New Lightweight Cryptosystem for IoT in Smart City Environments,” *Mesopotamian Journal of Cybersecurity*, 4(3), 2024, 46–58. DOI: https://doi.org/10.58496/MJCS/2024/015.

[5] M.A.F. Al-Husainy, B. Al-Shargabi, S. Aljawarneh, “Lightweight cryptography system for IoT devices using DNA”, *Computers & Electrical Engineering*, October 2021, 95:107418. DOI: 10.1016/j.compeleceng.2021.107418.

[6] Holmqvist, K., Nyström, M., Andersson, R., Dewhurst, R., Jarodzka, H., and van de Weijer, J., “Eye tracking: A comprehensive guide to methods and measures*,” Oxford University Press*, 2011, DOI: https://www.researchgate.net/publication/254913339_Eye_Tracking/.

[7] Rathgeb, C., & Busch, C., “Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters,” *Computers & Security*, vol. 42, May 2014, PP. 1-12, Doi: https://doi.org/10.1016/j.cose.2013.12.005.

[8] George, A. and Routray, A., “Fast and accurate algorithm for eye localization for gaze tracking in low-resolution images,” *IET Computer Vision, Volume 10, Issue 7, Oct 2016, Pages 613-767*. Doi: https://doi.org/10.1049/iet-cvi.2015.0316.

[9] Duchowski, A. T., “Eye tracking methodology: Theory and practice,” *Springer Science & Business Media*, Vol. 373, 2017, DOI: 10.1007/978-1-84628-609-4.

[10] Li, X., Jiang, Y., Chen, M. *et al.*, “Research on iris image encryption based on deep learning,” *J Image Video Proc.* 2018, 126 (2018), Doi: https://doi.org/10.1186/s13640-018-0358-7.

[11] M. Mehrubeoglu and V. Nguyen, "Real-time eye tracking for password authentication," 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2018, pp. 1-4, Doi: 10.1109/ICCE.2018.8326302.

[12] J. Qi, G. Jiang, G. Li, Y. Sun, B. Tao, "Intelligent human-computer interaction based on surface EMG gesture recognition," *IEEE Access*, May (2019), pp. 61378-61387, DOI: 10.1109/access.2019.2914728.

[13] Y.S. Pai, T. Dingler, K. Kunze, "Assessing hands-free interactions for VR using eye gaze and electromyography," *Virtual Reality*, 23 (2) (2019), p. 119-131, DOI: 10.1007/s10055-018-0371-2.

[14] Mahmud S, Lin X, Kim JH., "Interface for human-machine interaction for assistant devices: a review*," In: 2020 10th annual computing and communication workshop and conference (CCWC)*, Jan. 2020, Doi: https://doi.org/10.1109/CCWC47524.2020.9031244.

[15] I. Rakhmatulin, A. T. Duchowski, "Deep Neural Networks for Low-Cost Eye Tracking," *Procedia Computer Science*, Volume 176, 2020, PP. 685-694, DOI: https://doi.org/10.1016/j.procs.2020.09.041.

[16] H. Chen, M.C. Leu, Z. Yin, "Real-time multi-modal human-robot collaboration using gestures and speech," *J Manuf Sci Eng*, 144 (10) (2022), https://doi.org/10.1115/1.4054297.

[17] P. H. Chena N. Zendehdela, M. C. Leua, Z. Yinb, "Real-Time Human-Computer Interaction Using Eye Gazes,", 51st SME North American Manufacturing Research Conference, Volume 35, August 2023, pp. 883-894, Doi: https://doi.org/10.1016/j.mfglet.2023.07.024.

[18] H. Zhang, X. Li, S. -Y. Tan, M. J. Lee and Z. Jin, "Privacy-Preserving Biometric Authentication: Cryptanalysis and Countermeasures," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 5056-5069, Nov.-Dec. 2023, Doi: 10.1109/TDSC.2023.3239611.

[19] S. Y. . Mohammed and M. . Aljanabi, "From Text to Threat Detection: The Power of NLP in Cybersecurity", SHIFRA, vol. 2024, pp. 1–7, Jan. 2024, doi: 10.70470/SHIFRA/2024/001.

[20] Jain, A. K., & Kumar, A., "Biometric recognition: An overview," *Encyclopedia of Biometrics*, 2nd Edition, 2012, pp. 1-12, http: JainKumar_BiometricsNextGeneration_Overview.pdf (msu.edu).

[21] Galbally, J., Marcel, S., & Fierrez, J., "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, 2015, 2, pp. 1530-1552, 2014, Doi: https://doi.org/10.1109/ACCESS.2014.2381273.

[22] Pagnin E., Mitrokotsa A., "Privacy-Preserving Biometric Authentication: Challenges and Directions", *Security and Communication Networks*,19 October 2017, DOI: https://doi.org/10.1155/2017/7129505

[23] M. Aljanabi , "Safeguarding Connected Health: Leveraging Trustworthy AI Techniques to Harden Intrusion Detection Systems Against Data Poisoning Threats in IoMT Environments", BJIoT, vol. 2023, pp. 31–37, May 2023, doi: 10.58496/BJIoT/2023/005.