


Object Selection as a Biometric

Joyce Tlhoolebe ^{1,2,*} and Bin Dai ^{1,3} 

¹ School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China; daibin@home.swjtu.edu.cn

² The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

³ Peng Cheng Laboratory, Shenzhen 518055, China

* Correspondence: jtlhoolebe@my.swjtu.edu.cn

Abstract: The use of eye movement as a biometric is a new biometric technology that is now in competition with many other technologies such as the fingerprint, face recognition, ear recognition and many others. Problems encountered with these authentication methods such as passwords and tokens have led to the emergence of biometric authentication techniques. Biometric authentication involves the use of physical or behavioral characteristics to identify people. In biometric authentication, feature extraction is a very vital stage, although some of the extracted features that are not very useful may lead to the degradation of the biometric system performance. Object selection using eye movement as a technique for biometric authentication was proposed for this study. To achieve this, an experiment for collecting eye movement data for biometric purposes was conducted. Eye movement data were measured from twenty participants during choosing and finding of still objects. The eye-tracking equipment used was able to measure eye-movement data. The model proposed in this paper aimed to create a template from these observations that tried to assign a unique binary signature for each enrolled user. Error correction is used in authenticating a user who submits an eye movement sample for enrollment. The XORed Biometric template is further secured by multiplication with an identity matrix of size $(n \times n)$. These results show positive feedback on this model as individuals can be uniquely identified by their eye movement features. The use of hamming distance as additional verification helper increased model performance significantly. The proposed scheme has a 37% FRR and a 27% FAR based on the 400 trials, which are very promising results for future improvements.

Keywords: biometric authentication; biometrics; eye tracking; pattern recognition; saccades; machine learning



Citation: Tlhoolebe, J.; Dai, B. Object Selection as a Biometric. *Entropy* **2022**, *24*, 148. <https://doi.org/10.3390/e24020148>

Academic Editor: Carlos M. Travieso-González

Received: 9 November 2021

Accepted: 12 January 2022

Published: 19 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Security and privacy issues are common problems in the field of computer science, and they are a general national concern. Privacy is contextually based on the specifics of who should do what and where [1]. Recently, the availability of low-cost data that aids in ample data communication, securing data and applications from unauthorized identities is becoming very important to help control access to software, data, devices and physical buildings [2]. Despite the widespread use of passwords to authenticate users, there are many weaknesses and drawbacks associated with this method of user authentication [3]. For example, in a password authentication system, there is a verification table used to verify the users' passwords when they log in to the system [3]. If an event of a security breach occurs and the verification table is compromised by an intruder, then the whole system or parts of the system will be breached.

However, alphanumeric passwords are vulnerable to shoulder surfing attacks, dictionary attacks and social engineering attacks [4]. Shoulder surfing is whereby someone who is not intended to know the user's password can look over the user's shoulder as they enter the password and thereby obtain the password [5]. Social engineering attacks are

based on human interaction, and they normally involve tricking users to break security policies because they appear harmless and look appropriate [6]. For example, in a social networking site such as Facebook, the attacker can analyze and exploit the user's interest and send some recommendations based on the information that was gathered from their profile [7].

2. Biometric Authentication

As one of the countermeasures to the problems encountered with the use of passwords, the adoption of biometric authentication systems emerged. Biometric authentication is a system whereby a user is identified or verified with their physical or behavioral characteristics such as their iris pattern, DNA, fingerprints, voice and face [8]. The use of biometrics is growing rapidly and is used for authentication in applications such as border controls and access control to physical facilities [8,9]. This method of user authentication can also be used even in setting up profiles on mobile devices [8]. The use of biometric authentication methods developed as one of the solutions used to counter problems with traditional authentication methods such as the password. A significant growth in the market for biometric authentication is expected, from \$2.0 billion in 2015 to \$14.9 billion by 2024 [10]. However, in real applications, there are still some security concerns encountered with current biometric authentication methods [11]. It is possible for intruders to breach the security of the database storing the biometric information and steal it [10].

Eye movement as a biometric technique makes use of physiological and behavioral aspects, and these traits make this biometric difficult to copy [11–13] as compared to traditional authentication techniques. Eye movement biometrics identifies behavioral patterns and other information regarding physiological properties that generates eye movements [14]. Several studies showed that the use of eye movement for human identification is a promising research field [12–14]. In previous studies, a high level of accuracy has been achieved, such that eye movement biometric can be an independent biometric technique without being integrated with other modalities [14]. However, recognition error rates for this technique are still high, but recent progress has been promising [15]. The usability and acceptability of eye movement as a biometric technique can be highly influenced by the overall design of the interfaces and the objects used in extracting the eye movement pattern [16]. The movement of eyes can be obtained from observing images, reading of text, jumping points pattern, or any vision process, and this movement can be recorded using an eye-tracking device [13,17].

Research on eye movement as a biometric was first done in 2004 by Kasproski et al., where they designed a jumping point as their object of observation [15,18–20]. The jumping point was displayed in a computer screen to jump to different points of the screen, and they analyzed eye movement pattern of users as they watched the jumping point on the screen. The overall recordings of the movement patterns results were obtained from measuring features such as " . . . distance to stimulation, eye difference, Fourier and Wavelet transform of the eye signal . . . " [19]. A 16% average error rate was obtained from this method after the tests were done several times for each user [19]. The results of this method opened a research path for many researchers to carry out some investigations on this method but using different objects to carry out their experiments [18]. Instead of using one object as the stimulus, a study by [17] went further by doing experiments on different objects and combining them together. The experiment included presenting users with images of human faces followed by a white screen with a small cross at the center, a moving circle and black and white shapes that were randomly presented to record the movement of their eyes. Hotspots were also able to be recorded as they showed the highest concentrations of fixations as the user observed the objects mentioned above.

3. Acceptance and Privacy Issues of Biometric Systems

Although some biometric systems may provide high levels of security, the targeted group may not accept it, depending on the issues surrounding the privacy of users. A biometric system that is rejected by a large number of the targeted population is not suitable for use [21]. If a biometric system is comfortable and ease to use, that will highly contribute to its acceptance [22]. Users prefer little interaction with the biometric system, and they will deem it as being useable and more convenient for them. However, as a measure to minimize user interactions with the biometric systems, there are some biometric systems that are able to identify users and extract other additional information without the users' knowledge, and this has raised some privacy issues [22,23]. For example, biometric-based recognition systems such as the retina pattern recognition system may provide some additional background information about the health of the users' eyes, which therefore may deprive the users of this information [22]. As a second example, in a fingerprint-recognition system, if a person has some malformed fingers, this might be statistically associated with some certain genetic disorders [23].

However, the main issues on biometric systems is that biometric systems are associated with the conflict on how the data will be collected, protected and used, as well as the conflict with each individual's beliefs and values [24,25]. The flexibility of data movement on the internet also leads to loss of data control from user [13]. Some biometric identification systems such as the fingerprint systems may lead to the possibility of unwanted identifications of individuals since some systems have recently become centralized [21,23]. Weaknesses in the use of traditional methods have led to the evolution on the use of biometric authentication methods that use the "what you have" technique. This technique brought some advancement in security. These techniques include fingerprint, retina, iris, eye movement and face recognition. The use of a particular biometric technique depends on what you want the system to achieve. Studies have shown that using one or more biometric techniques can improve security. Eyes have features that produce useful information that can be used in biometric authentication. While different studies in to the general applicability of eye movement biometrics has been done, some of the proposed approaches had some high error rates and low identification rates. In this work, we consider measuring various characteristics of the eye movement pattern (the scan path) and analyzing those characteristics to uniquely identify individuals.

4. Materials and Methods

4.1. Participants

Data were collected from a total number of 20 participants. Participants were randomly personally invited and some were invited by email, and they were from different departments in the university. The age of the participants ranged from 18 to 38. The minimum age of participants was 18 years. From the targeted participants, all participants managed to engage to the end.

4.2. Tasks

The experiment consisted of one task, which involved choosing and finding objects displayed in 30 slides. All the slides displayed 15 different objects of the same size and different colors and all were equidistant with the same properties (feel and design). On the first slide, participants were asked to scan the objects displayed on the screen. The first slide was displayed for 30 s to give participants enough time to learn the objects, and the rest of the slides were each displayed for eight seconds. On the second slide until the last one, objects were re-arranged, and participants were tasked to choose any three objects of their choice. Re-arranging objects on the other slides was done to encourage participants to be fully engaged in the experiment as they were required to always look for the three objects that they chose.

4.3. Equipment and Software

The device used to record eye movements was the Senso Motoric Instruments (SMI) RED250 mobile eye tracker operating with a temporal resolution of 250 Hz. The objects used in the experiment were all designed with Microsoft PowerPoint 2013. The objects (stimuli) were presented on a white background flat screen monitor in a screen resolution of 1920×1080 pixels. The eye tracker was placed on a table and the objects (stimulus) were at a rough distance of approximately 50 cm from the participant's eyes. The software was able to give feedback during the calibration phase. This distance between the participant's eyes and the eye tracker was fixed with a 10 cm flexibility range due to differences in participants' body structure. Some were tall, and some were short and therefore the distance could not be strictly fixed to the same distance. The eye tracking equipment was installed with an eye positioning software that was able to guide the participants to position their eyes within the scene area. A red arrow blinked as an indication to show the participants the direction in which they should try to position their eyes. Data were analyzed using the Be Gaze 3.6.52 analysis software which is part of the former SMI (Senso Motoric Instruments) originally from Paris, France.

4.4. Feature Extraction and Selection

A complete scan path is described by its particular characteristics, and those characteristics can be used to uniquely identify individuals [12]. Figure 1 below shows a random selection of users scan paths. From the picture we could tell an object with the highest fixation duration because it has a bigger circle around it. Eye movement tracking equipment is a sophisticated tool that is able to measure a variety of properties of eye movement patterns. For this study, only certain properties that were needed were recorded and used. Even if the pattern can be the same, some properties of the patterns are completely different because physiological actions are influenced by brain activity [14]. The following metrics were measured and used for unique personal identification [12]: fixation duration, fixation count, scan path length, fixation frequency, saccade frequency count, saccade duration, saccade velocity and the object fixation duration. These metrics were measured based on each scan path for each individual.

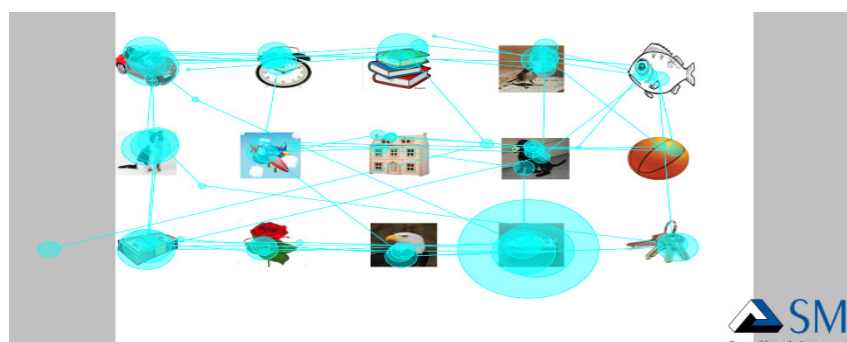


Figure 1. Scene Scan Path.

Fixation duration: this is the time in seconds that shows how long a participant took to fixate in the experiment.

Fixation Count: this is the total number of fixations the participants made in the entire experiment recording [12].

Dwell time: this is the time the participant spent looking within the boundary of an object.

Average blink Duration: this is the average number of blinks a participant made throughout the experiment.

Object fixation Duration: this is time in which participants fixated on particular objects. Duration of fixation on each object on the scene will be calculated. See appendix 3 for each object fixation duration.

Scan path length: this feature can be calculated by measuring the total distance between all the fixation points in a scan path [12].

Fixation frequency: this is the time in seconds in which the participant fixated on a particular object.

Saccade Amplitude average: A saccade is the movement of eyes between the fixations. The saccade amplitude is obtained by summing the horizontal and vertical saccade amplitudes and dividing them by the number of saccades.

Pupil diameter: this is the size of the pupil and is normally computed by the eye-tracking equipment. The average pupil size varies from 2 to 4 mm in diameter and it normally increases from about 4 mm in bright light and 8 mm in the dark [26].

Saccade frequency count: this is the speed in which the eyes move from one fixation point to the other.

Saccade duration average: this is the average time in milliseconds taken by an individual to complete the saccade [26]. Saccades are in most cases completed within an average time of ten milliseconds.

Saccade Velocity: the saccade velocity is the speed in which a saccade was completed.

5. Architecture of the Classification Process

From the 600 observations, 300 were used for enrollment and the other 300 were used as testing data. Figure 2 below shows the classification process which shows how data was analyzed. Cross validation was done by randomly selecting a sample from the entire sample except the instances defined in creating the template for enrollment in that specific trial., e.g., if the first 30 observations (3 realizations for a single user) are used to create user 1 biometric template then the cross-validation set was defined as a random trial from all other observations except the 30 that are used. The testing dataset contained only 1 realization for each user with the assumption that only 1 sample will be accepted and recognized as the attempt biometric.

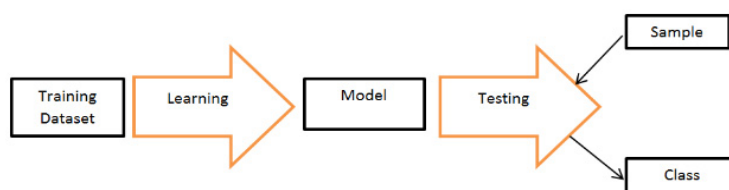


Figure 2. Architecture of the classification Process.

5.1. Classification Method

Let x_1, \dots, x_n be a correctly classified sample in classes $\theta_1, \dots, \theta_2$, where x_i takes values in a metric space upon which a distance function d is defined. We consider the pairs (x_i, θ^i) where the x_i 's represent the p-variate observation on the i 'th individual and θ^i is the class to which they belong. It is usually said that x_i belongs to θ^i , which means that the i 'th individual upon which measurements x_i have been observed belongs to category $\theta^i \in \{\theta_1, \dots, \theta_M\}$.

Consider a new pair of values (x, θ) where only x is observable and one wants to estimate the value of θ , using the training data that already have correctly classified observations. An observation

$$x' \in \{x_1, \dots, x_n\}$$

is denoted the nearest neighbor of x if [27]

$$\min_{i=1, \dots, n} dist(x_i, x) = dist(x', x)$$

The NN classification method assign the observation x the category θ^i of its nearest neighbor x_i . The decision rule k has to be modified in the case of a tie between classes.

5.2. Distance Function

A case is classified by a majority vote of its neighbors, with the case being assigned to the class most common amongst its k Nearest neighbors measured by a distance function. If $k = 1$, then the case is simply assigned to the class of its nearest neighbor. The value of k is usually small and an integer with positive value. If $k = 1$, class allocation of the sample is based on the nearest one neighbor within a certain distance.

5.3. Euclidian Distance

This is an instance-based classification algorithm similar to the k -Nearest Neighbor (kNN). Each new instance x is compared with existing ones $x' \in \{x_1, \dots, x_n\}$ using a distance metric, and the closest existing metric is used to assign a class θ^i to the new instance. The difference with this algorithm and the kNN is that instead of Euclidian distances, it uses the concept of entropy to define its distance measure. The Euclidean distance is a measure to find distance between two points. In Cartesian coordinates, if there are two points in Euclidian k -space, then the distance (*dist*) from/to is defined by Pythagoras's theorem. The formula is as follows [28]:

$$dist(x, y) = \sqrt{\sum_{i=1}^k (x_i - y_i)^2}$$

where a_i and b_i are the values of the i 'th argument of x, y vectors.

5.4. Naïve Bayes Classifier

This is a simple probabilistic classifier that applies the Bayes' theorem with strong assumptions of independence. This method assumes that the presence of a particular feature of a class is unrelated to any other feature [29]. Parameter estimation is done using the method of maximum likelihood, and the Bayes classifier needs only a small sample of training data to estimate parameters.

5.5. Naïve Bayes Model

The probability model can be presented as a conditional probability model

$$P(C|F_1, \dots, F_n)$$

where C represents a dependent class variable with a small number of classes, and F_1, \dots, F_n are some feature variables. The model can be extended and presented such that [30]

$$P(C|F_1, \dots, F_n) = \frac{P(C)P(F_1, \dots, F_n|C)}{P(F_1, \dots, F_n)}$$

which indicates that

$$\text{posterior} = (\text{prior} \times \text{likelihood}) / \text{evidence}$$

The naïve assumption of conditional independence of features means that for features F_i and F_j , there is conditional independence such that $i \neq j$. Under the assumption of independence, the conditional distribution over the class variable C can be expressed as [30]

$$P(C|F_1, \dots, F_n) = \frac{1}{Z} P(C) \prod_{i=1}^n P(F_i|C)$$

where Z is a scaling factor dependent only on F_1, \dots, F_n . There are k classes, and in practice, classes are often binary ($k = 2$).

5.6. K-Star Algorithm

This is an instance-based classification algorithm similar to the k-Nearest Neighbor (kNN). Each new instance x is compared with existing ones $x' \in \{x_1, \dots, x_n\}$ using a distance metric, and the closest existing metric is used to assign a class θ^i to the new instance. The difference with this algorithm and kNN is that instead of Euclidian distances, it uses the concept of entropy to define its distance measure.

5.7. Classification of K-Star

The classification with K-Star is made by summing the probabilities from the new instance to all of the members of a category. This must be done with the rest of the categories to finally select that with the highest probability [31,32]. The K-star algorithm uses entropic measures that are based on the probability of transforming an instance into another by choosing between all possible transformations using the random method. Using entropy as a measure for an instance distance is very beneficial. Information theory helps in computing the distance between the instances.

Let I be a set of instances that is possibly infinite and T be a finite set of transformations on I . Each T maps instances to instances as $t : I \rightarrow I$. The transformations T contain a distinguished member denoted σ , which maps instances to themselves for completeness ($\sigma(a) = a$). Let P be the set of all prefix codes from T^* , which are terminated by σ (stop symbol). Members of T^* and P uniquely define a transformation on I .

The K^* function is defined as [33]

$$K^*(b|a) = -\log_2 P^*(b|a)$$

where P^* , the probability function, is defined as the probability of all paths from distance a to distance b .

5.8. k Nearest Neighbor

k Nearest Neighbors is one of the simplest algorithms but it is very often accurate. Its main idea is that samples with the same classification tend to appear nearby. 'Nearby' refers to the distance between them being generally closer than the distance between samples with different classification. The distance may be calculated differently, but the Euclidean distance is used most frequently. Other distance measures include the Hamming distance and Manhattan/city block distance [30].

$$P(C|F_1, \dots, F_n) = \frac{1}{Z} P(C) \prod_{i=1}^n P(F_i|C)$$

where Z is a scaling factor dependent only on F_1, \dots, F_n . There are k classes and in practice classes are often binary ($k = 2$).

5.9. Naïve Bayes Classification

The Naïve Bayes classifier combines the probability model with a decision rule. The common approach is to choose the most probable hypothesis (called the maximum a posteriori or MAP decision rule). The classify function can be expressed as [34]

$$\text{classify}(f_1, \dots, f_n) = \operatorname{argmax} P(C = c) \prod_{i=1}^n P(F_i = f_i | C = c)$$

5.10. Support Vector Machine

The support vector machine (SVM) is a supervised machine learning algorithm that can learn how to attach labels to objects [35,36]. The SVM uses a sample of objects (training) separated into classes to find the hyper plane in the data that produces the largest minimum distance between objects.

A linear SVM problem can be presented in terms of a two-class identification problem. The hyper plane decision boundary can be presented such that [35]

$$f(x) = \beta((w * x) + b)$$

where 'x' is the training data, 'b' is the bias vector and 'w' is the weight vector, and the norm of w determines the Vapnik–Chervonenkis (VC) dimensions.

Mapping is used by SVM schemes that are designed to ensure that dot products of pairs of input data vectors can easily be computed in terms of variables in the original space (training data set). This is done in terms of a kernel function $k(x, y)$ selected to suit the problem.

5.11. J48

This is a widely algorithm used to construct decision trees. It is an implementation of C4.5 algorithm in Weka. Output for this algorithm is in the form of a decision tree with the roots that represent tests on an attribute and leaf nodes that represent classification [37]. An advantage of using this algorithm is that the results are easy to interpret because it works with nominal data and numeric data. A 98.51% accuracy was obtained by [37] when they compared the J48 with other decision trees under a 10-fold cross validation condition.

5.12. Statistical Presentation

Let the 'n' training vectors be denoted by $\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ such that $x_i \in R^n$ and $y_i \in \{-1, 1\}$. For linearly separable training data,

$$y_i(x_i * w + b) - 1 \geq 0; \text{ where } \forall i = 1, \dots, n$$

The margin of points between two points in different classes is defined by two hyperplanes $(x * w + b) = \pm 1$ such that no point can lie within this margin. Simplified calculation is done by converting the problem into the Lagrange framework and maximizing the value of the margin by minimizing the weights $\|w\|$.

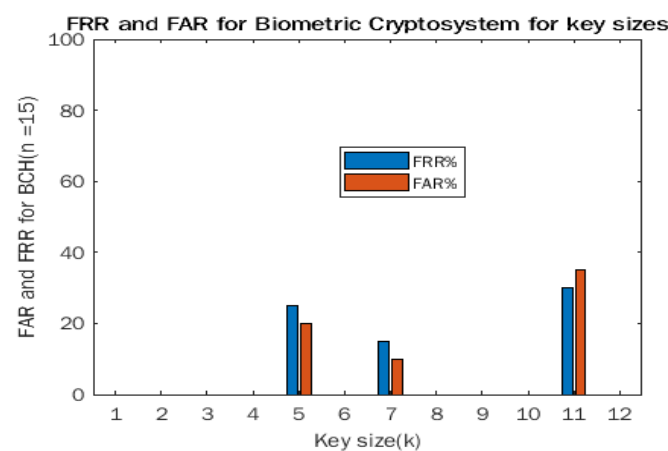
6. Results

From Table 1 below, the cryptosystem performs best where key size $k = 7$ returning the lowest FRR and FAR at 15% and 10%, respectively. A longer message length reduces the accuracy of the cryptosystem. The biometrics are binarized using the inter-class means difference from the intra-class means. This will return a zero when the column mean is less than the overall mean and a 1 otherwise. This helps to create an irreversible binary template and the initial binary data can be deleted. For experiment purposes, we have created a secret key of size 3 using a random number generator containing only ones and zeros [0,1]. This key/message is then run through BCH encoding after conversion to Galois field GF (2). The parameters for the BCH codes are ($k = 3$ and $n = 9$). The hash of the secret key is taken and stored later for user authentication. For the individual enrolling in the fuzzy commitment scheme, a secret key is further XORed with the biometric sample and the XORed biometric template is further secured by multiplication with an identity matrix of size $(n \times n)$. The simulation was run 400 times on the first 10 subjects with 200 legitimate trials and 200 false inquiries. The model performed poorly in identification task as the BCH encoder tended to correct errors too well. The use of hamming distance as additional verification helper increased model performance significantly. The proposed scheme has a 37% FRR and 27% FAR based on the 400 trials during the identification process. The results suggest that the scheme would perform better if integrated with another biometric to improve its performance.

Table 1. FRR and FAR for biometric cryptosystem for key sizes.

Message Length	Simulation Result	Mean	Min	Max
K = 5	FRR	25%	20%	50%
	FAR	20%	25%	40%
K = 7	FRR	15%	10%	30%
	FAR	10%	5%	25%
K = 11	FRR	30%	20%	50%
	FAR	35%	30%	55%

Figure 3 below shows a plot for the false rejection rate and the false acceptance rate for the biometric cryptosystem against the key size.

**Figure 3.** FRR and FAR.

7. Analysis

The dwell-in time was used to identify the objects that were chosen by each participant. Any three objects with the highest dwell-in time were shown to be the participant's choice from a list of the fifteen objects that were displayed. From a range of objects displayed on the scene, some objects attracted the participants' attention more so than others. Although the influence of color in the selection of objects is not within the scope of this study, bright colored objects had an influence on the selection of objects. The book was chosen by 50% of the participants as one of their choice for the three objects, followed by the rose and the ball, consecutively.

The performance of the machine learning classifier has been assessed based on the accuracy, precision, true positive rate, false positive rate, and the Receiving Operating Characteristic curve (ROC). As shown in the results for the classifiers under different conditions, they performed slightly differently under different testing conditions. The Naïve Bayes classifier has always performed better regardless of the testing condition used. A 93% accuracy rate was obtained using the 10-fold cross validation with a 0.93 true positive rate. Table 2 below show the performance of different machine learning classifiers based on the tenfold cross validation.

Table 2. Tenfold cross validation.

Classifier	Accuracy	Precision	True Positive	False Positive	ROC
K-Nearest Neighbor (IBK)	90%	0.72	0.71	0.02	0.89
Support vector Machine(SMO)	59%	0.62	0.59	0.02	0.95
KStar	46%	0.48	0.46	0.03	0.89
NaiveBayes	87%	0.93	0.93	0.02	0.86

8. Discussion

The experiment aimed to create a template from these observations that tried to assign a unique binary signature for each enrolled user. Error correction is used in authenticating a user who submits an eye movement sample for enrollment. Being able to uniquely identify individuals from a pool of users is an important aspect of security of computer systems and security in general.

Figure 4 below shows the enrollment, verification and validation process of users in to the biometric system.

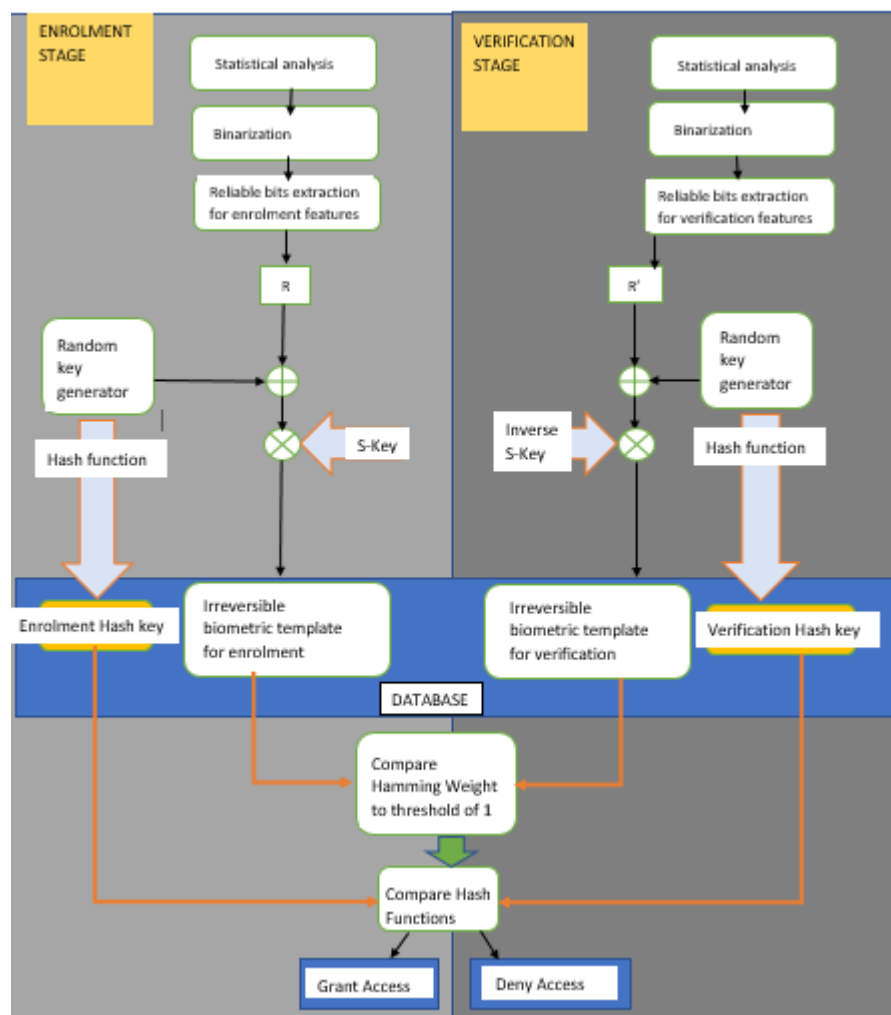


Figure 4. Fuzzy commitment flowchart.

Note that the permutation matrix proposed by [38] is not included in computation as a random key generation adds a heavy computational load to the system in trying to find an invertible $(n \times n)$ permutation matrix with an inverse.

For authentication/verification, a user I submits their eye movement sample, which is binarized using the mean as in the enrollment stage. This sample is drawn randomly from the joint feature vector matrix. For user 1, it is observations 1–30; user 2, observations 31–60; and so on. The helper data are made of the hash value of the encoded message and the variable ADS (User biometric + encoded message * identity matrix). ADS is multiplied with the inverse of identity matrix, and the query biometric sample is then added to obtain a corrupt version of the codeword through reverse arithmetic. The BCH decoder module is then used to decode the corrupt codeword and the hash function taken.

A comparison of the hash value with the one from enrollment opens for the legitimate user.

For additional protection, the hamming distance between the enrollment biometric template of and the query biometric template is used to aid decision by setting a threshold of 1. A legitimate attempt must have both of the following conditions: encoded codeword hash equal to decoded hash, and that maximum hamming distance must be 1 between query and enrollment binary templates.

Some previous works such as [15] measured the same eye movement metrics that we used in our study, but they did not use the same performance evaluation criteria, and therefore it is very difficult to compare the results of this study to other previous works. In comparison to the results to the results obtained in [20], an 83% accuracy rate was obtained during the classification process using the random forest method. Contrary to a study by [39], who conducted a study by measuring the saccadic eye movement signal from 109 young subjects, measured the users eye movement and focused only on measuring one scanpath feature, in our study, an 80–90% correct identification rate was obtained for saccadic eye movements. Based on the size of our data set, the chosen machine learning classifiers chosen were suitable for classifying the data. The number of tasks performed for this study could also be increased for comparison of the results. Collecting data from more participants could have been beneficial in terms of increasing the reliability of the presented results.

9. Conclusions

The main aim and objective of this study was to explore the potential of object selection using eye movement as an effective biometric. The results obtained from this study are very promising and show that it is possible to uniquely identify individuals by the unique features of their eye movement. The results show positive feedback on this study. The results from the machine learning classifiers showed a 93% accuracy rate. The proposed scheme has a 37% FRR and 27% FAR based on the 400 trials, which are very promising results. The results suggest that the scheme would perform better if integrated with another biometric to increase its performance. It is hoped that the ideas and results obtained from this study will advance and contribute to the understanding of eye movement as biometrics and provide some advancements in the eye-movement research field. Currently, the use or acceptance of eye movement biometric is relatively low as some advances in the emerging researches are still growing.

Author Contributions: J.T. performed the conceptualization, methodology, theoretical work, experiments, analyzed the data, designed the work, and drafted the original work. B.D. reviewed, revised, validated, and supervised, and administered the work. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key R&D Program of China under Grants2019YFB1803400, 2020YFB1806405; in part by the National Natural Science Foundation of China under Grant 62071392; in part by the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University (No. ISN21-12); in part by the central government to guide local scientific and technological development under Grant No. 2021ZYD0001; in part by the 111 Project No.111-2-14; in part by U1734209; and in part by the research fund of the Pengcheng Lab under grant PCL2021A04.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data used in this work are available from the corresponding author upon reasonable request.

Acknowledgments: Authors would like to thank the anonymous reviewers for careful reading of the manuscript and providing constructive comments and suggestions which have helped them to improve the quality of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Security Guidance for Critical Areas of Focus in Cloud Computing. 2017. Available online: <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/> (accessed on 1 September 2021).
2. Choudhary, S.K.; Naik, A.K. Multimodal Biometric Authentication with Secured Templates—A Review. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1062–1069. [CrossRef]
3. Ku, W.-C. Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture. *IEEE Trans. Neural Netw.* **2005**, *16*, 1002–1005. [CrossRef] [PubMed]
4. A Novel Image-Based Implicit Password Authentication System (IPAS) for Mobile and Non-Mobile Devices | Elsevier Enhanced Reader. Available online: <https://reader.elsevier.com/reader/sd/pii/S0895717712001719?token=E97B30A5442FBCB6A154DD626D34242AA36B627146593BF0C6F0A69D41C16096FA7268AD66A58970AD3706B503F0123E&originRegion=eu-west-1&originCreation=20210907172958> (accessed on 8 September 2021).
5. Shoulder-Surfing Resistant Graphical Password System | Elsevier Enhanced Reader. Available online: <https://reader.elsevier.com/reader/sd/pii/S1877050915003208?token=9C0C4593D7E5D1C832F49CFB82447A36C0C4B07258D7DE729A59590BE245A6826D75BB3741C6E030AF5C64AA070B440A&originRegion=eu-west-1&originCreation=20210907173231> (accessed on 8 September 2021).
6. Bullée, J.-W.; Montoya, L.; Pieters, W.; Junger, M.; Hartel, P. The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *J. Exp. Criminol.* **2015**, *11*, 97–115. [CrossRef]
7. Irani, D.; Balduzzi, M.; Balzarotti, D.; Kirda, E.; Pu, C. Reverse Social Engineering Attacks in Online Social Networks. In *Detection of Intrusions and Malware, and Vulnerability Assessment*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 55–74. [CrossRef]
8. Bednarik, R.; Kinnunen, T.; Mihaila, A.; Fränti, P. Eye-Movements as a Biometric. In Proceedings of the Scandinavian Conference on Image Analysis, Copenhagen, Denmark, 15–17 June 2005.
9. Kasprowski, P. Human Identification Using Eye Movements. Ph.D. Thesis, Silesian University of Technology, Gliwice, Poland, 2004. [CrossRef]
10. Does Biometric Authentication Hold the Key to a Bright Future or Pandora’s Box? | The Japan Times. Available online: <https://www.japantimes.co.jp/news/2015/11/02/reference/does-biometric-authentication-hold-the-key-to-a-bright-future-or-pandoras-box/> (accessed on 8 September 2021).
11. Dhingra, A.; Kumar, A.; Hanmandlu, M.; Panigrahi, B.K. Biometric Based Personal Authentication Using Eye Movement Tracking. In *Swarm, Evolutionary, and Memetic Computing*; Springer International Publishing: Cham, Switzerland, 2013; pp. 248–256. [CrossRef]
12. Holland, C.; Komogortsev, O.V. Biometric identification via eye movement scanpaths in reading. In Proceedings of the 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–8. [CrossRef]
13. Saeed, K.; Chaki, R.; Cortesi, A.; Wierzchoń, S. Computer Information Systems and Industrial Management. In Proceedings of the 12th IFIP TC 8 International Conference, CISIM 2013, Krakow, Poland, 25–27 September 2013.
14. George, A.; Routray, A. A score level fusion method for eye movement biometrics. *Pattern Recognit. Lett.* **2016**, *82*, 207–215. [CrossRef]
15. Brooks, M.; Aragon, C.R.; Komogortsev, O.V. Perceptions of interfaces for eye movement biometrics. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–8. [CrossRef]
16. Vetter, C. The effects of colors on behavior. Available online: <https://neurofied.com/effects-of-color-on-behavior/> (accessed on 8 September 2021).
17. Riccio, D. A New Gaze Analysis Based Soft-Biometric. In *Mexican Conference on Pattern Recognition, MCPR 2013: Pattern Recognition*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 136–144. [CrossRef]
18. Rigas, I.; Economou, G.; Fotopoulos, S. Human eye movements as a trait for biometrical identification. In Proceedings of the 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 23–27 September 2012; pp. 217–222. [CrossRef]
19. Srivastava, N.; Agrawal, U.; Roy, S.K.; Tiwary, U.S. Human identification using Linear Multiclass SVM and Eye Movement biometrics. In Proceedings of the 2015 Eighth International Conference on Contemporary Computing (IC3), Noida, India, 20–22 August 2015; pp. 365–369. [CrossRef]

20. Holland, C.D.; Komogortsev, O.V. Complex eye movement pattern biometrics: Analyzing fixations and saccades. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–8. [[CrossRef](#)]
21. A Survey of Biometrics Security Systems. Available online: <https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/> (accessed on 9 September 2021).
22. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 4–20. [[CrossRef](#)]
23. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42. [[CrossRef](#)]
24. Sutrop, M. Ethical Issues in Governing Biometric Technologies. In *Ethics and Policy of Biometrics*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 102–114. [[CrossRef](#)]
25. Campisi, P. *Privacy and Security in Biometrics*; Springer: London, UK, 2013. [[CrossRef](#)]
26. The Parameters of Eye Movement. Available online: <https://www.liverpool.ac.uk/~jpccknox/teaching/Eymovs/params.htm> (accessed on 17 September 2021).
27. Data Mining: Concepts and Techniques, 3rd ed. Available online: <https://www.elsevier.com/books/data-mining-concepts-and-techniques/han/978-0-12-381479-1> (accessed on 3 November 2021).
28. Precalculus: A Functional Approach to Graphing and Problem Solving, 6th ed. Available online: <https://www.oreilly.com/library/view/precalculus-a-functional/9780763751777/> (accessed on 3 November 2021).
29. Learn Naive Bayes Algorithm | Naive Bayes Classifier Examples. Available online: <https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained/> (accessed on 17 September 2021).
30. Rish, I. An Empirical Study of the Naive Bayes Classifier. In *IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence*; IBM: New York, NY, USA, 2001.
31. Teoh, A.B.J.; Kim, J. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electron. Express* **2007**, *4*, 724–730. [[CrossRef](#)]
32. Secure Biometric Template Protection via Randomized Dynamic Quantization Transformation | IEEE Conference Publication | IEEE Xplore. Available online: <https://ieeexplore.ieee.org/document/4547645> (accessed on 17 September 2021).
33. Aljazzar, H.; Leue, S. K*. A heuristic search algorithm for finding the k shortest paths. *Artif. Intell.* **2011**, *175*, 2129–2154. [[CrossRef](#)]
34. Data Mining: Practical Machine Learning Tools and Techniques, 3rd ed. Available online: <https://www.elsevier.com/books/data-mining-practical-machine-learning-tools-and-techniques/witten/978-0-12-374856-0> (accessed on 3 November 2021).
35. Noble, W.S. What is a support vector machine? *Nat. Biotechnol.* **2006**, *24*, 1565–1567. [[CrossRef](#)] [[PubMed](#)]
36. Foody, G.; Mathur, A. Toward intelligent training of supervised image classifications: Directing training data acquisition for SVM classification. *Remote Sens. Environ.* **2004**, *93*, 107–117. [[CrossRef](#)]
37. Weka 3—Data Mining with Open Source Machine Learning Software in Java. Available online: <https://www.cs.waikato.ac.nz/ml/weka/> (accessed on 17 September 2021).
38. Chauhan, S.; Sharma, A. Improved fuzzy commitment scheme. *Int. J. Inf. Technol.* **2019**, *6*, 1–11. [[CrossRef](#)]
39. Zhang, Y.; Juhola, M. On Biometrics with Eye Movements. *IEEE J. Biomed. Health Inform.* **2017**, *21*, 1360–1366. [[CrossRef](#)] [[PubMed](#)]