

Article

An Efficient Confidence Interval-Based Dual-Key Fuzzy Vault Scheme for Operator Authentication of Autonomous Unmanned Aerial Vehicles

Jungin Choi ¹ , Juhee Lee ²  and Aeyoung Kim ^{3,*} ¹ Faculty of Liberal Education, Seoul National University, Seoul 08826, Republic of Korea; junginchoi@snu.ac.kr² J.MARPLE, Seoul 06642, Republic of Korea; jhlee@jmarple.ai³ School of Computing and Artificial Intelligence, Hanshin University, Osan 18101, Republic of Korea

* Correspondence: aeyoung.kim@hs.ac.kr

Abstract: The fuzzy vault is an innovative way to share secret keys, combining traditional cryptography with biometrics and biometric template protection. This method forms the basis for the reliable operation of unmanned aerial vehicles (UAVs) through anonymizing drone operators and safely using their data and onboard information. However, due to the inherent instability of biometrics, traditional fuzzy vault schemes face challenges, such as reduced recognition rates with increased chaff points, impractical runtimes due to high-order polynomial reconstruction, and susceptibility to correlation attacks. This paper proposes an efficient fuzzy vault scheme to address these challenges. We generate two secret keys based on biometrics: the first key is produced from the operator's unique features like the face and iris, using a confidence interval; the second key, used to construct a polynomial, is based on what the operator remembers. These dual-key fuzzy vaults enable the stable generation of genuine points during encoding, easy extraction during decoding, and effective operator authentication while maintaining anonymity. Our experimental results demonstrate improved security and secret acquisition accuracy using the AR face database. These results are achieved regardless of increased false vaults, enabling real-time polynomial reconstruction and resilience against correlation attacks. Importantly, our enhanced fuzzy vault scheme allows the application of this secure, real-time authentication process, safeguarding the anonymity of drone operators.

Keywords: fuzzy vault scheme; biometric authentication; template protection; anonymous; confidence interval; operator authentication; autonomous UAVs; security for internet of things



Citation: Choi, J.; Lee, J.; Kim, A. An Efficient Confidence Interval-Based Dual-Key Fuzzy Vault Scheme for Operator Authentication of Autonomous Unmanned Aerial Vehicles. *Appl. Sci.* **2023**, *13*, 8894. <https://doi.org/10.3390/app13158894>

Academic Editor: Gianluca Lax

Received: 1 July 2023

Revised: 26 July 2023

Accepted: 28 July 2023

Published: 2 August 2023



Copyright: © 2023 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

Mutual communication environments based on wired, wireless, and mobile networks give us various service models for convenience in many domains, such as communication, education, banking, payments, entertainment, shopping, etc. Security systems are organized with devices, protocols, algorithms, and various security policies and procedures to apply more powerful security to eliminate vulnerabilities in these service models. Specifically, end-to-end or application layers in the security systems are mainly based on authentication and authorization factors (what users remember, such as a password, and what users have, such as a security card) and modern cryptographic algorithms (e.g., AES, RSA, and ECC). In these systems, the most general thought is that more security is associated with less convenience because security improvements generally require a user to possess and remember additional factors with complicated secret keys. However, these security solutions do not prevent illegal sharing and proxies. These are severe vulnerabilities in which root or increased permissions can be passed to an unauthorized user, such as an attacker, despite a system equipped with robust security solutions. Fortunately, adding biometrics to an authentication system and biometrics-based keys to cryptographic algorithms have become good solutions for added security in any system [1–5].

Applying biometrics to a general cryptographic algorithm-based security system protects against illegitimate sharing and proxies while improving security and usability [6]. Although using biometrics confers a significant security advantage, combining them with traditional cryptographic algorithms because all acquired biometrics from a sensor have different bit sequences, while those in a cryptographic key are the same. The fusion of biometrics and cryptography—using biometric features in conventional cryptographic algorithms—is generally referred to as bio-cryptography, and there has been increasing interest in this concept [7–9]. The initial purpose of bio-cryptography is to protect the biometrics themselves, and recently, the technique has been extended to the generation and sharing of a biometrics-based secret key [10–13]. Two general approaches exist to the relationship between a biometric and its secret key: key binding and key generation. In key generation, the secret key is generated from biometrics, which includes biometric information; however, in the key binding approach, the secret key is generated from another resource or by a cryptographic mechanism, so it does not include any information from biometrics. Only biometrics is used to hide it by binding, shielding, etc. Whereas notable solutions, such as the fuzzy vault scheme, have been proposed as key binding solutions, applicable key generation schemes have not yet been proposed—despite several attempts—to the best of our knowledge [7].

The fuzzy vault scheme is the most practical key binding scheme based on the polynomial reconstruction problem [13]. Some researchers have applied it to protect biometric templates because they are irreplaceable. The template is hidden in the polynomial in the fuzzy vault for biometric template protection. Well-known fuzzy vault schemes are mainly based on fingerprints [14–18]. In addition to fingerprints, the fuzzy vault for variable biometrics such as faces, irises, signatures, and palmprints has also been proposed [19–25]. To improve it for template protection, some researchers have extensively studied applying (1) cancellation with periodic transformation, (2) multimodal with more than two biometrics such as fingerprints, hand veins, face, palm veins, and so on, (3) lattice masks for providing several requirements (e.g., diversity and revocability) without the error correcting code, (4) smart card environments considering automatic fingerprint alignment, verification accuracy, template size, and (5) chaotic system-based multimodal considering the forgery, a significant difference of intra-class, and the security of unimodal biometric leakage [26–32].

Others have used it to share secret information or a secret key with conventional cryptography. Originally A. Juels and his colleagues also introduced their scheme focusing on secret sharing or key distribution [13]. Many modified fuzzy vault schemes that use various biometric features (e.g., face, iris, or signature) have since been proposed based on this preliminary version and have tried various strategies to improve their performance [5,33–37]. More recently, there have been attempts at applying a biometric cryptography scheme to physical unclonable function (PUF) [38], Body Area Networks (BAN) [2,39–43], Electrocardiogram (ECG) [44], or wireless networks for symmetric key distribution through the transformation of fuzzy vault schemes.

With each application, researchers have sought to improve the security, efficiency, or practicality of the fuzzy vault scheme; however, several problems still need to be solved [45,46]. There is a drop-off in recognition rates when the number of chaff points increases, the runtime of higher order polynomial reconstruction is unrealistic for real-world applications, and the scheme remains vulnerable to a correlation attack [47–49]. In this paper, to solve these problems, we focus on the improved fuzzy vault for key or secret sharing.

Significantly, our enhanced fuzzy vault scheme paves the way for the practical implementation of a secure, real-time authentication process, safeguarding the anonymity of drone operators for unmanned aerial vehicles (UAVs) you can trust. In the context of drone operation, where secure control and data privacy are paramount, our proposed system can authenticate operators securely and swiftly while maintaining their anonymity. This proposed implementation acknowledges the importance of ensuring security without

sacrificing operator convenience and privacy. The anonymous operator authentication enabled by our enhanced fuzzy vault scheme demonstrates the potential of biometric cryptography in the increasingly prominent field of drone technology.

The organization of this paper is as follows: Section 2 introduces the fuzzy vault scheme for binding biometric templates and sharing secret keys, Section 3 describes a genuine point generation scheme based on confidence interval analysis and uses it to improve the practicality of the fuzzy vault scheme, and Section 4 presents the analyzed result of it and compares the differences from the existing quantum modular adder. Finally, Section 5 presents conclusions.

2. Related Works

The Fuzzy Vault Scheme

The fuzzy vault scheme is the most popular key-binding-based bio-cryptographic algorithm. It can help share secret information such as a password, PIN, or short key for protecting biometric templates. The key in a conventional cryptographic algorithm has the same bit sequence every time it is used. However, biometric features have a different bit sequence at every sensor reading, making it almost impossible to generate a conventional cryptographic key from biometric features. Instead of devising a key generation scheme from biometrics, the fuzzy vault scheme is an alternative solution for applying biometric-based security advantages to existing cryptography by binding the secret key with biometric features.

The fuzzy vault scheme, proposed by Juels and Sudan [13], is a biometric cryptosystem based on the polynomial reconstruction problem and error-correcting codes. It is an improvement on the previous research by Juels and Wattenberg [12]. Since its creation, more practical fuzzy vault schemes have been proposed by many researchers; a representative work is the fingerprint-based fuzzy vault scheme proposed by Uludag et al. [14,15].

Juels and Sudan's fuzzy vault scheme consists of LOCK and UNLOCK algorithms that encode and decode a secret message using biometric features same as Algorithms 1 and 2. The parameters are a finite field F of cardinality q , a constructed polynomial $P(x)$, polynomial degree k , a number of genuine points t , a number of chaff points r , the number of all points $n(k \leq t \leq r < n < q)$, a secret S , biometric features $f = \alpha_1, \dots, \alpha_t$ and $f' = \alpha'_1, \dots, \alpha'_t$ ($t \leq t'$), a set of genuine points $G = (\alpha_1, p(\alpha_1)), \dots, (\alpha_t, p(\alpha_t))$, a set of chaff points $C = (\alpha_1, y_1), \dots, (\alpha_r, y_r)$, a set of all points $R = (\alpha_1, p(\alpha_1)), \dots, (\alpha_t, p(\alpha_t)), (\alpha_{t+1}, y_{t+1}), \dots, (\alpha_n, y_n)$ when $n = t + r$, and a set of candidate points $Q = (\alpha'_1, y'_1), \dots, (\alpha'_t, y'_t)$.

Algorithm 1: Locking Algorithm in Juels and Sudan's Fuzzy Vault Scheme

input : A secret S and biometric features f

output: A set of all points R

- 1 Initialize R to 0;
 - 2 Construct $P(x)$;
 - 3 The secret S is divided into $s_0, \dots, s_{k-1}$ and encoded in coefficients of $P(x) = s_0 + s_1x^1 + \dots + s_{k-1}x^{k-1}$;
 - 4 Generate G ;
 - 5 G is the output of the polynomial projection $(\alpha_1, p(\alpha_1)), \dots, (\alpha_t, p(\alpha_t))$ by calculating $P(x)$ with f , for which each element is an input of $P(x)$. The cardinality of G is t , and every element in G is a genuine point on the polynomial;
 - 6 Generate C ;
 - 7 $\alpha_i \in F_q$ and $y_i \in F_q$ ($t+1 \leq i \leq n, n = t+r$) are randomly picked. It is checked whether $\alpha_i \notin f$ and $y_i \notin p(\alpha_1), \dots, p(\alpha_t)$. If not, choose and check a random number repeatedly. Every (α_i, y_i) in $C = (\alpha_1, y_1), \dots, (\alpha_r, y_r)$ is a chaff point that does not lie on $P(x)$;
 - 8 Return R as a permutation of G and C ;
-

Algorithm 2: Unlocking Algorithm in Juels and Sudan's Fuzzy Vault Scheme**input** : A set of all points R and biometric features $f' = \alpha_1', \dots, \alpha_{t'}'$ **output**: A secret S

- 1 Initialize Q to 0;
- 2 Extract candidate genuine points from R by using f' ;
- 3 Every element in R is compared with f' . For $i = 1, \dots, t'(\alpha_j, y_j)$ ($1 \leq j \leq t'$) as a candidate for a genuine point in R is found when $\alpha_j \approx \alpha_i'$, i.e., $|\alpha_j - \alpha_i'| < \varepsilon$, and added to Q ;
- 4 Reconstruct $P'(x)$;
- 5 The candidate polynomial $P'(x)$ is reconstructed with Q using the Reed-Solomon decoding algorithm, an error-correcting code in network communications, to recover S correctly. If an attacker tries to reconstruct $P'(x)$ without any biometric information from f' , the number of cases required to calculate $P'(x)$ is $C(n, k+1)$, where $n = t + r$, which is the complexity of the fuzzy vault scheme;
- 6 Return S' as the coefficients in $P'(x)$;

After the introduction of the fuzzy vault scheme, Uludag [14] proposed a more practical version with fingerprints. Many modified fuzzy vault schemes have since been proposed based on these preliminary versions. Some of these have been analyzed, and their efficiency or security vulnerabilities compared [47–49].

In these previous works, researchers have encountered the problems of decreasing recognition rates with increasing chaff points, practical implementation of polynomial reconstruction using Reed–Solomon decoding, and correlation attacks that reconstruct a polynomial by exploiting the similarity of biometric features [17,18,35,36,45,50]. In this paper, we are mainly focused on some issues as follows:

- Decreasing recognition rate with increasing chaff points
The fuzzy vault scheme is based on the polynomial reconstruction problem, which cannot determine polynomial $P(x)$ without $k+1$ genuine points, where k is the degree of $P(x)$. The security of vault construction via $P(x)$ for hiding secret S depends on the number of chaff points used [13], though increasing this number creates a trade-off between security and usability. To find the $k+1$ genuine points in UNLOCK, if $\alpha_i' \in f'$ satisfies $|\alpha_j - \alpha_i'| < \varepsilon$ where $\alpha_j \in f$, point α_j can be recognized as a candidate for a genuine point from vault R . If the $k+1$ candidate points are recognized as elements of Q , the polynomial can be constructed successfully, and secret S' recovered because $P'(x) = P(x)$ and $S' = S$. However, if the number r of chaff points in $C \subset R$ is increased to improve security, more chaff points (α_i, y_i) exist that may satisfy $|\alpha_j - \alpha_i'| < \varepsilon$ and be misrecognized as genuine points despite having valid biometric features as follows: $\{(\alpha_i, y_i) \notin G\} \wedge \{(\alpha_i, y_i) \in C\}$ ($1 \leq i \leq t$)
- Practical implementation of polynomial reconstruction using Reed–Solomon decoding
The Reed–Solomon decoding algorithm confirms that $P'(x) = P(x)$. The complexity of validating this is $C(t', k+1)$ in the UNLOCK algorithm. To find a valid polynomial, the calculation is run $C(t', k+1)$ times in the worst case. If the cardinality t' of Q is larger, the complexity increases, and the scheme's usability is reduced. In previous work on this problem, Y. J. Lee et al. [25], Q. Li et al. [45], and H. Liu et al. [46] have prescribed that special use of Reed–Solomon decoding in the UNLOCK algorithm is not appropriate.
- Correlation attacks to reconstruct a polynomial using the similarity of biometric features
If an attacker can acquire biometric features $f'' \approx f$ or $f'' \approx f'$, given $f'' = \alpha_1'', \dots, \alpha_{t''}''$, where $t + r \leq t''$, the attacker can determine $Q, P'(x), S'$. Features f'' can be generated or cracked; the attacker can generate random numbers for t'' points and use these to create f'' , or she can crack similar biometric features to serve as f'' . In either case, the

attacker can calculate $P'(x)$ by including $k + 1$ candidate points in f'' . This problem also increases when the number of chaff points increases because more similar points exist. Many researchers, not only those studying fuzzy vaults, have tried to solve the correlation attack problem with cancelable biometrics.

Researchers have also tried to solve these problems and improve the security of the fuzzy vault scheme by increasing the number of chaff points generated by using efficient methods [35,36]. However, these attempts have yet to be successful.

3. Confidence Interval-Based Fuzzy Vaults

The proposed confidence interval-based fuzzy vault scheme is a bio-cryptography scheme based on key binding that uses helper data extracted by confidence intervals from biometrics. This scheme is modeled on the fuzzy vault [13] and the fuzzy fingerprint vault [14,15]. Features of the proposed method that differentiate it from previous versions include a significant goal and stored target, a controlled number of feature points, and candidate polynomial reconstruction attempts. The proposed scheme aims to protect private information or secret keys for secure sharing using biometrics. Bio-cryptographic schemes have two major aims, including the fuzzy vault scheme. The first is protecting biometrics, as they are finite identification information. If registered and used biometrics are exposed, they become useless. For this reason, many biometrics researchers are concerned with this goal. The second is to protect or share a secret key, which is very important in cryptographic algorithms using biometrics. This goal can be accomplished by binding the key with biometrics or generating the key from biometrics. Key generation techniques are rarely proposed because of the difficulty in implementing them.

This paper aims to protect a secret key for secure sharing by binding it with biometrics. The biometrics in this scheme are considered public rather than secret or private information because traces of the biometrics themselves or derived data persist. Therefore, biometrics can be transmitted via networks, such as between 2 and 7 in Figure 1. The target stored in a secure token or database (1 and 6 as shown in Figure 1) is a set of confidence intervals, in contrast with the vaults in the previous scheme. The set of confidence intervals is generated using the *t*-test-based prediction scheme described in [50] and used to calculate the genuine vaults. Extracted biometrics features (2 in Figures 1 and 2a) are input into the set in the security token or database (1 in Figure 1), and the genuine vaults (3 in Figures 1 and 2b) are output as a calculation result from the secure area 1.

The number of feature points can be ensured to be of polynomial order in the proposed scheme. The number of features for polynomial reconstruction and pieces in the secret key is one more than in polynomial order. This is always satisfied because the features are extracted by principal component analysis (PCA), which effectively increases the polynomial order and secret size by any desired amount.

In previous works, the number of reconstruction attempts for the candidate polynomial is one compared to $C(t', k + 1)$ times. If 1 is equal to 6 and 2 is identical to 7 in Figure 3, 3 as a calculation result of the input is equal to 8, which will be used for reconstruction. The genuine points are generated by these data (8 in Figure 1) and the polynomial (4 in Figure 1). Then, the genuine points on the polynomial are mixed with chaff points, which are not on the polynomial. The mixed result is a vault (5 in Figure 1); vaults are then transmitted for decoding. In the decoding stage, genuine points (10 in Figure 3) are easily extracted from the vaults using the data from 8 in Figure 3. The extracted genuine points are used to reconstruct the original polynomial (11 in Figure 3).

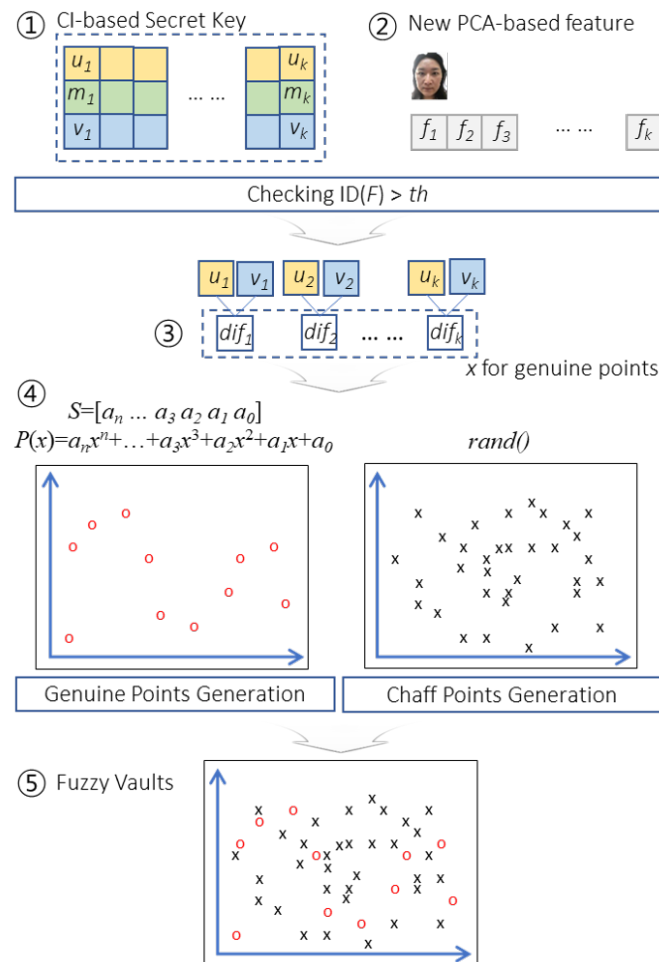
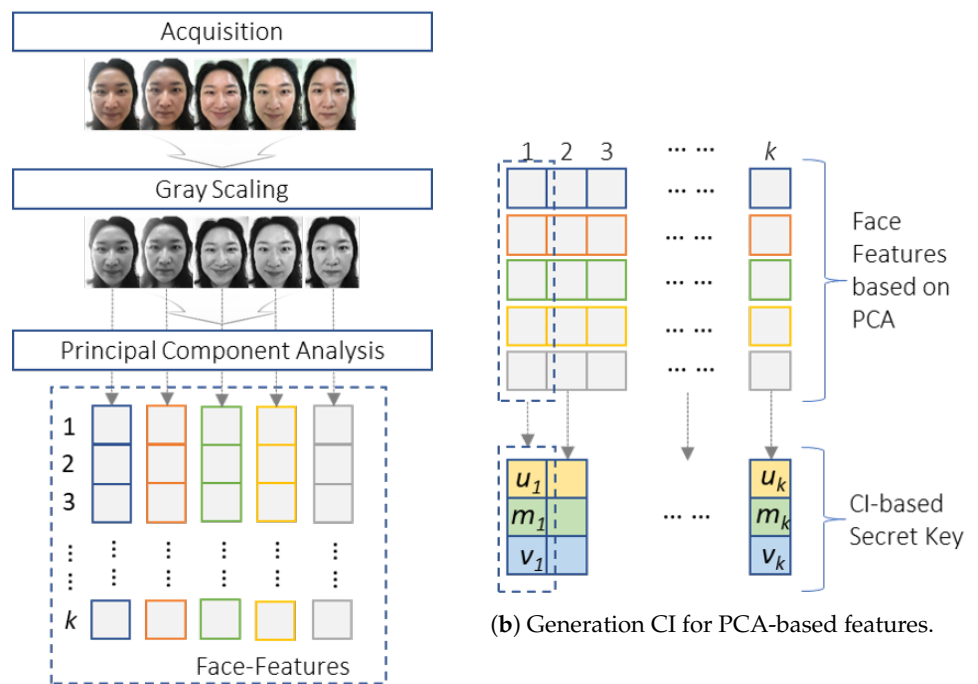


Figure 1. The proposed confidence interval fuzzy vault scheme: LOCK.



(a) Extracting face features based on PCA.

Figure 2. Extracting PCA-based face features and Generation CI.

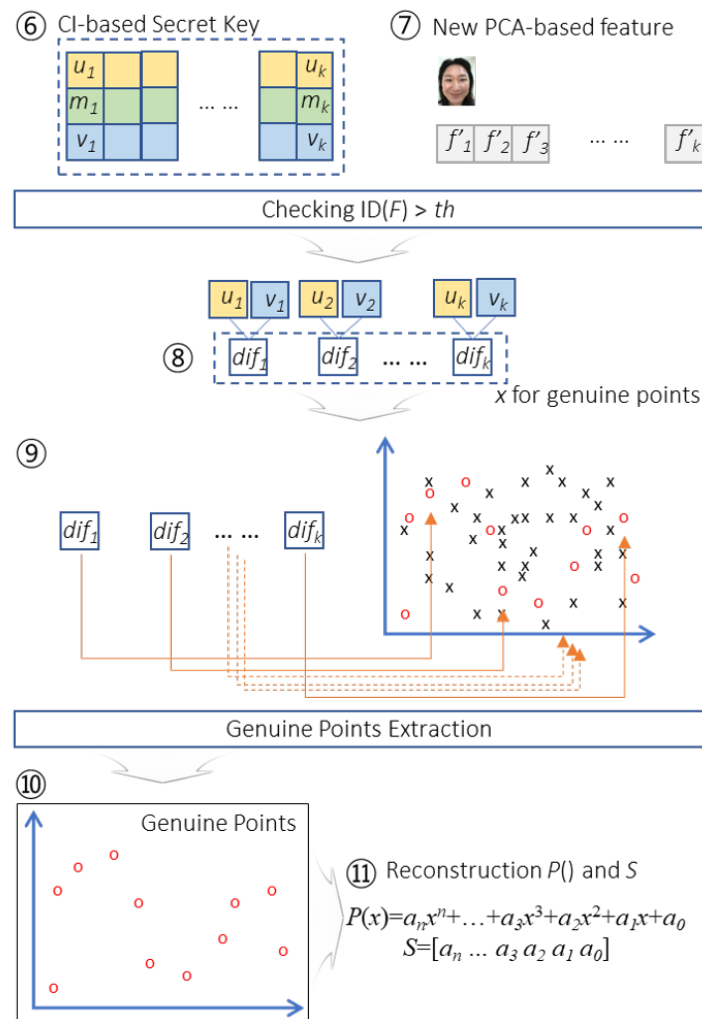


Figure 3. The proposed confidence interval fuzzy vault scheme: UNLOCK.

Algorithms 3 and 4 are composed of two parts: the encoding stage for locking the secret into the biometrics and the decoding stage for unlocking the secret from the biometrics by the polynomial using confidence intervals. The encoding and decoding algorithms are as follows:

Algorithm 3: Encoding (Locking The Secret Key) Algorithm.

input : a secret key S and features $F = f_1, \dots, f_t$
output: a set V of vectors (x_i, y_i) where $i = 1 : (k + r + 1), x_i, y_i \in F_q$

```

1  $V, X \leftarrow \emptyset$ ;
2 if  $ID(F) > th$  then
3   for  $i = 1$  to  $k + 1$  do
4      $dif_i \leftarrow abs(u_i - v_i)$ ;
5      $x_i \leftarrow sin(dif_i)$ ;
6      $X \leftarrow X \cup x_i$ ;
7   end
8    $DS(S)$ ;
9   for  $i = 1$  to  $k + 1$  do
10     $(x_i, y_i) \leftarrow (x_i, P(x_i))$ ;
11    if  $x_i \notin X$  then
12       $V \leftarrow V \cup (x_i, y_i)$ ;
13    else
14       $i \leftarrow i - 1$ ;
15    end
16  end
17  for  $i = 1$  to  $r$  do
18     $x_i \leftarrow rand()$ ;
19     $(x_i, y_i) \leftarrow (x_i, P(x_i))$ ;
20    if  $x_i \notin \{X_j \mid (x_j, y_j)\}$  where  $j = 1 : i$  then
21       $V \leftarrow V \cup (x_i, y_i)$ ;
22    else
23       $i \leftarrow i - 1$ ;
24    end
25  end
26  return  $V$ ;
27 else
28   return 0;
29 end

```

Algorithm 4: Decoding (Unlocking The Secret Key) Algorithm.

input : a set V of vectors (x_i, y_i) where $i = 1 : (k + r + 1)$ and features $F = f_1', \dots, f_t'$

output: a secret key S

```

1  $X, G \leftarrow \emptyset$ ;
2 if  $ID(F) > th$  then
3   for  $i = 1$  to  $k + 1$  do
4      $dif_i \leftarrow abs(u_i - v_i)$ ;
5      $x_i \leftarrow sin(dif_i)$ ;
6      $X \leftarrow X \cup x_i$ ;
7   end
8   for  $i = 1$  to  $k + 1$  do
9     if  $x_i \in V$  then
10       $G \leftarrow G \cup (x_i, y_i)$ ;
11    end
12  end
13   $RP(G)$ ;
14   $S \leftarrow C_1 \parallel \dots \parallel C_k$ ;
15  return;
16 else
17   return 0;
18 end

```

4. Experimental Results

Experiments were conducted to evaluate the performance of the confidence-interval-based fuzzy vault scheme. To assess its effectiveness in a bio-cryptographic system, we used faces [51] and implemented them in MATLAB R2023a on a computer with a 3.40 GHz CPU (i7-3770), 8 GB RAM, and 64-bit Windows. For these experiments, the proposed scheme assumed that the confidence interval set for each of the 50 subjects was generated from qualifying face images. There are originally five face images in the database per subject, three to four of which were used to generate a confidence interval set. Qualifying faces underwent PCA, the most basic preprocessing method for dimension reduction and feature extraction in recognition schemes [52,53]. The threshold value for classifying a face as qualified is a recognition rate of 50% by PCA and our previous works based on the confidence interval [50,53].

The set of confidence intervals is organized by the generation algorithm of the t -test-based prediction scheme shown in [50]. The confidence interval set has cardinality equal to the number of features and is saved in a secure token or database on the client and a server through a secure channel. This set calculates x_i , generating the genuine points to share the secret key. The genuine points in the proposed scheme result from calculating the difference between the upper and lower bounds of the saved confidence intervals. Before this calculation, this scheme has to check whether each PCA-based feature from an acquired face is under the upper bound and over the lower bound. Suppose the including rate is over the threshold, a system parameter for decision by $ID(F) > th$ in the encoding and decoding algorithms. In that case, access to the confidence interval is allowed for calculating the genuine points. Otherwise, it is not permitted, and we cannot calculate them. The confidence interval is stable information and equal data on the encoding and decoding side. And so, the genuine points generated by this confidence interval set in encoding are also completely the same as with the genuine points in decoding. In this proposed system, the confidence interval set is the key to solving the previous problems.

The genuine points based on it can increase chaff points without decreasing the recognition rate, encoding and decoding time, and increasing the risk of correlation attacks.

Figure 4 shows an example confidence interval set marked on the bar graph, with features from acquired faces marked with a circle for 20 principal components. Using more principle components is also possible because the face is a high-dimension trait for extracting enough features. In our previous work, we tested the number of principal components with AR Face DB for quality assessment [51] and used 20 principle components. The bar graph consists of upper and lower bounds. The i -th bar represents the confidence interval of the i -th feature in several qualified faces for confidence interval registration, such that $1 \leq i \leq 20$. In the example, non-satisfied features, which are under the lower bound or over the upper bound, are the 2nd, 3rd, 5th, 7th, 9th, 11th, and 14th bars, respectively. In decoding, the satisfaction rate of the acquired face is 65% (13/20) and allows the use of the confidence interval set if the threshold is 50%.

Figure 5 shows an example of the difference from the confidence interval set. The values are calculated regarding the difference between the upper and lower bounds by $dif_i \leftarrow abs(u_i - v_i)$ in the encoding and decoding algorithm. Figure 6 shows an example of a normalized difference with a range from -1 to 1 , normalized from the original ranges shown in Figure 5 by the function $\sin()$. That is because the original ranges are not appropriate to be input values for polynomials with a high degree.

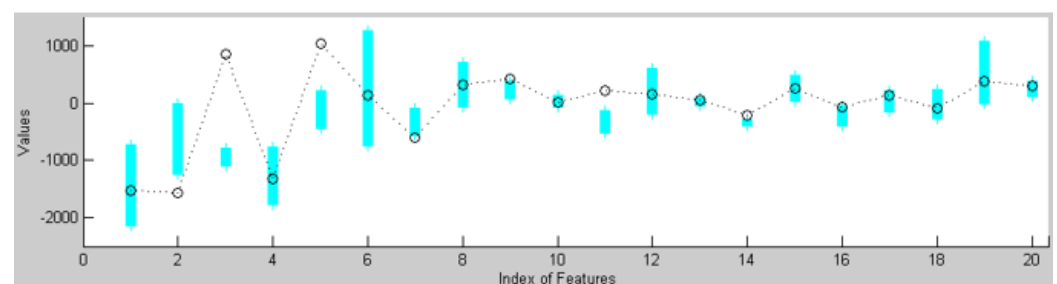


Figure 4. Example of the CI and the newly acquired face where $k = 20$.

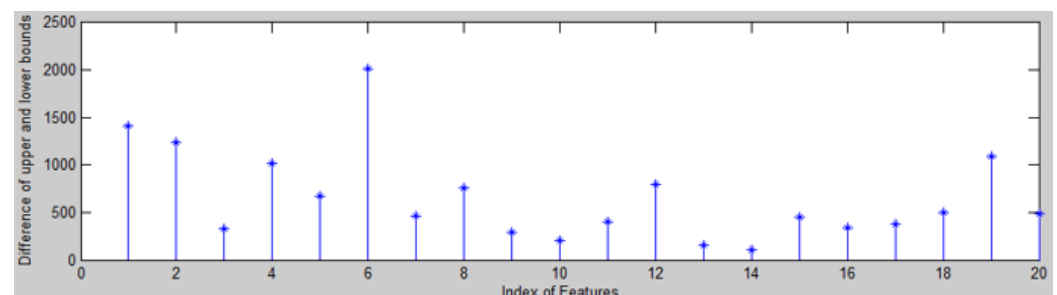


Figure 5. Example of differences of upper and lower bounds of the confidence interval set.

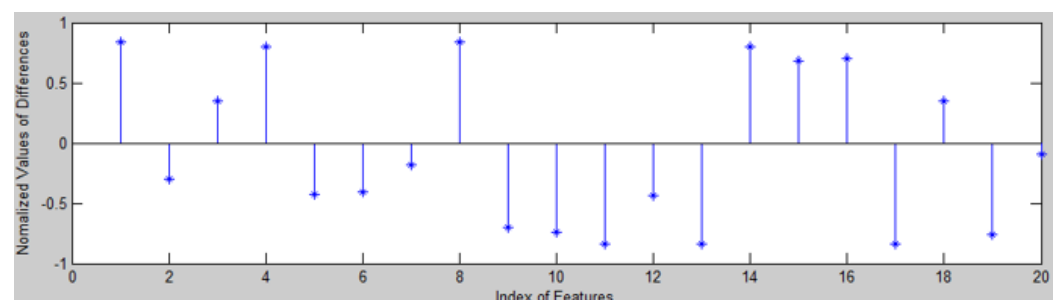


Figure 6. Example of normalized difference values.

To investigate the distribution of vaults by using difference values, the normalized difference, marked with circles shown in Figure 7, is made by the representation of the difference shown in Figure 6. Here, the X-axis is for difference values before normalization, and the Y-axis is for normalized different values. The genuine points are generated with these normalized difference values. The total vaults in the proposed scheme will consist of $k + 1$ genuine points from them and r chaff points from random numbers, where $r \gg k$.

Other values for the chaff points in Figure 8, marked with X, are made by representatives of r random numbers generated by the function *rand()*. Figure 8 shows the distribution with 1000 random numbers ($r = 1000$) included in the vaults, whereas Figure 9 shows a case including 200 random numbers ($r = 200$). Although the chaff points from these random numbers are increased to 1000 in Figure 8 from 200 in Figure 9, the secret S can be successfully shared without a significant increase in execution time, even as the security to protect the secret S is enhanced. That is because this increase causes an increase in the complexity to crack the genuine points by brute force attack: to $C(1020, 9)$ from $C(220, 9)$ in these examples.

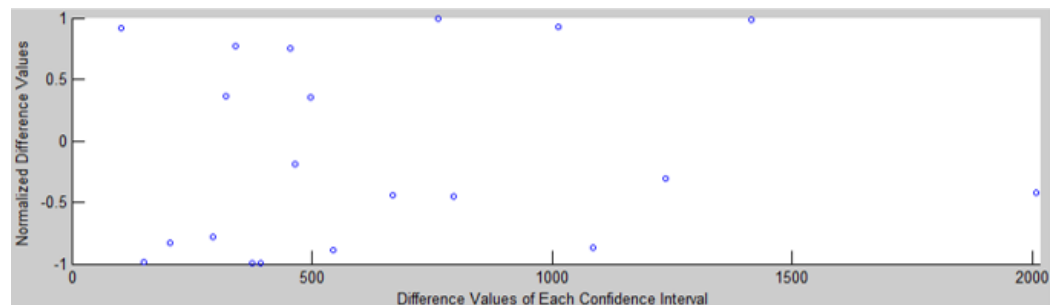


Figure 7. Example of normalized difference values for genuine points.

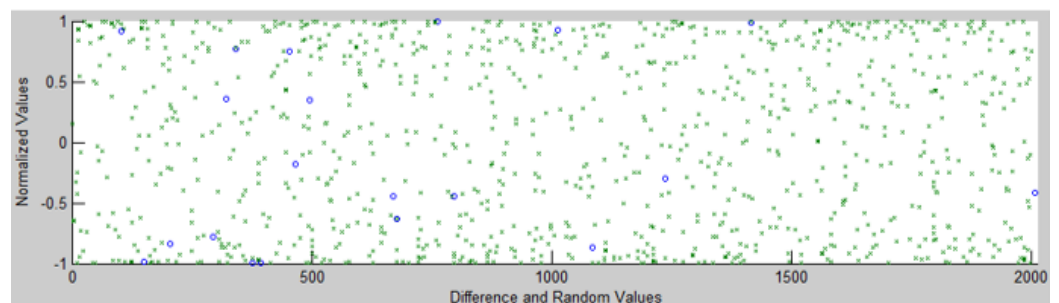


Figure 8. Example of 20 normalized difference values for genuine points with 1000 random numbers for chaff points.

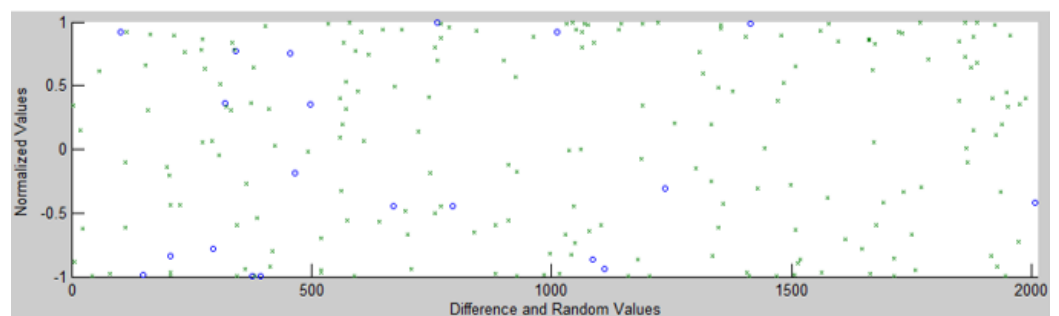


Figure 9. Example of 20 normalized difference values for genuine points with 200 random numbers for chaff points.

Accuracy, complexity against attack, and performance time are assessed by varying the parameters used, such as k for the degree, r for the number of chaff points, and S for

the secret key. Accuracy depends on the secret S obtained from the decoding stage. The proposed scheme's accuracy is 1, and the FAR (False Accept Rate) and FRR (False Reject Rate) are 0.

The complexity, which is the number of exhaustive searches for an attacker to determine S , is calculated as in Uludag et al. [7]. In their research, the complexity is an average of 5.3×10^{10} evaluations for vaults containing 218 points (18 genuine, 200 chaff), and the number of elements for the polynomial reconstruction is nine. In previous studies, it was challenging to increase the degree or the number of chaff or genuine points, although doing so increased the complexity of the fuzzy vault.

However, in our experiments, it is easier to increase this number. For a case with 220 points (20 genuine, 200 chaff) and nine elements of the polynomial with degree 8, there are a total of $C(220, 9) = 2.8 \times 10^{10}$ combinations. Only $C(20, 9) = 167,960$ of these combinations will unlock the vault and reveal the secret. Therefore, the complexity is $C(220, 9)/C(20, 9) = 1.7 \times 10^{10}$ evaluations for an attacker to crack the vault. For a case with 220 points and 13 polynomial elements with degree 12, the complexity is $C(220, 13)/C(20, 13) = 4.1 \times 10^{15}$. The complexities for degrees 8 and 12 for a case with 1020 points are $C(1020, 9)/C(20, 9) = 1.9 \times 10^{16}$ and $C(1020, 13)/C(20, 13) = 2.5 \times 10^{24}$, respectively. A higher degree or more chaff points leads to greater complexity. This greater complexity indicates the number of operations in unlocking that an attacker has to perform, and it means that an operation without the user's biometric features cannot extract a secret key from the vaults within polynomial time, indicating that the security strength is high.

Figure 10 shows encoding and decoding times based on the polynomial degree and the number of chaff points in the box plot. Each box shows distributions of running time in encoding and decoding among polynomial degrees 6 to 12 where chaff points are the same. The same colored box is a pair; one in encoding time and the other in decoding time. Encoding time with the lock algorithm increases with the number of chaff points for generating them, but there is no significant decoding time with the unlock algorithm based on confidence interval. Then, the number of chaff points does not affect the decoding time. Such running time between encoding and decoding shows little difference compared to the existing fuzzy vault execution time according to the increase in chaff points.

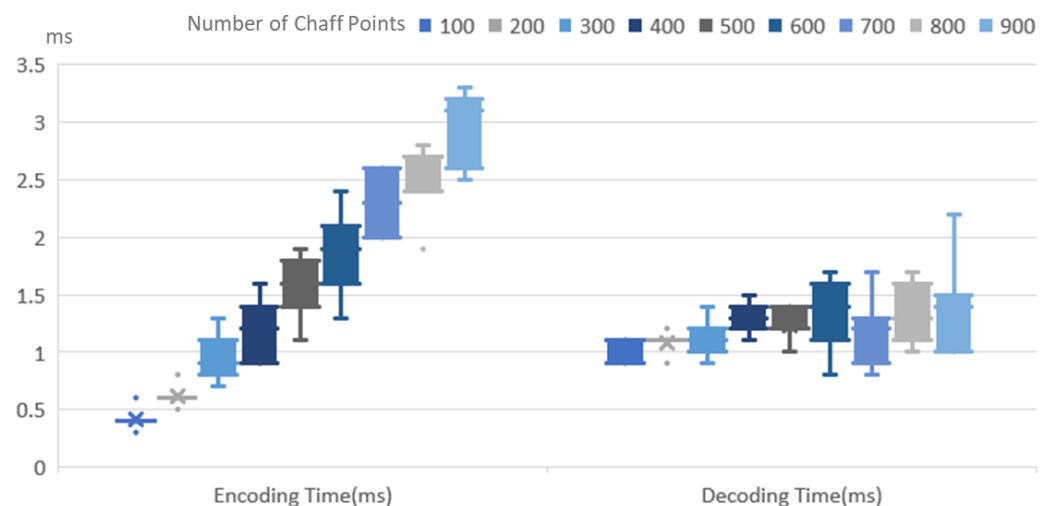


Figure 10. Encoding and decoding time by degree and number of chaff points.

Table 1 compares the performance with the latest research including execution time by Yang, J. et al. [38]. Yang's execution time for both encoding and decoding, like the results of other fuzzy vault schemes, increases according to the increase in the polynomial degree and the number of chaff points. The combination of evaluation for unlocking the secret key in decoding by Yang's is $C(k + m, d + 1)$ in Table 2, but ours is $C(k, d + 1)$ and unaffected by the number of chaff points. On the other hand, in both schemes, the number

of combinations that an attacker without correct information from the user's biometrics has to calculate to guess the secret key is the same, $C(k + m, d + 1)$.

Table 1. Comparison of the performance with the latest research by Yang, J. et al. [38].

	Genuine Points (k)	Chaff Points (m)	Degree of Polynomial (d)	Lock Time (ms)	Unlock Time (ms)
[38]	40	100	20	706.3	<25,000
	40	300	12	593.8	<5000
	40	500	20	1209.6	<50,000
Ours	20	100	8	0.4	0.9
	20	500	8	1.4	1.2
	20	1000	8	1.5	1.5
	20	1000	10	3.6	1.1
	20	1000	12	3.8	1.5

Table 2. Comparison of the Unlock strategy and complexities with the latest research by Yang, J. et al. [38].

	Unlock Strategy	Evaluation Complexity	Guessing Complexity
[38]	Iterated Lagrange with Von Neumann	$C(k + m, d + 1)$	$C(k + m, d + 1)$
Ours	Iterated Lagrange with Confidence Interval	$C(k, d + 1)$	$C(k + m, d + 1)$

5. Conclusions

The fuzzy vault scheme is a breakthrough in secure key sharing, seamlessly integrating traditional cryptography with biometric techniques and template protection. This strategy underpins the secure and anonymous usage of drone operators' information. Nevertheless, due to the inherent noise and variability in biometrics, conventional fuzzy vault schemes have been plagued with challenges, including declining recognition rates as chaff points increase, unrealistic runtimes attributed to high-order polynomial reconstruction, and susceptibility to correlation attacks. This paper introduces an enhanced version of the fuzzy vault scheme to tackle these issues. We employ a dual-key approach based on biometric features: the first key is derived from unique operator attributes, such as facial and iris patterns, utilizing confidence interval; the second key, essential for creating a polynomial, is based on what the operator can recall. This dual-key fuzzy vault system facilitates the consistent generation of genuine points in the encoding phase, simplifies extraction during decoding, and assures effective authentication of operators while preserving their anonymity. Importantly, our proposed system has the potential to bring a secure, real-time authentication process to the forefront of drone operations, ensuring the operators' anonymity.

Our experimental results, drawn from testing with the AR face database, exhibit improved security and increased accuracy in secret acquisition. Notably, we observed that the encoding and decoding time of the fuzzy vault was at most 3.5 ms across vault sizes ranging from 100 to 1000. Furthermore, the decoding time remained stable despite increasing chaff points, underscoring the system's capacity for real-time polynomial reconstruction and resilience against correlation attacks.

These advancements persist regardless of an increase in false vaults, highlighting the robustness of our enhanced fuzzy vault scheme. More importantly, the efficiency and stability of the improved fuzzy vault scheme, coupled with its capacity to withstand real-time demands, make it highly suitable for authenticating drone operators in real-world drone deployments. It provides a secure method for operators to authenticate themselves while maintaining anonymity, thus presenting a tangible solution to drone operators' security and privacy challenges. This substantial development in bio-cryptography not only signifies a future where security, efficiency, and user convenience can harmoniously

coexist, but it also demonstrates a practical application of these principles in the burgeoning field of drone technology without compromising the essential aspect of real-time response.

However, this technique still includes information that needs to be memorized, such as passwords, and thus has limitations in providing authentication that satisfies security and convenience at the same time. Fuzzy extractor, another technique of the bio-cryptosystem, is a method of generating a password and a secret key purely from biometric information, but in the previously proposed scheme, the process is very complicated, and the information to be stored is very large in GB and TB units, making it difficult to use realistically. Therefore, future research will move toward generating passwords or secret keys from biometric information like fuzzy extractor based on the results of this research but designing a lightweight technique that can be applied to IoT devices, including UAVs.

Author Contributions: Conceptualization, A.K.; methodology, A.K. and J.L.; software, A.K. and J.C.; validation, J.C., A.K. and J.L.; formal analysis, A.K.; investigation, J.C., A.K. and J.L.; resources, A.K.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, J.C., A.K. and J.L.; visualization, J.L.; supervision, A.K.; project administration, A.K.; funding acquisition, A.K. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding: Basic Science Research Program supported this research through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2020R1I1A1A01071768) and the Korea Agency for Infrastructure Technology Advancement (KAIA) grant funded by the Ministry of Land, Infrastructure and Transport, the Ministry of Science and ICT, and the Ministry of Trade, Industry and Energy (22DPIW-C153691-04).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Tuyls, P.; Akkermans, A.H.; Kevenaar, T.A.; Schrijen, G.J.; Bazen, A.M.; Veldhuis, R.N. Practical biometric authentication with template protection. In Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication, Hilton Rye Town, NY, USA, 20–22 July 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 436–446.
2. Mahendran, R.K.; Velusamy, P. A secure fuzzy extractor-based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Comput. Commun.* **2020**, *153*, 545–552. [\[CrossRef\]](#)
3. Kaur, P.; Kumar, N.; Singh, M. Biometric cryptosystems: A comprehensive survey. *Multimed. Tools Appl.* **2022**, *82*, 16635–16690. [\[CrossRef\]](#)
4. Patil, S.D.; Raut, R.; Jhaveri, R.H.; Ahanger, T.A.; Dhade, P.V.; Kathole, A.B.; Vhatkar, K.N. Robust authentication system with privacy preservation of biometrics. *Secur. Commun. Netw.* **2022**, *2022*, 7857975. [\[CrossRef\]](#)
5. Wesley, A.B. Authentication-based multimodal biometric system using exponential water wave optimization algorithm. *Multimed. Tools Appl.* **2023**, *82*, 30275–30307.
6. Jain, A.K.; Ross, A.; Pankanti, S. Biometrics: A Tool for Information Security. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 125–143. [\[CrossRef\]](#)
7. Uludag, U.; Pankanti, S.; Prabhakar, S.; Jain, A.K. Biometric cryptosystems: Issues and challenges. *Proc. IEEE* **2004**, *92*, 948–960. [\[CrossRef\]](#)
8. Xi, K.; Hu, J. Bio-cryptography. In *Handbook of Information and Communication Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 129–157.
9. Rathgeb, C.; Uhl, A. A Survey on Biometric Cryptosystems and Cancelable Biometrics. *EURASIP J. Inf. Secur.* **2011**, *2011*, 3. [\[CrossRef\]](#)
10. Baghel, V.S.; Prakash, S.; Agrawal, I. An enhanced fuzzy vault to secure the fingerprint templates. *Multimed. Tools Appl.* **2021**, *80*, 33055–33073. [\[CrossRef\]](#)
11. Jain, A.K.; Kumar, A. Biometrics of next generation: An overview. *Second. Gener. Biom.* **2010**, *12*, 2–3.
12. Juels, A.; Wattenberg, M. A fuzzy commitment scheme. In Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1–4 November 1999; pp. 28–36.
13. Juels, A.; Sudan, M. A fuzzy vault scheme. *Des. Codes Cryptogr.* **2006**, *38*, 237–257. [\[CrossRef\]](#)
14. Uludag, U.; Jain, A.K. Fuzzy fingerprint vault. In Proceedings of the Workshop: Biometrics: Challenges Arising from Theory to Practice, Cambridge, UK, 22–27 August 2004; pp. 13–16.

15. Uludag, U.; Pankanti, S.; Jain, A.K. Fuzzy Vault for Fingerprints. *Proc. AVBPA LNCS* **2005**, *3546*, 310–379.
16. Nandakumar, K.; Jain, A.K.; Pankanti, S. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Trans. Inf. Forensics Sec.* **2007**, *2*, 744–757. [\[CrossRef\]](#)
17. Tams, B. Unlinkable minutiae-based fuzzy vault for multiple fingerprints. *IET Biom.* **2015**, *5*, 170–180. [\[CrossRef\]](#)
18. Tams, B.; Mihailescu, P.; Munk, A. Security considerations in minutiae-based fuzzy vaults. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 985–998. [\[CrossRef\]](#)
19. Wang, Y.; Plataniotis, K.N. Fuzzy vault for face based cryptographic key generation. In Proceedings of the Biometrics Symposium, Baltimore, MD, USA, 11–13 September 2007.
20. Wu, L.; Yuan, S. A face based fuzzy vault scheme for secure online authentication. In Proceedings of the Second International Symposium on Data, Privacy, and E-Commerce, Buffalo, NY, USA, 13–14 September 2010; pp. 45–49.
21. Lee, Y.J.; Bae, K.; Lee, S.J.; Park, K.R.; Kim, J. Biometric key binding: Fuzzy vault based on iris images. In Proceedings of the International Conference on Biometrics, Seoul, Republic of Korea, 27–29 August 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 800–808.
22. Hao, F.; Anderson, R.; Daugman, J. Combining crypto with biometrics effectively. *IEEE Trans. Comput.* **2006**, *55*, 1081–1088.
23. Kholmatov, A.; Yanikoglu, B. Biometric cryptosystem using online signatures. In *Proceedings of the International Symposium on Computer and Information Sciences*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 981–990.
24. Kumar, A.; Kumar, A. Development of a New Cryptographic Construct Using Palmprint Based Fuzzy Vault. *EURASIP J. Adv. Signal Process.* **2009**, *2009*, 967046. [\[CrossRef\]](#)
25. Lee, Y.J.; Park, K.R.; Lee, S.J.; Bae, K.; Kim, J. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Trans. Syst. Man Cybern. Part B Cybern.* **2008**, *38*, 1302–1313.
26. Dang, T.K.; Truong, Q.C.; Le, T.T.B.; Truong, H. Cancellable fuzzy vault with periodic transformation for biometric template protection. *IET Biom.* **2016**, *5*, 229–235. [\[CrossRef\]](#)
27. Lalithamani, N.; Sabirigiriraj, D.M. Technique to Generate a Face and Palm Vein-Based Fuzzy Vault for a Multi-Biometric Cryptosystem. *Mach. Graph. Vis.* **2014**, *23*, 97–114. [\[CrossRef\]](#)
28. Lalithamani, N.; Sabirigiriraj, M. Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem. *Imaging Sci. J.* **2015**, *63*, 111–118. [\[CrossRef\]](#)
29. You, L.; Wang, T. A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion. *Soft Comput.* **2019**, *23*, 3843–3851. [\[CrossRef\]](#)
30. Rathgeb, C.; Tams, B.; Merkle, J.; Nesterowicz, V.; Korte, U.; Neu, M. Multi-Biometric Fuzzy Vault based on Face and Fingerprints. *arXiv* **2023**, arXiv:2301.06882.
31. Moon, D.; Chung, Y.; Seo, C.; Kim, S.Y.; Kim, J.N. A practical implementation of fuzzy fingerprint vault for smart cards. *J. Intell. Manuf.* **2014**, *25*, 293–302. [\[CrossRef\]](#)
32. Yasuda, M.; Sugimura, Y. Biometric key-binding using lattice masking. *Secur. Commun. Netw.* **2015**, *8*, 3405–3414. [\[CrossRef\]](#)
33. Dong, X.; Kim, S.; Jin, Z.; Hwang, J.Y.; Cho, S.; Teoh, A.B.J. Secure chaff-less fuzzy vault for face identification systems. *ACM Trans. Multim. Comput. Commun. Appl.* **2021**, *17*, 1–22. [\[CrossRef\]](#)
34. Rathgeb, C.; Merkle, J.; Scholz, J.; Tams, B.; Nesterowicz, V. Deep face fuzzy vault: Implementation and performance. *Comput. Secur.* **2022**, *113*, 102539. [\[CrossRef\]](#)
35. Nguyen, T.H.; Wang, Y.; Ha, Y.; Li, R. Improved chaff point generation for vault scheme in bio-cryptosystems. *IET Biom.* **2012**, *2*, 48–55. [\[CrossRef\]](#)
36. Nguyen, M.T.; Truong, Q.H.; Dang, T.K. Enhance fuzzy vault security using nonrandom chaff point generator. *Inf. Process. Lett.* **2016**, *116*, 53–64. [\[CrossRef\]](#)
37. Draper, S.C.; Khisti, A.; Martinian, E.; Vetro, A.; Yedidia, J.S. Using distributed source coding to secure fingerprint biometrics. In Proceedings of the 2007 IEEE International Conference on Acoustics, Speech and Signal Processing, Honolulu, HI, USA, 15–20 April 2007; p. II-129.
38. Yang, J.; Chen, S.; Cao, Y. A PUF-Based Key Storage Scheme Using Fuzzy Vault. *Sensors* **2023**, *23*, 3476. [\[CrossRef\]](#)
39. Yao, L.; Liu, B.; Wu, G.; Yao, K.; Wang, J. A biometric key establishment protocol for body area networks. *Int. J. Distrib. Sens. Netw.* **2011**, *7*, 282986. [\[CrossRef\]](#)
40. Zheng, G.; Fang, G.; Orgun, M.A.; Shankaran, R. A comparison of key distribution schemes using fuzzy commitment and fuzzy vault within wireless body area networks. In Proceedings of the IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, Hong Kong, China, 30 August–2 September 2015; pp. 2120–2125.
41. Venkatasubramanian, K.K.; Banerjee, A.; Gupta, S.K.S. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Trans. Inf. Technol. Biomed.* **2010**, *14*, 60–68. [\[CrossRef\]](#) [\[PubMed\]](#)
42. Hu, C.; Cheng, X.; Zhang, F.; Wu, D.; Liao, X.; Chen, D. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In Proceedings of the IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2274–2282.
43. Miao, F.; Jiang, L.; Li, Y.; Zhang, Y.T. Biometrics based novel key distribution solution for body sensor networks. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Minneapolis, MN, USA, 3–6 September 2009; pp. 2458–2461.

44. Zheng, G.; Fang, G.; Orgun, M.A.; Shankaran, R.; Dutkiewicz, E. Securing wireless medical implants using an ECG-based secret data sharing scheme. In Proceedings of the 14th International Symposium on Communications and Information Technologies, Incheon, Republic of Korea, 24–26 September 2014; pp. 373–377.
45. Li, Q.; Liu, Z.; Niu, X. Analysis and problems on fuzzy vault scheme. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, 18–20 December 2006; pp. 244–250.
46. Liu, H.; Sun, D.; Xiong, K.; Qiu, Z. Is fuzzy vault scheme very effective for key binding in biometric cryptosystems? In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, China, 10–12 October 2011; pp. 279–284.
47. Adler, A. Vulnerabilities in biometric encryption systems. In Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication, Hilton Rye Town, NY, USA, 20–22 July 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 1100–1109.
48. Scheirer, W.J.; Boulton, T.E. Cracking fuzzy vaults and biometric encryption. In Proceedings of the Biometrics Symposium, Baltimore, MD, USA, 11–13 September 2007.
49. Kholmatov, A.; Yanikoglu, B. Realization of correlation attack against the fuzzy vault scheme. In Security, forensics, steganography, and watermarking of multimedia contents X. *Proc. Int. Soc. Opt. Photonics* **2008**, 6819, 681900.
50. Kim, A.; Lee, S. A prediction scheme of recognition performance using confidence interval. *IEICE Electron. Express* **2012**, 9, 133–139. [[CrossRef](#)]
51. CVC Technical Report 24: The AR Face Database. Available online: <http://www2.ece.ohio-state.edu/~aleix/ARdatabase.html> (accessed on 23 July 2023).
52. Turk, M.; Pentland, S. Eigenfaces for Recognition. *J. Cogn. Neurosci.* **1991**, 3, 71–86. [[CrossRef](#)] [[PubMed](#)]
53. Kim, A.; Lee, S. Quality Assessment Method of Biometrics for Estimating Authentication Result in User Authentication System. *J. KIISE Comput. Pract. Lett.* **2010**, 16, 242–246.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.