7-6-2019

A cancelable iris- and steganography-based user authentication system for the Internet of Things

Wencheng Yang
Edith Cowan University

Song Wang

Jiankun Hu

Ahmed Ibrahim
Edith Cowan University

Guanglou Zhang
Edith Cowan University

See next page for additional authors

10.3390/s19132985

Yang, W., Wang, S., Hu, J., Ibrahim, A., Zheng, G., Macedo, M. J., ... Valli, C. (2019). A cancelable iris- and steganography-based user authentication system for the Internet of Things. *Sensors*, *19*(13), Article 2985. Available here

sensors

MDPI

Article

A Cancelable Iris- and Steganography-Based User Authentication System for the Internet of Things

Wencheng Yang [1,*], Song Wang [2], Jiankun Hu [3], Ahmed Ibrahim [1], Guanglou Zheng [1], Marcelo Jose Macedo [1], Michael N. Johnstone [1] and Craig Valli [1]

[1] Security Research Institute, Edith Cowan University, Perth, WA 6207, Australia
[2] Department of Engineering, La Trobe University, Melbourne, VIC 3083, Australia
[3] School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia
[*] Correspondence: w.yang@ecu.edu.au; Tel.: +61-863-045-210

Received: 24 May 2019; Accepted: 4 July 2019; Published: 6 July 2019

check for updates

Abstract: Remote user authentication for Internet of Things (IoT) devices is critical to IoT security, as it helps prevent unauthorized access to IoT networks. Biometrics is an appealing authentication technique due to its advantages over traditional password-based authentication. However, the protection of biometric data itself is also important, as original biometric data cannot be replaced or reissued if compromised. In this paper, we propose a cancelable iris- and steganography-based user authentication system to provide user authentication and secure the original iris data. Most of the existing cancelable iris biometric systems need a user-specific key to guide feature transformation, e.g., permutation or random projection, which is also known as key-dependent transformation. One issue associated with key-dependent transformations is that if the user-specific key is compromised, some useful information can be leaked and exploited by adversaries to restore the original iris feature data. To mitigate this risk, the proposed scheme enhances system security by integrating an effective information-hiding technique—steganography. By concealing the user-specific key, the threat of key exposure-related attacks, e.g., attacks via record multiplicity, can be defused, thus heightening the overall system security and complementing the protection offered by cancelable biometric techniques.

Keywords: iris; feature data protection; cancelable; steganography

1. Introduction

In Internet of Things (IoT) networks, things, also called smart objects, are connected by wireless networks, producing and consuming data in order to perform their function. The term, IoT, was proposed by Ashton [1] in 1999. Since then, the IoT has drawn increasing attention from researchers in both academia and industry [1]. Smart objects in the IoT are commonly bound with sensors and computing capabilities, which enable them to sense the surrounding environment, communicate with each other, and potentially make a decision without (or with limited) human intervention.

Because of the energy and computing constraints of smart objects (e.g., cameras), rather than relying on their limited resources, data need to be collected and transmitted wirelessly by smart objects to remote central servers for further processing in the scenario of remote surveillance IoT networks. However, for such IoT networks, security threats such as unauthorized access can significantly impact on data confidentiality and user privacy. Therefore, user authentication for the purpose of access control plays a key role in establishing trust between users of smart objects and remote servers. A reliable authentication system ensures that the users of smart objects are the genuine, legitimate users, so that trust can be established and data integrity can be guaranteed. The capability of an authentication system to detect imposters determines the trust level in the IoT environment [2].

Passwords and tokens are traditional methods of user authentication. However, passwords can be easily forgotten and tokens may be stolen or lost. As an alternative, biometric authentication is becoming more attractive since biometric traits cannot be lost and do not need to be remembered [3,4]. Biometric recognition systems achieve authentication based on "who you are", because any individual's biometrics, e.g., iris and fingerprints, are unique [2]. Many biometric traits can be used for biometric recognition, such as fingerprints, face, iris, and palm prints. Among these options, the iris is highly reliable due to the unique and stable features it offers [4]. The iris begins to form from the third month of embryonic life. The unique pattern on the iris' surface is generated during the first year of life and formation of this unique pattern is random and unaffected by genes [5], so even identical twins have different iris patterns.

IoT devices tend not to use source authentication for a range of reasons, which might be related to, for example, architectural constraints, power consumption, device memory, or simply the assumption that all devices in a network are trustworthy by default, and, therefore, authentication is unnecessary. El-hajj et al. [6] presented a survey of IoT authentication schemes. The authors pointed out that traditional authentication is unsuitable for the IoT setting due to the nature of IoT devices, despite ZigBee (as an example of a wireless IoT protocol) using 128 bit AES encryption. El-Hajj et al. [6] split authentication schemes according to the authentication factor, token use, authentication procedure, authentication architecture, IoT layer, and, finally, whether the scheme is hardware-based. In their analysis, biometric-based authentication has particular strengths, such as ease of use and unforgettable credentials, as well as resistance to certain types of attack. Figure 1 shows that biometrics methods fit into the physical context of IoT authentication.

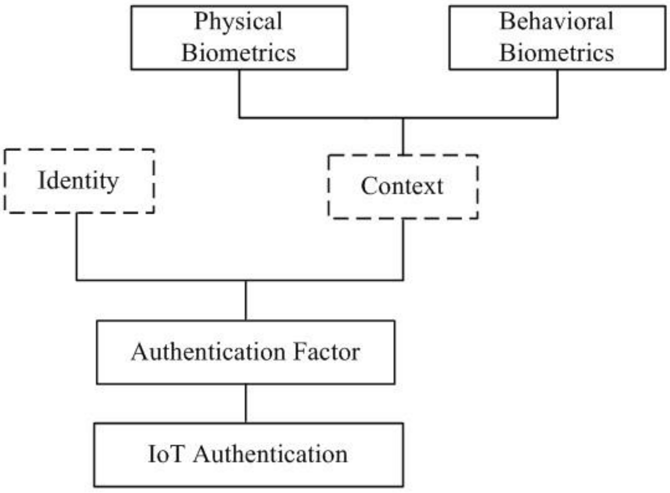

Figure 1. A partial taxonomy of authentication schemes for IoT devices (adapted from [6]).

With the aforementioned benefits of biometric authentication, one option is to leverage several biometrics in sequence in multi-modal verification, as reported by Blasco and Peris-Lopez [7]. Such a strategy may be better than non-biometric methods, but it relies on multiple biometrics, which is not necessarily feasible in the context of IoT devices. Nonetheless, the concept of combining authentication methods is sound, as noted by Arjona et al. [8], who used a combination of a biometric approach and a physically unclonable function. It is, therefore, worthwhile to consider fusing biometric recognition with another technique as a more secure means of authentication. Along this line of thinking, in this paper, we propose a cancelable iris- and steganography-based user authentication system for IoT networks. In the proposed scheme, the cancelable iris-based authentication system employs a user-specific secret key as the transformation parameter to guide non-invertible transformation. However, there is a potential risk associated with the user-specific key. That is, if it is acquired by an adversary, he/she may use it to restore the original iris feature data, which is likely to compromise the authentication system. To mitigate this potential risk, we integrate an effective information-hiding technique—steganography with cancelable iris biometrics. Unlike existing cancelable biometric authentication systems, in our scheme, the user-specific key is not generated and transmitted together with the users' biometric data to the server for authentication purposes. Instead, it is hidden within other media data, e.g., collected images, which are sent to the server separately. Concealing the existence of the user-specific key enhances the security of the iris-based authentication system.

The rest of this paper is organized in the following order. Relevant research in the biometric-based IoT and cancelable iris-based biometrics are presented in Section 2. The cancelable iris- and steganography-based user authentication system is proposed in Section 3. In Section 4, experimental results are reported and discussed. Finally, the conclusion is provided in Section 5.

2. Related Work

2.1. Biometric-Based IoT Networks

With the advantages (e.g., uniqueness, convenience) of biometrics over password- and token-based traditional authentication, many researchers have been working on developing biometric-based methods for user authentication in IoT networks. For instance, in [2], Kashif et al. proposed an authentication framework using biometrics and wireless device radio fingerprinting for user authentication. The proposed framework not only can verify the monitored healthy data from the correct patient, but also ensures the integrity of the data. In [9], Kantarci et al. introduced a cloud-centric biometric identification architecture, which couples both the biometric scheme and context-aware technique to protect mobile applications from unauthorized access. In [10], Karimian et al. applied electrocardiogram (ECG) signals to authentication in an IoT system, as they observed that ECG biometrics are reliable, secure, and easy to implement. In [11], Maček et al. presented a scheme with multimodal biometrics (face and iris) for authentication. In this scheme, the face and iris images are obtained simultaneously using the high-quality, built-in cameras of mobile devices, e.g., laptops, smartphones, and tablets. One drawback of this scheme, as pointed out by the authors, is the acceptability of iris biometrics and the privacy concerns surrounding the stored face and iris templates.

In [12], Shahim et al. attempted to authenticate users using both the users' hand geometry scan and a series of gestures on a Raspberry Pi platform. In [13], a lightweight multi-factor remote user authentication scheme was developed by Dhillon and Kalra. In the proposed scheme, the use of computationally less expensive hash functions and XOR (exclusive or) operations make the scheme suitable for resource-constrained IoT devices. In [14], Punithavathi et al. proposed a cloud-based lightweight cancelable fingerprint authentication system. The experimental results and analysis showed that the proposed fingerprint authentication system achieved state-of-the-art recognition performance with less computing time, thus rendering it a good candidate for IoT networks.

2.2. Cancelable Iris-Based Biometrics

Although the benefits of biometrics make biometric systems an appealing alternative to password- or token-based authentication for IoT devices, a major issue in biometric-based authentication systems is that any individual's biometric traits are not replaceable. The loss of original biometric feature data in one application means that it is lost forever and also affects all other applications that use the same feature set [15,16]. The compromise of original biometric feature data leads to serious security and privacy concerns. Therefore, it is vital to protect the original biometric feature data. One important biometric data protection technique is known as cancelable biometrics. In a cancelable biometric system, the original biometric feature data are converted into an irreversible version by applying a one-way transformation. The transformed feature data are mathematically non-invertible, and, if compromised, they can be easily revoked and replaced with another transformed version by changing the parameter key, which is user-specific [17]. Cancelable biometrics was first proposed by Ratha et al. [18]. Later, three different transformation functions, Cartesian transformation, Polar transformation, and Functional transformation, were developed by Ratha et al. to generate a practical cancelable fingerprint authentication system [19].

Compared with those common biometric traits, e.g., fingerprints and face, the iris provides good reliability and high recognition accuracy, so it has been employed in many biometric authentication systems. There is ongoing research into cancelable iris biometrics. In [20], Zuo et al. proposed four different methods to generate cancelable iris biometrics for improving the security and privacy of iris templates. The authors also discussed the strengths and drawbacks of these four methods. In [21], Hämmerle-Uhl et al. introduced two different transformations, block re-mapping and mesh-warping. With different parameter settings, system performance can be well maintained with only marginal post-transformation degradation. For example, the block re-mapping achieved an equal error rate (EER) of 1.2% after transformation, compared with EER = 1.1% before transformation. In [22], Kanade et al. incorporated two factors, iris and password, to generate cancelable iris templates. Specifically, a user-specific key is used to shuffle the iris code and an Error Correcting Code (ECC) is employed to decrease feature variation to achieve better recognition performance. In [23], Pillai et al. designed cancelable iris biometrics based on sectored random projections. Two steps, feature extraction and random projections, are included in this method. The experimental results show that the criterion for cancelability is met.

In [24], Jenisch and Uhl applied block permutation and remapping to protecting the iris template. Specifically, in the permutation operation, blocks of the feature texture are rearranged, controlled by a permutation key, and in the remapping operation, some blocks are mapped on top of the other blocks to make the reconstruction of the iris image more difficult. In [25], Hämmerle-Uhl et al. implemented key-dependent wavelet transformations to build non-invertible iris templates. In this approach, the extracted iris features are highly sensitive to slight variations in key parameters. The experimental results show that the accuracy of the proposed scheme is similar before and after feature transformation.

In [26], Rathgeb et al. presented an adaptive Bloom filter-based cancelable iris recognition system. The Bloom filters can map part of a binary template to Bloom filter-based representations, which are irreversible. This system is alignment-free because the Bloom filter-based features do not require image pre-alignment. In [4], Lai et al. introduced the "Indexing-First-One" (IFO) hashing. Two mechanisms, Hadamard product code and module thresholding functions, are proposed to further improve the security and performance of the IFO hashing.

The existing issue: In the abovementioned iris-based authentication schemes, the non-invertible transformations rely on user-specific keys (or parameters), which can also be referred to as key-dependent transformations. However, in some schemes, e.g., [21,24], when the key, which is used to guide the transformation, is known by an adversary, the transformation can be reversed easily. In random projection based schemes, e.g., [23], if multiple transformed feature vectors and keys are lost, the adversary can restore the original feature vector from the attacks via record multiplicity (ARM) [27,28]. The exposure of the user-specific key leaks useful information, which may be exploited by the adversary. In this case, the security of the iris recognition system is under threat. In order to enhance key protection, Tran et al. [29] split the key into different camouflage images based on Shamir's Secret Sharing Scheme. However, this approach is cloud-based and does not suit the conventional operation under discussion.

Contributions of this work: To reduce the risk introduced by the exposure of user-specific keys, we propose a cancelable iris- and steganography-based user authentication system. This system uses a cancelable biometric technique to secure the original biometric data. Furthermore, the steganography [30] technique is employed to hide the user-specific key, which is required by cancelable biometrics. In this way, we can enhance the overall security of the user authentication system by complementing the protection provided by a cancelable biometric technique.

3. The Proposed Cancelable Iris- and Steganography-Based System

In a remote surveillance IoT network, smart objects are responsible for continuously monitoring targeted areas and transmitting monitored data, (e.g., images) back to the server. In certain cases, the user may need to access a smart object for an update. To prevent unauthorized access, user authentication plays a critical role. In this paper, user authentication is performed by a cancelable iris- and steganography-based authentication system. The entire user authentication process of the proposed system is illustrated in Figure 2, which includes three major phases—Phase (a): iris feature generation and transformation, Phase (b): hiding the user-specific key with steganography, and Phase (c): matching on the server. These three phases correspond to Section 3.1, Section 3.2, and Section 3.3, respectively.

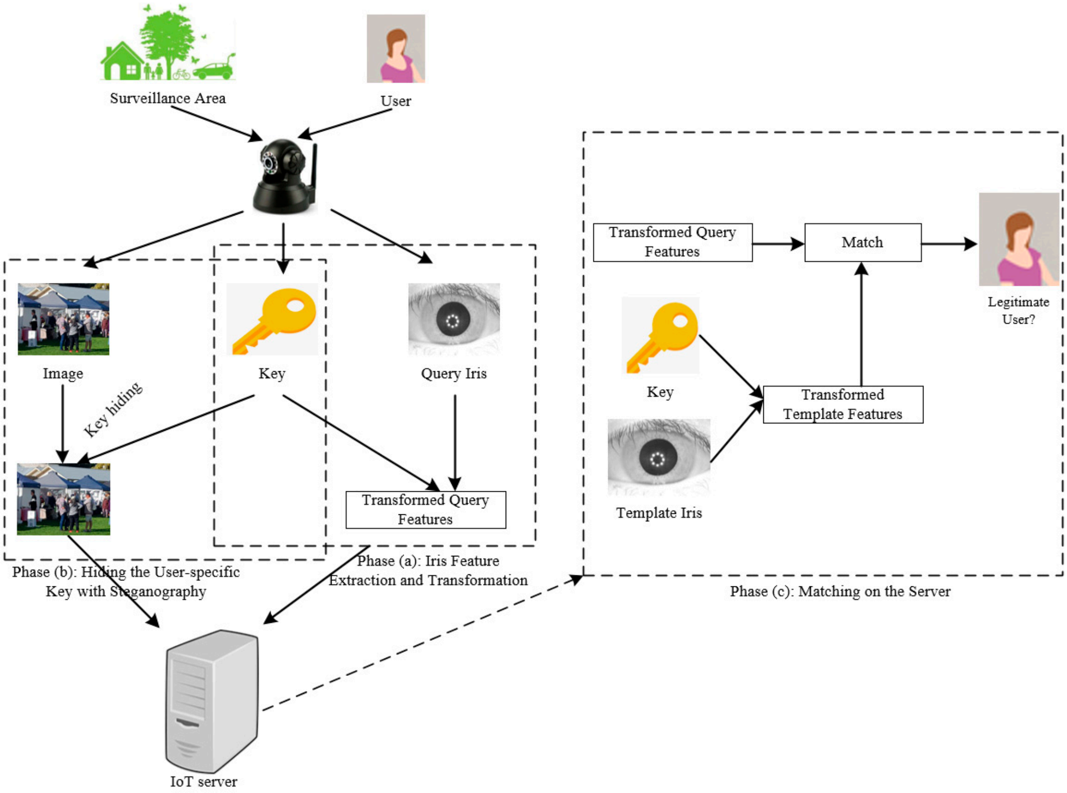
Surveillance Area
User
Image
Key
Query Iris
Key hiding
Transformed Query Features
Phase (b): Hiding the User-specific Key with Steganography
Phase (a): Iris Feature Extraction and Transformation
IoT server
Transformed Query Features
Match
Legitimate User?
Key
Transformed Template Features
Template Iris
Phase (c): Matching on the Server

Figure 2. The entire authentication process of the proposed system.

To focus on the relevant issues, we assume that the user of smart objects has registered his/her iris (i.e., template data stored in the server) prior to the deployment of the IoT network. The server has superior computing power and security compared to the deployed smart objects. The following processes (Sections 3.1–3.3) are carried out when a user wants to access the IoT devices or services through the proposed user authentication system.

3.1. Iris Feature Extraction and Transformation

When a camera captures an image of a user's iris, three steps are typically required for the authentication system to generate features from the iris image, as demonstrated in Figure 3. The first step is to isolate the iris region, which is called iris segmentation. The iris region is defined as the area between two circles, one circle being the boundary between the iris and sclera (the green circle in Step 1 of Figure 3) and the other circle being the boundary between the iris and pupil (the red circle in Step 1 of Figure 3). After the iris region is isolated and segmented from the eye image, the second step is normalization, which unwraps the iris region into a rectangle with fixed dimensions, as shown in Step 2 of Figure 3. With the normalization step, two eye images of the same iris under different conditions can provide features at the same spatial location. The last step is feature extraction, as shown in Step 3 of Figure 3. This step creates the iris feature vectors in a specific data format, e.g., a binary string.

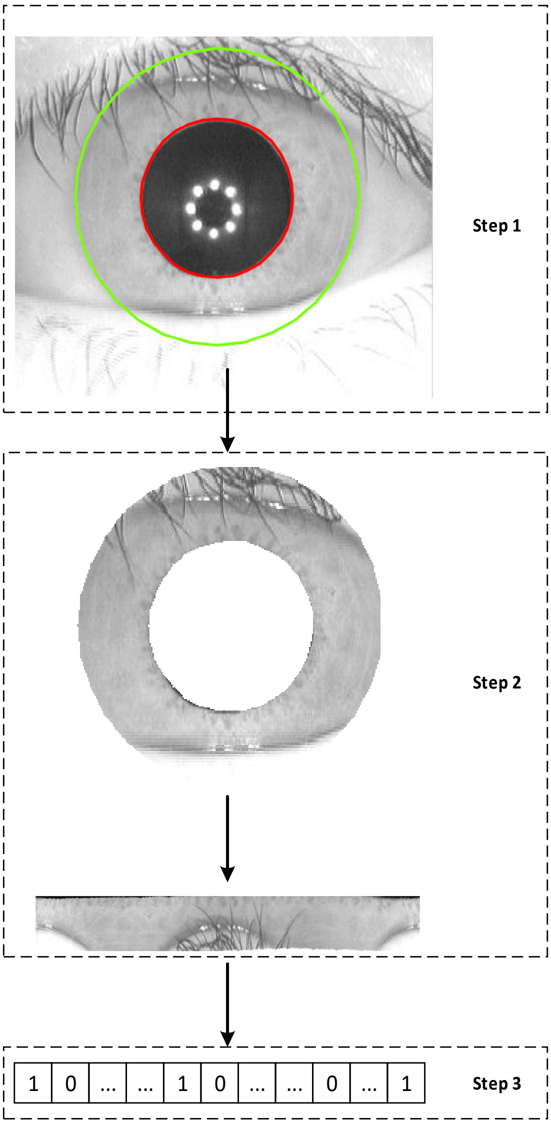

Figure 3. Three iris feature generation steps—Step 1: segmentation, Step 2: normalization, and Step 3: feature extraction.

There are many existing algorithms for extracting iris features from an iris image, such as Masek's algorithm [5] and the algorithm in [31]. In this paper, VeriEye SDK (Software Development Kit) [32] from Neuro Technology is adopted to extract iris features. Assume that F is the original iris feature extracted by VeriEye SDK. This feature vector contains 2348 bytes, each of which is an integer in the range of [0, 255]. To reduce intra-class variation and also convert the integer values into binary, in this work, quantization is applied to each element of the feature vector F. Specifically, elements that are located in [0, 255 × 1/4] are represented by the binary value of '00'. Elements that fall in [255 × 1/4, 255 × 2/4] are assigned the binary value of '01'. Similarly, elements that belong to [255 × 2/4, 255 × 3/4] are given the binary value of '10' and elements in the range of [255 × 3/4, 255] are represented by the binary value of '11'. After quantization, the original feature vector F is converted to a binary feature vector F_b. The size of F_b is 4696 (= 2348 × 2) bits, because each element in F is quantized into two bits in F_b.

Because of iris rotation in the iris image acquisition process, after the binary feature vector F_b is obtained, feature shifting is needed before further operations take place, such as non-invertible transformation and matching on the server. In this work, the template feature F_b^T stored in the server does not need any shifting, but each query feature vector F_b^Q is shifted up to N bits left and up to N bits right (the superscripts T and Q stand for 'template' and 'query'). Each bit shift creates a new variant of the query feature vector F_b^Q. Therefore, including F_b^Q itself, a total of $2N + 1$ binary strings, $\mathbf{F}_B^Q = \left\{F_b^Q(-N), \ldots, F_b^Q(0), \ldots, F_b^Q(N)\right\}$, are generated from this shifting operation, where "−" denotes left shift and $F_b^Q(0)$ means F_b^Q itself without shifting (i.e., a 0 bit shift).

If the query feature set $\mathbf{F}_B^Q$ is directly sent to the server without any protection and obtained by the adversary, the original iris features can be retrieved, leading to serious consequences, such as identity loss. To protect $\mathbf{F}_B^Q$, we employ a random projection based transformation, guided by a user-specific key [33]. Specifically, whenever the proposed authentication system receives a user's iris image, a new user-specific key K is generated as a seed to construct a projection matrix $\mathbf{M}$, which is of size $m \times n$, where $m \leq n$. Then, the non-invertible transformation is applied to each element of the query feature set $\mathbf{F}_B^Q$, given by

$$\mathbf{y}^Q(i) = \mathbf{M}F_b^Q(i) \tag{1}$$

where $i \in [-N, N]$. As a result, a feature set containing $2N$+1 vectors, $\mathbf{Y}^Q = \left\{\mathbf{y}^Q(i)\right\}_{i \in [-N,N]}$ is generated. The application of random projection in Equation (1) forms an underdetermined system that has non-unique solutions. Even if both the transformed feature vector $\mathbf{y}^Q(i)$ and the projection matrix $\mathbf{M}$ (or user-specific key K) are obtained by the adversary [34], it is computationally hard to find the query vector $F_b^Q(i)$.

3.2. Hiding the User-Specific Key with Steganography

The transformed query feature vector $\mathbf{y}^Q(i)$ is derived from Equation (1) using the projection matrix $\mathbf{M}$ generated by the user-specific key K as a seed. If K_1 is set to be different to K_2, the generated projection matrix, $\mathbf{M}_1$, is different to $\mathbf{M}_2$. The security of $F_b^Q(i)$ in Equation (1) is based on a well-known result about an underdetermined system of linear equations. However, according to [27,28], if the adversary can acquire multiple transformed feature vectors and their corresponding projection matrixes (or user-specific key K), then the original query feature vector $F_b^Q(i)$ can be retrieved by launching the ARM (attacks via record multiplicity). Therefore, protecting the secret key K is critical in defending against the ARM.

To protect the user-specific key K, we chose an established information-hiding technique named steganography to hide K in a cover image [30]. It is noteworthy that steganography differs from cryptographic techniques. A cryptographic method would scramble the key so that it cannot be understood, while steganography hides the key so it cannot be seen. There are some popular methods in steganography. For example, see e.g., [35,36], where different redundancies in a cover image are exploited for hiding data. In [37], the data is hidden in the least significant bits (LSBs) of a cover image, and in [38], the data is hidden in the frequency domain.

Since the objective of this paper is to design an authentication system that improves the security of the cancelable iris biometrics by hiding the secret key K, we implemented an online steganography program [39]. An image before key hiding and after key hiding is shown in Figure 4, which is impossible to distinguish with the naked eye. Note that the cover image can be any image out of a number of images collected by smart objects in a targeted surveillance area.

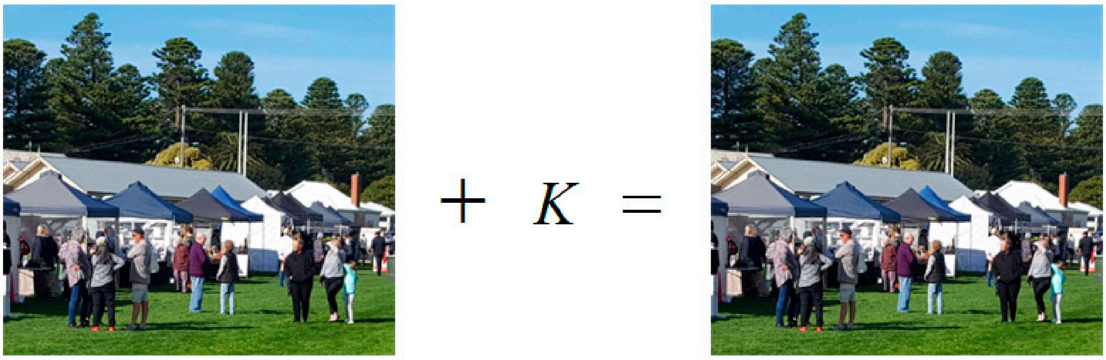

Figure 4. An image before key hiding (**left**) and after key hiding (**right**). The difference between them is impossible to distinguish with the naked eye.

3.3. Matching on the Server

After the operations of query feature transformation and key hiding with steganography, the transformed feature set $\mathbf{Y}^Q$ is sent to the server, while the user-specific key K hidden in one of the numerous images is also sent to the server, but separately. Once the user-specific key K is retrieved at the server, the same transformation is performed to the stored template feature F_b^T, guided by the projection matrix $\mathbf{M}$, which is generated by the user-specific key K. That is,

$$\mathbf{y}^T = \mathbf{M}F_b^T. \tag{2}$$

In the matching process, the template feature vector $\mathbf{y}^T$ is compared with each element in the query feature set $\mathbf{Y}^Q = \left\{\mathbf{y}^Q(i)\right\}_{i\in[-N,N]}$. The similarity score between $\mathbf{y}^T$ and each element $\mathbf{y}^Q(i)$ in $\mathbf{Y}^Q$ is calculated by using Equation (3) below:

$$S_i = 1 - \frac{\left\|\mathbf{y}^T - \mathbf{y}^Q(i)\right\|_2}{\left\|\mathbf{y}^T\right\|_2 + \left\|\mathbf{y}^Q(i)\right\|_2} \tag{3}$$

where $\|\cdot\|_2$ is the 2-norm. Then, a score array $S = [S_0, S_1, \ldots, S_{2N}]$ is obtained and the maximum score $S_{\max}$ in S is chosen as the final matching score between the template and query iris images to reach a verdict. The similarity score $S_{\max}$ ranges from 0 to 1 with 1 meaning that the template and the query match exactly [40,41]. If the matching score is larger than a predefined threshold, then the query is a legitimate user registered in the server, and vice versa.

4. Experimental Results

4.1. Database Selection and Experimental Environment

The evaluation of the proposed method is conducted over the following three publicly available iris databases:

CASIA-IrisV3-Interval [42]: This database includes 2639 iris images from 395 classes (eyes) captured with a close-up iris camera. The resolution of the iris image is 320 × 280 pixels. In our experiments, we only selected the left eye images (a total of 1332 images).

MMU-V1 [43]: This database includes 450 images (five images per iris and two irises per subject), contributed by 45 individuals using a semi-automated camera, LG IrisAccess 2200, dedicated to Iris capturing. The resolution of the iris image is 320 × 240 pixels. All the images were involved in our experiments.

UBIRIS-V1-Session 1 [44]: This database contains 1214 iris samples from 241 individuals. The resolution of the iris image is 200 × 150 pixels. In our experiments, the first five iris samples of each of the 241 individuals from the first session were used (a total of 1205 images).

Three samples from each database are illustrated as examples in Figure 5. The experiments in this work were conducted using MATLAB on a laptop with a 2.50 GHz Intel i5-2450M dual-core CPU, 8 GB of RAM, and a 64 bit Windows 7 operating system. Further, as noted in Section 3, the VeriEye SDK [32] from Neuro Technology was adopted to extract the iris features. Because the feature extraction of 179 images and 30 images from the CASIA-IrisV3-Interval and UBIRIS-V1-Session 1 databases was unsuccessful using VeriEye, they were excluded from the experiments.

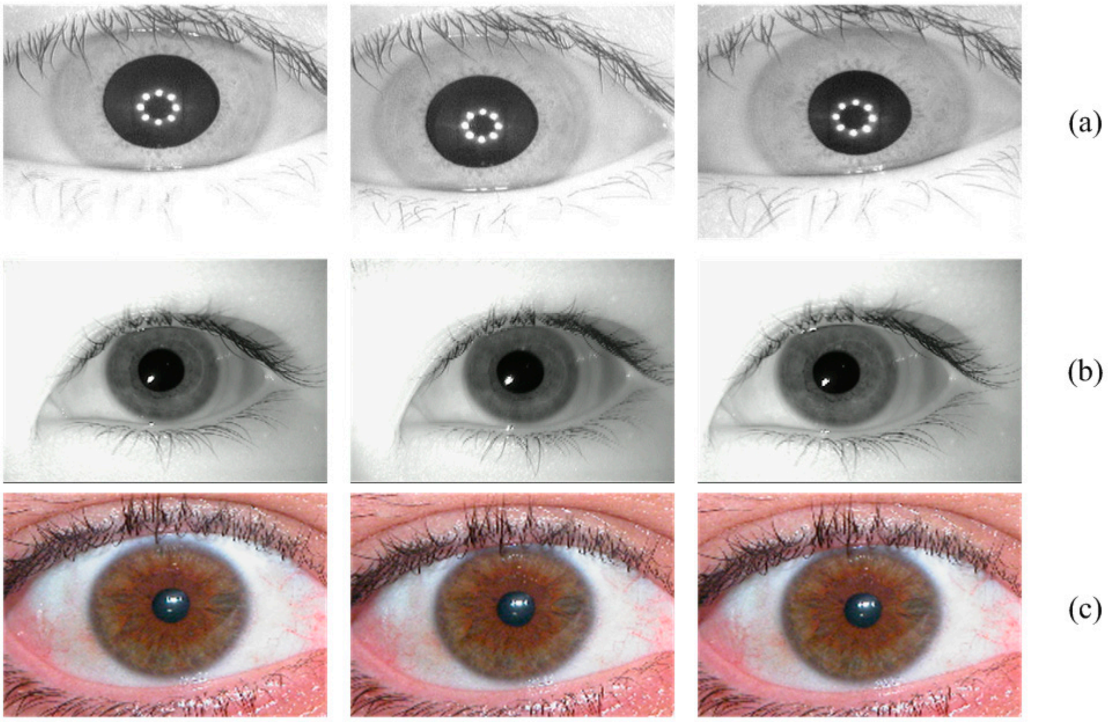

Figure 5. Three iris samples from the CASIA-IrisV3-Interval, MMU-V1, and UBIRIS-V1-Session 1 databases, in (**a**), (**b**), and (**c**), respectively.

4.2. Performance Evaluation

Three performance indicators were employed to measure system performance. They are (1) false rejection rate (FRR), (2) false acceptance rate (FAR), and (3) equal error rate (EER) [45]. In our experiments, the first image of each eye was considered as the template and the remaining images of the same eye were taken as the query to calculate the FRR, while the first image of each eye was regarded as the template and the first image of all other eyes was used as the query to calculate the FAR. The third indicator, EER, is defined as the error rate when FRR is equal to FAR.

The effect of shifting by a different number of bits was evaluated using original binary features (features before applying transformation), in order to find the optimal parameter setting of N. Note that because the original feature is in a binary format, we use Equation (4) from [46] to calculate the similarity score. Equation (3) in this paper is used to calculate the similarity score of the transformed feature data. The EERs of the proposed system using a different N with the original binary features on three different databases are listed in Table 1. It can be seen that, the system with the original binary features achieves the best performance when N = 4, 8, and 2 for the CASIA-IrisV3-Interval, MMU-V1, and UBIRIS-V1-Session 1 databases, respectively. Thus, these databases are chosen as the parameters for evaluating the system performance in the transformed domain.

Table 1. System performance with untransformed features using different parameter N. EER, equal error rate.

Shifting Parameter	$N = 2$	$N = 4$	$N = 8$
CASIA-IrisV3-Interval	EER = 0.62%	EER = 0.22%	EER = 0.22%
MMU-V1	EER = 2.11%	EER = 1.89%	EER = 1.77%
UBIRIS-V1-Session 1	EER = 2.43%	EER = 2.52%	EER = 2.53%

4.2.1. The Effect of Transformation Parameters on System Performance

With the feature transformation, we also evaluated and analysed how the transformation parameters, e.g., the size ($m \times n$) of the projection matrix $\mathbf{M}$, impact system performance. This test was carried out on the CASIA-IrisV3-Interval database. Here, n has a fixed value of 4696, which is equal to the length of the binary feature vector F_b. We varied the value of m from 500 to 2000 to examine the effect of different sizes of the projection matrix on system performance. The Receiver Operating Characteristic (ROC) curves in terms of FAR and FRR [47] under different m values are shown in Figures 6–8. In the figures, the similarity score threshold varies from 0 to 1. The performance of the proposed method under different m values is EER = 1.66%, 2.41%, and 5.19% when m = 2000, 1000, and 500, respectively. It can be seen that the proposed system performs worse as m decreases. This is because less information about the original features is preserved with a greater dimension cut (smaller m), leading to performance degradation. Moreover, similar to the analysis in [48], we evaluated the imposter score distribution of the proposed system using the transformed feature vector of different dimensions (i.e., giving m different values) on the CASIA-IrisV3-Interval database, as demonstrated in Figure 9. The mean and standard deviation of the similarity score distribution with dimension m = 2000 are 0.4988 and 0.0072, respectively, compared with 0.5070 (mean) and 0.0093 (standard deviation) when dimension m = 500. It can be seen that the differences in the mean and standard deviation values are very small—only 0.0082 and 0.0021, respectively. Although the difference in the feature dimensions of the two imposter tests causes such discrepancies, it also demonstrates that there is a safe and fairly constant dissimilarity distance when different transformed feature vectors are compared, according to [48].

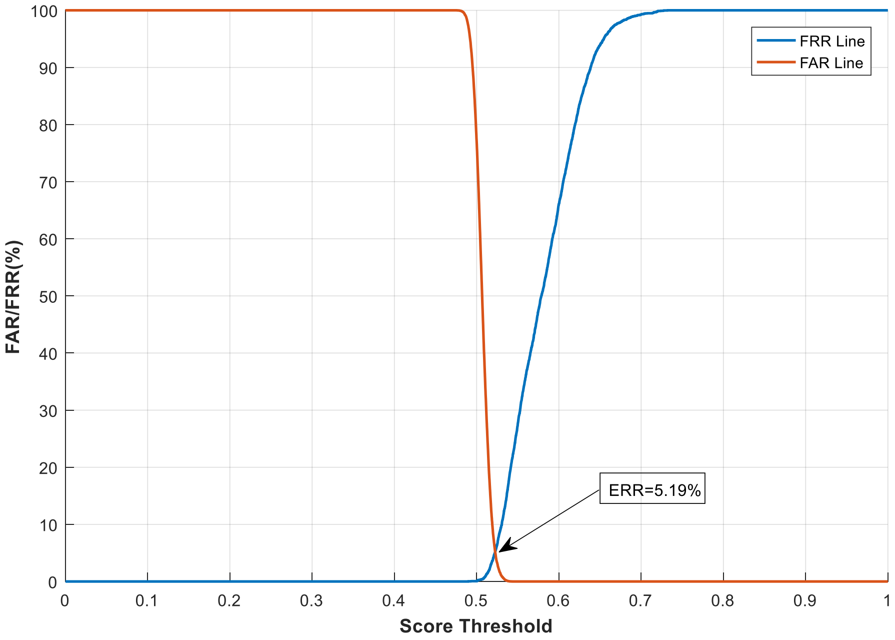

Figure 6. System performance under different score thresholds, with m = 500 on the CASIA-IrisV3-Interval database. FRR, false rejection rate; FAR, false acceptance rate.

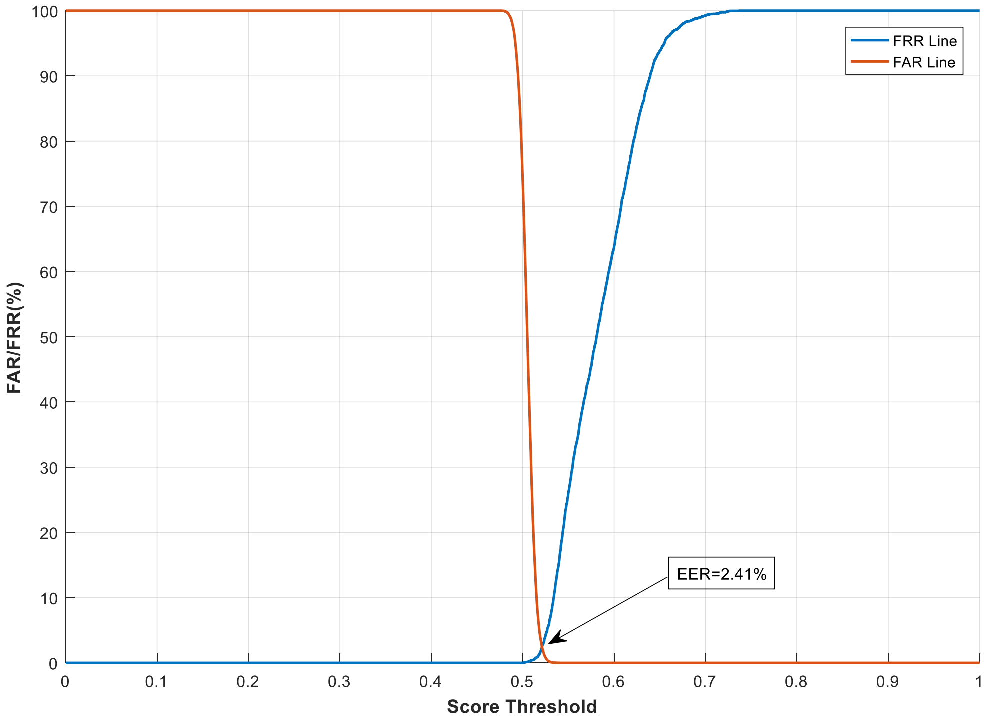

Figure 7. System performance under different score thresholds, with m = 1000 on the CASIA-IrisV3-Interval database.

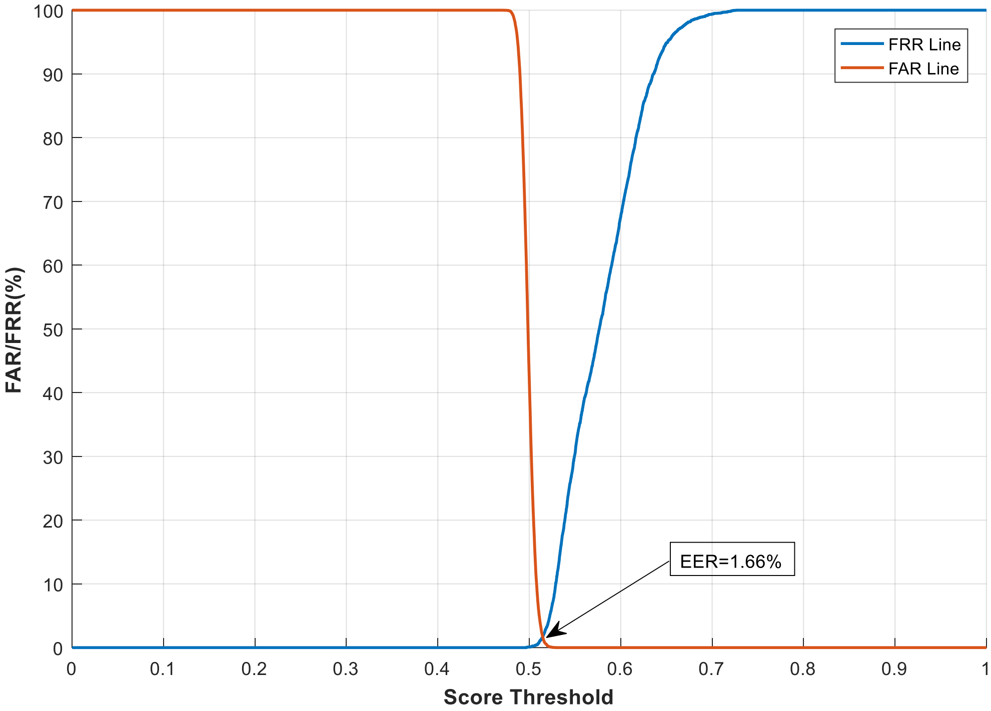

Figure 8. System performance under different score thresholds, with m = 2000 on the CASIA-IrisV3-Interval database.

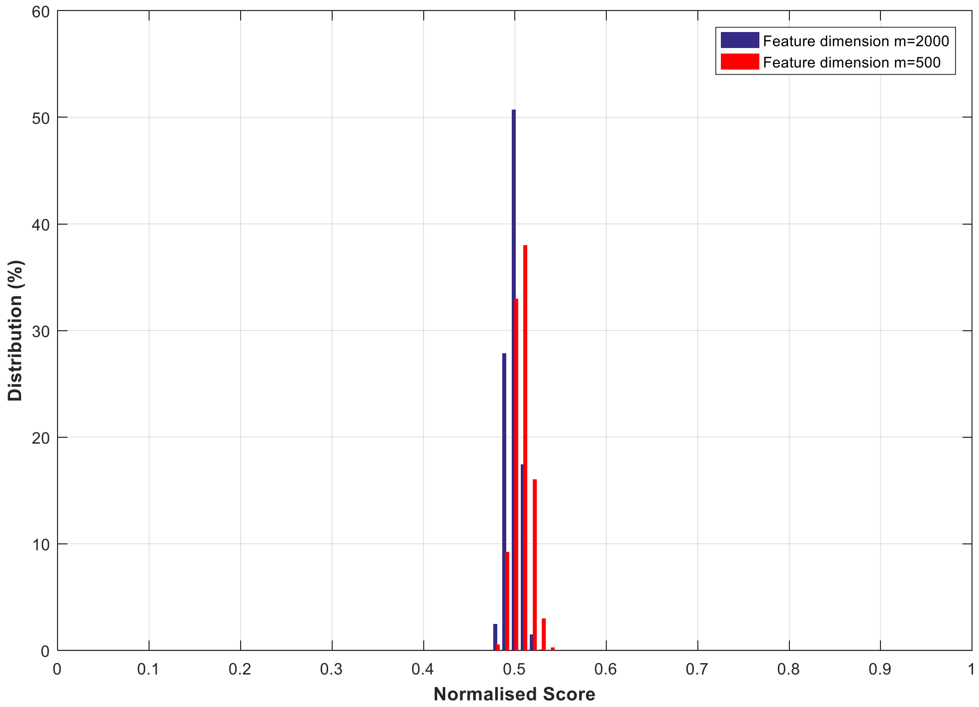

Figure 9. Distribution of the similarity scores of imposter tests with different feature dimensions on the CASIA-IrisV3-Interval database.

4.2.2. Comparison with Other Similar Systems

In the meantime, the performance of the proposed scheme is compared with other similar existing cancelable iris schemes, as shown in Table 2. It can be seen that experiments of most existing methods were carried out on the CASIA-IrisV3-Interval database, for which the proposed system performs better than [20,49], but slightly worse than other schemes. On the MMU-V1 and UBIRIS-V1-Session 1 databases, the proposed system outperforms the methods in [50,51]. More importantly, one obvious advantage of the proposed system is its heightened security, since the user-specific key K is hidden using steganography, which significantly increases the difficulty of launching key exposure-related attacks, e.g., ARM.

Table 2. System performance in terms of EER (%) using transformed features in comparison with similar methods.

Methods	Databases		
	CASIA-IrisV3-Interval	**MMU-V1**	**UBIRIS-V1-Session 1**
Bin-combo in Zuo et al. [20]	4.41%	-	-
Jenisch and Uhl [24]	1.22%	-	-
Uhl et al. [25]	1.07%	-	-
Rathgeb et al. [26]	1.54%	-	-
Ouda et al. [49]	6.27%	-	-
Jin et al. [4]	0.54%	-	-
Radman et al. [51]	-	-	9.48%
Zhao et al. [50]	1.06%	5.50%	13.44%
Proposed (m = 2000)	1.66%	4.78%	3.00%

EER of [20,49] are quoted from [4].

5. Conclusions

In this paper, we have designed a user authentication system for IoT networks. The proposed system is equipped with a cancelable iris and a steganography-based mechanism for key hiding. To protect the original iris data, feature quantization and shifting are conducted on the original feature vectors before the random projection-based feature transformation in order to achieve better recognition performance. Furthermore, to address the key exposure-related attacks, e.g., ARM, which existing key-dependent cancelable biometric systems are susceptible to, we propose to further enhance the security of the cancelable iris biometrics using steganography by hiding user-specific keys. In the future, we will investigate different types of transformation functions and study how to properly hide the secret key under various scenarios, e.g., in a mobile environment.

Author Contributions: Software, M.M.; Writing—original draft preparation, W.Y., S.W., G.Z., A.I.; writing—review and editing, S.W., J.H., G.Z., A.I., M.J.M., M.N.J., C.V.; supervision, J.H. and C.V.

Funding: This research received no external funding.

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

References

1. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
2. Habib, K.; Torjusen, A.; Leister, W. A novel authentication framework based on biometric and radio fingerprinting for the IoT in eHealth. In Proceedings of the 2014 International Conference on Smart Systems, Devices and Technologies (SMART), Paris, France, 20–24 July 2014; pp. 32–37.
3. Macedo, M.J.; Yang, W.; Zheng, G.; Johnstone, M.N. A comparison of 2D and 3D Delaunay triangulations for fingerprint authentication. In Proceedings of the 2017 Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017; pp. 108–115.
4. Lai, Y.-L.; Jin, Z.; Teoh, A.B.J.; Goi, B.-M.; Yap, W.-S.; Chai, T.-Y.; Rathgeb, C. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognit.* **2017**, *64*, 105–117.
5. Masek, L. Iris Recognition. Available online: https://www.peterkovesi.com/studentprojects/libor/ (accessed on 19 April 2019).
6. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
7. Blasco, J.; Peris-Lopez, P. On the Feasibility of Low-Cost Wearable Sensors for Multi-Modal Biometric Verification. *Sensors* **2018**, *18*, 2782. [CrossRef] [PubMed]
8. Arjona, R.; Prada-Delgado, M.; Arcenegui, J.; Baturone, I. A PUF-and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors* **2018**, *18*, 2429. [CrossRef]
9. Kantarci, B.; Erol-Kantarci, M.; Schuckers, S. Towards secure cloud-centric internet of biometric things. In Proceedings of the 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, Canada, 5–7 October 2015; pp. 81–83.
10. Karimian, N.; Wortman, P.A.; Tehranipoor, F. Evolving authentication design considerations for the internet of biometric things (IoBT). In Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, Pittsburgh, PA, USA, 1–7 October 2016; p. 10.
11. Maček, N.; Franc, I.; Bogdanoski, M.; Mirković, A. Multimodal Biometric Authentication in IoT: Single Camera Case Study. In Proceedings of the 8th International Conference on Business Information Security, Belgrade, Serbia, 15 October 2016; pp. 33–38.
12. Shahim, L.-P.; Snyman, D.; du Toit, T.; Kruger, H. Cost-Effective Biometric Authentication using Leap Motion and IoT Devices. In Proceedings of the Tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), Nice, France, 24–28 July 2016; pp. 10–13.
13. Dhillon, P.K.; Kalra, S. A lightweight biometrics based remote user authentication scheme for IoT services. *J. Inf. Secur. Appl.* **2017**, *34*, 255–270. [CrossRef]
14. Punithavathi, P.; Geetha, S.; Karuppiah, M.; Islam, S.H.; Hassan, M.M.; Choo, K.-K.R. A Lightweight Machine Learning-based Authentication Framework for Smart IoT Devices. *Inf. Sci.* **2019**. [CrossRef]

15. Yang, W.; Hu, J.; Wang, S. A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement. *IEEE Trans. Inf. Forensics Sec.* **2014**, *9*, 1179–1192. [CrossRef]
16. Yang, W.; Hu, J.; Wang, S.; Stojmenovic, M. An Alignment-free Fingerprint Bio-cryptosystem based on Modified Voronoi Neighbor Structures. *Pattern Recognit.* **2014**, *47*, 1309–1320.
17. Wang, S.; Yang, W.; Hu, J. Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs. *Pattern Recognit.* **2017**, *66*, 295–301. [CrossRef]
18. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634. [CrossRef]
19. Ratha, N.K.; Chikkerur, S.; Connell, J.H.; Bolle, R.M. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 561–572. [CrossRef] [PubMed]
20. Zuo, J.; Ratha, N.K.; Connell, J.H. Cancelable iris biometric. In Proceedings of the 2008 19th International Conference on Pattern Recognition, Tampa, FL, USA, 8–11 December 2008; p. 4.
21. Hämmerle-Uhl, J.; Pschernig, E.; Uhl, A. Cancelable iris biometrics using block re-mapping and image warping. In Proceedings of the 12th International Conference on Information Security, Pisa, Italy, 7–9 September 2009; pp. 135–142.
22. Kanade, S.; Petrovska-Delacrétaz, D.; Dorizzi, B. Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009; pp. 120–127.
23. Pillai, J.K.; Patel, V.M.; Chellappa, R.; Ratha, N.K. Sectored random projections for cancelable iris biometrics. In Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 14–19 March 2010; pp. 1838–1841.
24. Jenisch, S.; Uhl, A. Security analysis of a cancelable iris recognition system based on block remapping. In Proceedings of the 2011 18th IEEE International Conference on Image Processing (ICIP), Brussels, Belgium, 11–14 September 2011; pp. 3213–3216.
25. Hämmerle-Uhl, J.; Pschernig, E.; Uhl, A. Cancelable iris-templates using key-dependent wavelet transforms. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; p. 8.
26. Rathgeb, C.; Breitinger, F.; Busch, C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; p. 8.
27. Quan, F.; Fei, S.; Anni, C.; Feifei, Z. Cracking cancelable fingerprint template of Ratha. In Proceedings of the 2008 International Symposium on Computer Science and Computational Technology, Shanghai, China, 20–22 December 2008; pp. 572–575.
28. Li, C.; Hu, J. Attacks via record multiplicity on cancelable biometrics templates. *Concurr. Comput. Pract. Exp.* **2014**, *26*, 1593–1605. [CrossRef]
29. Tran, Q.N.; Wang, S.; Ou, R.; Hu, J. Double-layer secret-sharing system involving privacy preserving biometric authentication. In *User-Centric Privacy and Security in Biometrics*; Institution of Engineering and Technology: London, UK, 2017; pp. 153–170. [CrossRef]
30. Johnson, N.F.; Jajodia, S. Exploring steganography: Seeing the unseen. *Computer* **1998**, *31*, 26–34. [CrossRef]
31. Ma, L.; Tan, T.; Wang, Y.; Zhang, D. Efficient iris recognition by characterizing key local variations. *IEEE Trans. Image Process.* **2004**, *13*, 739–750. [CrossRef] [PubMed]
32. VeriEye, S.D.K. Neuro Technology. Available online: http://www.neurotechnology.com/verieye.html (accessed on 19 April 2019).
33. Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. A Fingerprint and Finger-vein Based Cancelable Multi-biometric System. *Pattern Recognit.* **2018**, *78*, 242–251. [CrossRef]
34. Wang, S.; Deng, G.; Hu, J. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognit.* **2017**, *61*, 447–458. [CrossRef]
35. Boncelet, C.G.J.; Marvel, L.M.; Retter, C.T. Spread Spectrum Image Steganography. U.S. Patent No. 6,557,103, 29 April 2003.
36. Agrawal, N.; Gupta, A. DCT domain message embedding in spread-spectrum steganography system. In Proceedings of the Data Compression Conference, Snowbird, UT, USA, 16–18 March 2009; p. 433.
37. Dumitrescu, S.; Wu, X.; Wang, Z. Detection of LSB steganography via sample pair analysis. *IEEE Trans. Signal Process.* **2003**, *51*, 1995–2007. [CrossRef]

38. Qi, X.; Wong, K. An adaptive DCT-based mod-4 steganographic method. In Proceedings of the 2005 IEEE International Conference on Image Processing, Genova, Italy, 11–14 September 2005.
39. Online Steganography Program. Available online: https://stylesuxx.github.io/steganography/ (accessed on 19 April 2019).
40. Yang, W.; Hu, J.; Wang, S.; Chen, C. Mutual dependency of features in multimodal biometric systems. *Electron. Lett.* **2015**, *51*, 234–235. [CrossRef]
41. Yang, W.; Wang, S.; Zheng, G.; Chaudhry, J.; Valli, C. ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures. *J. Supercomput.* **2018**. [CrossRef]
42. CASIA-IrisV3. Available online: http://www.cbsr.ia.ac.cn/IrisDatabase.htm (accessed on 15 April 2019).
43. MMU-V1 Iris Database. Available online: https://www.cs.princeton.edu/~{}andyz/irisrecognition (accessed on 10 June 2019).
44. Proença, H.; Alexandre, L.A. UBIRIS: A noisy iris image database. In Proceedings of the 13th International Conference on Image Analysis and Processing, Cagliari, Italy, 6–8 September 2005; pp. 970–977.
45. Yang, W.; Wang, S.; Zheng, G.; Valli, C. Impact of feature proportion on matching performance of multi-biometric systems. *ICT Express* **2018**, *5*, 37–40. [CrossRef]
46. Yang, W.; Hu, J.; Wang, S.; Wu, Q. Biometrics based Privacy-Preserving Authentication and Mobile Template Protection. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 7107295. [CrossRef]
47. Zhao, D.; Luo, W.; Liu, R.; Yue, L. Negative iris recognition. *IEEE Trans. Dependable Secur. Comput.* **2015**. [CrossRef]
48. Daugman, J.; Downing, C. Searching for doppelgängers: Assessing the universality of the IrisCode impostors distribution. *IET Biom.* **2016**, *5*, 65–75. [CrossRef]
49. Ouda, O.; Tsumura, N.; Nakaguchi, T. Tokenless cancelable biometrics scheme for protecting iris codes. In Proceedings of the 2010 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, 23–26 August 2010; pp. 882–885.
50. Zhao, D.; Fang, S.; Xiang, J.; Tian, J.; Xiong, S. Iris Template Protection Based on Local Ranking. *Secur. Commun. Netw.* **2018**, *2018*, 4519548. [CrossRef]
51. Radman, A.; Jumari, K.; Zainal, N. Fast and reliable iris segmentation algorithm. *IET Image Process.* **2013**, *7*, 42–49. [CrossRef]