IEEE Open Journal of the Computer Society

Received 28 November 2021; accepted 16 December 2021. Date of publication 24 December 2021;
date of current version 13 January 2022. The review of this paper was arranged by Associate Editor Peng Li.

Digital Object Identifier 10.1109/OJCS.2021.3138332

A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol

QUANG NHAT TRAN, BENJAMIN PETER TURNBULL, MIN WANG (Member, IEEE), AND JIANKUN HU (Senior Member, IEEE)

The University of New South Wales, Canberra, ACT 2600, Australia

CORRESPONDING AUTHOR: JIANKUN HU (e-mail: j.hu@adfa.edu.au).

This work was supported by ARC funds under Grants DP190103660, DP200103207, and LP180100663.

ABSTRACT Biometric authentication is, over time, becoming an indispensable complementary component to traditional authentication methods that use passwords and tokens. As a result, the research interest in the protection techniques for the biometric template has also grown considerably. In this paper, we present a light-weight AI-based biometric authentication that operates based on the binary representation of a biometric instance. In details, a binary classifier will be trained using the binary strings that represent the intraclass and interclass biometric subjects. The Support Vector Machine and Multi-layer Perceptron Neural Network are chosen as the classifier to evaluate the fingerprint-based and iris-based authentication capability. Afterward, the authenticated biometric string is fed to a hash function to produce a hash value, which is to be used in a Zero-Knowledge-Proof Protocol for the purpose of privacy preservation. In order to improve the recognition of the classifier, we devise a simple yet efficient strategy to enhance the discriminativeness of the binary strings and name it the Composite Features Retrieval. We evaluated the proposed method with the four publicly available fingerprint datasets FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2 and the iris dataset UBIRISv1. The promising performance shows this method's capability.

INDEX TERMS Biometrics, multilayer perceptron, neural network, support vector machine, binary.

I. INTRODUCTION

Biometric authentication systems have blossomed over the last few years as the mobile devices are becoming more and more popular. As biometrics cannot be forgotten or lost like passwords or token, such authentication method is a must-have feature in any mobile phones and devices. Biometrics are also increasingly used as a second factor of authentication, especially as the costs of such systems are quickly lowering.

A normal process of using biometric authentication requires two steps:

- Enrollment: The biometric samples are presented to the sensor. The features of the samples are enrolled and stored as a template.
- Authentication: A query biometric sample is presented to the sensor. The same features are extracted and compared with the stored template. A matching decision means the pass of the authentication.

However, this process is vulnerable to a template compromise attack which can expose the important features of the biometrics. If a malicious adversary is able to retrieve this template, not only can they use it to cross-authenticate other applications that use the same template, but also the owner loses one biometric forever. Biometric authentication has been widely deployed in mobile devices such as mobile phones and laptops which are easily lost or get stolen. Once such device is in the wrong hands, there exist many adversary attacks that can retrieve sensitive information or data stored in the platform via side channel attacks [1]. These include hill-climbing attacks on the embedded biometrics template [2], for example. Given these attacks, there have been measures to protect the biometric template. These can be partitioned into Information Hiding Techniques, Protocol-based Protection, Non-invertible Transformation, and Direct Biometric Key Generation [3]. Cancellable biometrics template is a popular method due to its

simplicity and the capacity of revoking the compromised template [4]–[9]. However, most of the transformation-based cancellable template designs are vulnerable to attacks via record multiplicity [10]. Gunasinghe and Bertino have proposed an interesting privacy-preserving iris biometrics authentication framework by embedding the support vector machine (SVM) into the zero knowledge protocol (ZKP) [11]. There exist two issues with this framework: (1) Biometrics query samples fed into the SVM classifier need to go through the error correction code (ECC). Hence, it could potentially distort the original distribution of biometrics samples, resulting in a classifier that is highly dependent on a specific ECC in use. It could also cause the potential issue of over-fitting. (2) In order to achieve the authentication accuracy performance, this framework needs to hard-code the mapping between the SVM classifier's class label and the template string. This secret mapping, which could be easily revealed once the device has been compromised.

In this paper, we present an enhanced privacy-preserving biometrics fingerprint authentication scheme which can address these problems. Our enhancements are from these main aspects: (1) We move the ECC component to the output of the SVM classifier and use the hashed value of the ECC output as the secret participating in the subsequent ZKP protocol. The proposed scheme does not distort the original biometrics feature distribution that is fed into the SVM classifier and does not store any secret in the device either. (2) In order to address the potential issue of performance degradation by removing the hard-coded secret mapping, we propose a composite biometric feature retrieval. The proposed scheme does not distort the original biometric feature distribution that is fed into the classifier and does not store any secret in the device either. Experimental evaluation of the proposed scheme is conducted over the public fingerprint databases FVC2002-DB1, FVC2002-DB2, and FVC2002-DB3 [12].

The rest of the paper is organized as follows: Section II reviews the related work in the field; the details of our method are presented in Section III while experimental results are shown in Section IV; finally, Section V concludes the paper.

II. RELATED WORK

SVM is a popular machine learning technique and has been widely used, especially in the field of biometric authentication. Jonsson *et al.* [13] showed their support for the hypothesis that SVM is able to retrieve the discriminatory features from the training dataset to build a robust model for face classification by performing extensive experiments to evaluate the influence of the representation space and the photometric normalization on SVM's performance. Park and Park [14] generated iris codes using two Gabor filters and applied SVM to create a fused score. There have been some other works that employed the same concept of using SVM as the tool for score fusion: Wang and Han [15] presented a multimodal biometric authentication scheme of face and iris that considers score fusion as a classification problem which is solved using SVM. Wang and Han [16] proposed a multimodal biometric authentication system that integrates face, iris, and palmprint in which all modality combinations are assessed and applied by parallel SVM's for scores fusion. Kang and Park [17] proposed a multi-unit iris authentication that leverages the SVM as the tool for score fusion. Vanthana and Muthukumar [18] used SVM for iris authentication in which iris features are extracted using Gray Scale Co-occurence Matrix and Hausdorff Dimension). However, the authors did not report on the accuracy performance of the proposed method. In addition, this method still requires the storage of the template image. Liau and Isa [19] improved the performance by applying a feature selection process to select an optimal feature set. Targeting the gender classification problem, Bansal *et al.* [20] achieved an accuracy rate of 83.06% when using the SVM to classify the irises.

SVM has also shown robustness when working specifically with fingerprints. In 2000, Yao *et al.* [21] utilized a multiclass strategy based on Error Codes Corrections with FingerCode [22] and showed that SVM shows promising performance in comparison with other methods. In 2010, Kristensen [23] utilized the SVM to perform a four-class fingerprint classification based on the singular point type. The overall accuracy achieved though was still limited as accurate singular point detection on fingerprint was still unstable at the time. Chen *et al.* [24] proposed to use a SVM as a filter to identify and reject the truncated fingerprint images, thus improving the accuracy of the proposed fingerprint authentication system to 90.7%. Alias [25] presented an SVM-based fingerprint classification model that achieved accuracy of 94.7%. Recently, Do [26] proposed to train a neural network on top of the SVM classifiers that are trained from the features to improve the classification performance. Though achieving the maximum rate of 96.70%, the author implemented this method on a self-collected dataset with a vast amount of data, which is an advantage for the use of neural network training. It would be more comprehensive if the publicly available datasets FVC were used.

In addition to the traditional biometrics, the SVM classifier has also been applied to other modalities. Hejazi *et al.* [27] explored the use of one-class and binary SVM with different feature extraction algorithms on the Electrocardiogram (ECG), showing that given sufficient data, one-class SVM is a robust option for ECG verification. Eude and Chang [28] presented an SVM-based model for the authentication of keystroke dynamic. Ali and Tapert [29] also targeted keystroke dynamic but proposed a hybrid approach that uses a Partially Observable Hidden Markov Model (POHMM) for features extraction and a one-class SVM for authentication. The proposed method achieved an average EER of 0.086% on the CMU keystroke dataset.

The Multilayer Perceptron (MLP) Neural Network has also been applied as in the field of biometric. As early as 1991, Leung *et al.* [30] used an MLP to extract the minutiae of the fingerprint image for matching. Semwal *et al.* [31] devised an MLP-based gait identification system that can predict early stage of diseases that are related to human walking. Mai *et*

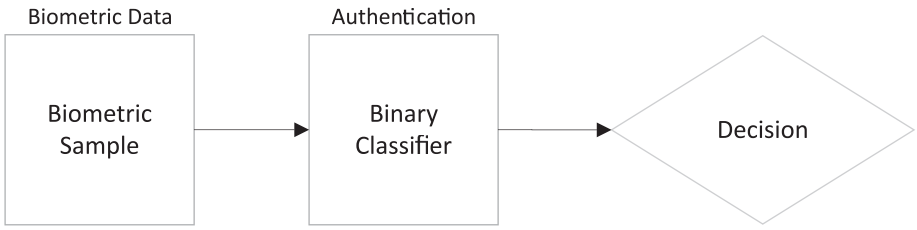


FIGURE 1. Traditional authentication.

al. [32] implemented both the MLP and the Radial Basis Function Neural Networks for Electrocardiogram (ECG) classification, achieving accuracy rates of above 98% and 97%, respectively. Gawande and Ladhake [33] also employed a single-hidden-layer MLP that takes ten features (seven statistical and three morphological) as input. This scheme reported accuracy of 99.76%.

On the other hand, there have been a myriad of works on integrating the Zero-Knowledge Proof protocols with biometric authentication [34]–[36], as such approaches help authenticate a user using the biometric data without the need to present it. The central concept shared among the most of these works is to integrate multi-factor authentication, including biometrics authentication into a cryptography Zero-Knowledge Proof protocol to authenticate a user without having to expose the biometric data, thus achieving privacy preservation. Compared with the popular approach using cancellable templates for the privacy protection, embedding a classifier such as the SVM into the ZKP protocol has the advantage of hiding the biometric template in a cryptography strong commitment. However, classification (e.g, SVM)-based approaches normally possess an inferior authentication accuracy performance compared with conventional template based matching performance. Hence, privacy-preserving biometrics authentication schemes based on embedding a classifier with the ZKP protocol would often require some extra elements of secrets in the protocol which would compromise its privacy-preserving strength. A representative scheme [11] would need to hard-coded secret mapping between a class (subject) label of the multi-class SVM classifier and the binary template stream that is hidden in the commitment of the ZKP. In their experimental evaluation, the size of the subjects is less than 300 which could be easily broken via a brute-force attack.

III. PROPOSED METHOD

In our work, beside the traditional strategy that uses the features from a single image illustrated in Fig. 1, we proposed a strategy that utilizes the composite features from double images as indicated in Fig. 3. This strategy combines the features from two images of the sample biometric subject to create the so-called composite feature, which is used for both training and testing the classifier.

In the first stage, which is illustrated in the Fig. 2, the biometric data is processed and filtered by a classifier before being corrected by the ECC. In more detail, first, biometric features are extracted and represented in the form of binary representation. Then, a model for each subject is trained using the binary data. When a query comes, after its features in the binary format have been retrieved, the model verifies the authenticity of the query. If it is authenticated by the model, the query is passed to the ECC to be prepared for hash string generation, which is described in later sections.

Due to the flexibility of the scheme, any biometric features that can be represented in binary form is compatible with our proposed scheme, though a different composite biometric feature might be used. In this paper, we evaluate the proposed scheme with fingerprint and iris, which are among the most widely used biometric modalities.

A. FINGERPRINT WITH BITSTRING REPRESENTATION BY NORMALIZED LOCAL STRUCTURES

The raw fingerprint bitstring representation proposed in [37] will be adopted. This single fingerprint image based feature presentation is constructed from the normalized local structures. At first, the minutiae of a fingerprint are extracted. Then, for each minutia being set as the reference, two sets of local structure features are extracted: Minutiae-based Local Structure (MBLS) and Texture-Based Local Structure (TBLS). As two sets of features are extracted, a subspace projection is applied to reduce the dimensionality of both feature sets before fusion. The fused local structures from a set of fingerprints are fed into a K-means clustering to produce K clusters. As a query fingerprint is assessed, it goes through the same process. Its bitstring b_f is created by applying the K-means clustering based on the clusters created before. The i-th bit is set to 1 if the i-th cluster contains any minutia of the fingerprint. After this process, a fingerprint is represented by a 4,500 b long binary string. A detailed description of this method can be found in [37].

B. IRIS WITH BITSTRING REPRESENTATION BY PERCEPTUAL HASH

Perceptual hash (pHash) of a multimedia file is its fingerprint that is derived from its content's features [38]. In this paper, we use the Discrete Cosine Transformation (DCT) pHash from the pHash library implemented by Zauner [39]: At first, the input image is converted to greyscale using luminance. Afterward, the image is resized to the size of 32×32 to simplify the computation of the DCT by using a 7×7 kernel for convolution. The DCT matrix is generated based on

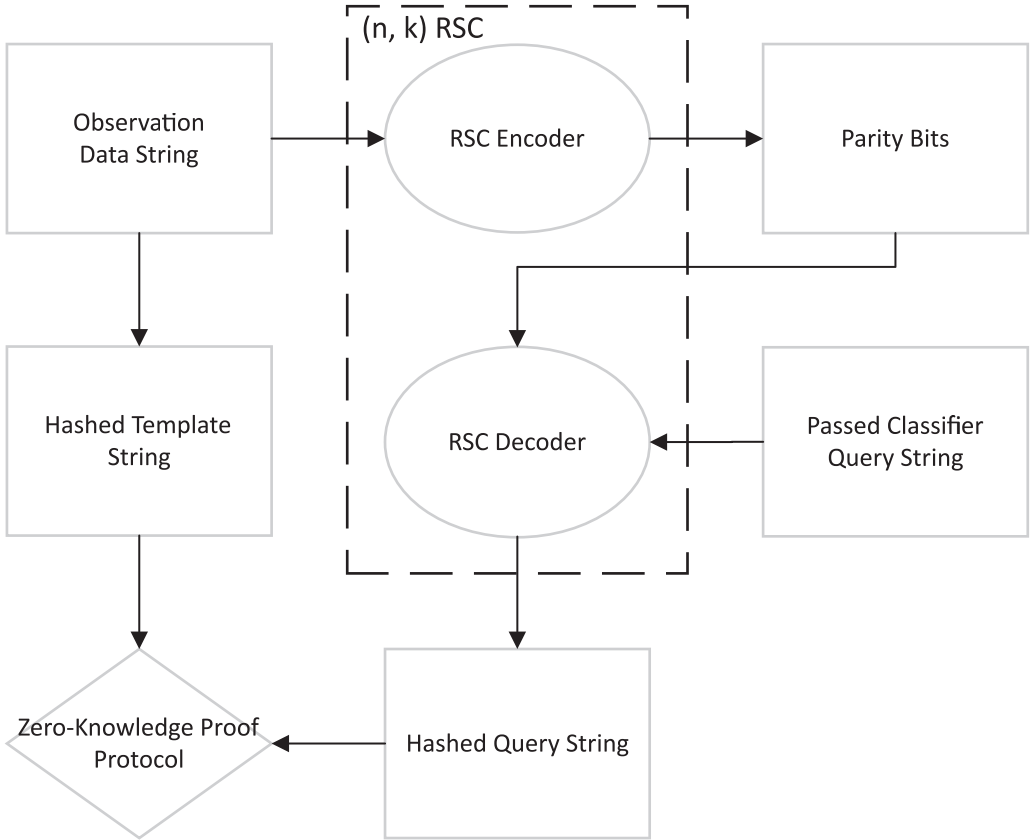


FIGURE 2. Overall scheme.

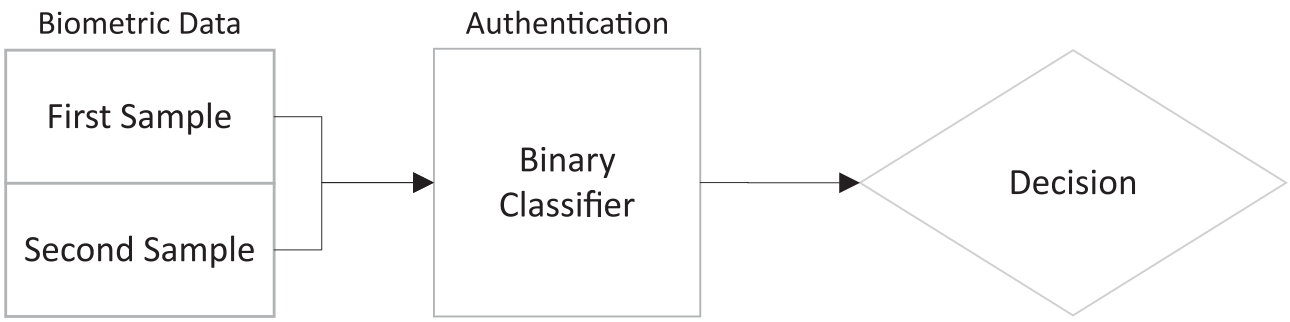


FIGURE 3. Composite feature-based authentication.

this resized image. A 8×8 DCT coefficient matrix is then calculated. The pHash value is computed by normalizing the elements of the one dimensional array created from the DCT coefficient matrix with its median. The details of how pHash works and is implemented can be found in [39].

Following the method in [11], the pHash of an iris image is extracted as follows: First, a segmentation process is applied onto the image to identify the iris region. After that, the pHash of the segmented iris image is generated. This step results in an integer in the range of $[0, 2^{64} - 1]$. This number is then translated to its corresponding binary form, which is used to represent the iris image.

C. COMPOSITE FEATURES RETRIEVAL

Traditional biometric authentication uses the features extracted from a single biometric image. However, due to the noise, the features extracted from this single biometric image are not discriminative enough. Importantly, if these features are used for template construction, the error rates are hypothetically high. Therefore, it is crucial that stable features are selected to be used for matching. We refer to this process as: Composite Features Retrieval (CFR). With the sparse binary representation from [37], this process is as simple as follows:

Given two binary representations b_1 and b_2 that belong to the same subject, a new binary representation b_c with the same

TABLE 1. Number of Samples

	Fingerprint		Iris	
	Traditional	CFR	Traditional	CFR
Samples/subject	8	28	5	10
Total samples	800	2800	1205	2410

TABLE 2. Amount of Data Used for Testing and Training for Each Biometric Subject in a Database

		FVC Databases		UBIRIS	
		Traditional	CFR	Traditional	CFR
Training	Positive	6	22	4	8
	Negative	594	2178	960	1920
Testing	Positive	2	6	1	2
	Negative	198	594	240	480

length is constructed by selecting only the common bit 1's positions between two binary strings. The newly generated binary string b_c is the input data to the model trainer.

Upon applying the CFR, the number of samples per subject increases: The FVC databases now, instead of having eight samples per subject as they did previously, contain $\binom{8}{2} = 28$ samples per subject. Similarly, the original UBIRISv1 database has 241 subjects with 5 samples each while the CFR-based strategy has $\binom{5}{2}$ samples per subject. The detailed comparison of before and after applying the CFR is shown in Table 1

Prior to training a model, we label binary strings from the same subject as positive data while those that are from different subject as negative data. How these two types of data are used is presented in the next sections.

D. AI-BASED CLASSIFIERS

In this section, we will present the details of the settings for each AI-based classifiers we employ: the Support Vector Machine and the Multilayer Perceptron Neural Network.

First, we construct a dataset for each of the subjects in a database. Afterward, we separate this dataset such that: 80% of the data is used for training while the rest 20% is used for testing. The specific amount of data that we use for training and testing is different for each strategy. This information is presented in the Table 2.

As we can see, for fingerprint, there will be $2 \times 100 = 200$ positive tests and 198×100 negative tests for the traditional strategy. On the other hand, the CFR-based strategy yields $6 \times 100 = 600$ positive tests and $594 \times 100 = 59,400$ negative tests. Similarly, traditional strategy for iris yields 241 positive and 57,840 negative tests while CFR-based strategy yields 482 positive and 115,680 negative tests.

1) SUPPORT VECTOR MACHINE CLASSIFIER

SVM is a widely applied classifier [40]. Given a set of classes Y and a set of attributes X with $|Y|$ and $|X|$ being the total number of classes and attributes, respectively, the Support Vector Machine (SVM) finds the hyper planes that assign each attribute x in the set X to a class y in the set Y. In our scheme,

TABLE 3. Parameters Used for the MLP Neural Network Training

Parameter	Value
Number of hidden layers	1
Number of neurons/hidden layers	100-500
Activation function	ReLU
Solver	Adam
Alpha	10^{-4}
Learning rate	0.001
Maximum number of iterations	200

we have chosen SVM for subject identification due to the following reasons:

- The publicly available databases for fingerprints and iris posses limit number of samples per subject. Hence, the model has to be trained in a data-restricted environment.
- The purpose of the scheme is to verify a user's authenticity. Therefore, it is a binary decision: Yes/No.

SVM does not require a huge amount of data to train a model. More importantly, SVM was traditionally designed for binary decision. Hence, we believe that SVM is an appropriate choice for the verification role.

SVM uses some kernel functions to optimize the process of assigning training data x to its associated class y. Similar to [11]'s, our method uses Radial Basis Function (RBF) as the kernel function whose parameters C and γ are chosen from a 10-fold cross validation grid search. Our proposed scheme differs in the sense that the SVM we use outputs a binary decision, instead of the class label as in [11]. This is because we want the classifier to give a yes/no decision without exposing any information about the subjects in the database.

2) MULTI-LAYER PERCEPTRON NEURAL NETWORK

In addition to the SVM, we also employed the Multi-layer Perceptron (MLP) Neural Network to evaluate and compare the performance. MLP belongs to the Feed-forward Neural Network. It has three kinds of layers: input layer, hidden layer, and output layer. The data flows from the input layer to the hidden layer where all the computational tasks occur before it gets transfered to the output layer. While SVM is a good classifier against linearly distributed data, MLP is a strong tool to classify non-linearly separable data.

In our work, we implemented a vanilla neural network, the details of the parameters used are given in Table 3.

E. HASHED ECC

As a model is being trained, ECC is applied with one of the positive observations in the training dataset. Specifically, an (n, k) RSC is used to encode the observation where n is the codeword length and k is the number of parity bits that determines how many errors can be corrected. After this step, the k parity bits retrieved are stored along with the hash value of the observation. These parity bits are used for error corrections on the query binary string. Fig. 2 visualizes this process. In this section, we will present how we preprocess the biometric binary representation to input into the (n, k) RSC.

1) HASHED FINGERPRINT BITSTRING

At first, the 4500-bit string b_f is chunked down into groups of eight bits each. Since 4500 does not divide 8, we padded four bits of '0' to make the last byte complete. This yields a string of byte B_S of 563 bytes.

In our scheme, we use an RSC with a fixed codelength $n_f = 255$. The number of parity bits k_f that determines how many errors can be corrected ($\frac{k}{2}$) is dynamically changed. Since $n_f < 563$, the string of bytes is chunked into the length of $n_f - k_f$ bytes each as input for the RSC. For instance, given that $k_f = 32$, B_f consists of three sub-strings. The first two substrings are $(255 - k)$ byte-long while the last substring is $563 - 2(255 - k) = 53 + 2\,k$ byte-long. Normally the last substring is not long enough to be the input of the RSC scheme. The RSC will pad with the byte of '0' to make it long enough. In the encoding phase, the parity bits p_i for each substring are generated. After this phase, the set of parity bits $P = \{p_i\}_{i=1}^{3}$ for each substring are stored along with the hash of the input byte string. In the decoding phase, after the query is chunked and padded, the parity bits are appended to the end of each substring and inserted into the decoder. If there are maximum $\frac{k_f}{2}$ errors in a substring, it is correctable to the original byte string. The hash of the query is compared against the template hash stored in the system.

2) HASHED IRIS BITSTRING

The length l_i of the iris bitstring is 64-bit long. Hence, we applied an RSC with codelength $n_i = 127$. The number of parity bit k_i ranges are chosen such that: $l_i + k_i + p_i = n_i$ where p_i is the number of padded bits '0' due to the fact that the iris bitstring is not long enough to serve as the input of the RSC. After being corrected by the RSC, the hashed iris bitstring is stored with the parity bits.

F. CHAUM-PEDERSEN PROTOCOL

The Chaum-Pedersen is one of the interactive Zero Knowledge Proof protocols. It allows the verification of a secret without having to reveal it. In our case, it is used to authenticate the user if he can present the original hash string. Assume that **P** is the prover and **V** is the verifier. **P** needs to prove to **V** that he/she possesses the hash string S without revealing it.

Chaum-Pedersen Protocol [41]:

- Let G be a cyclic group of prime order q generated by some generator $g \in G$.
- Let C be a challenge space used by the verifier **V**, which is a subset of Z_q.
- **P** produces the triplet (u, v, w), $v = g^S$, $w = u^S$. The triplet is a public parameter which is accessible by both the prover and the verifier. S will become the commitment of the prover.

When **P** needs to prove to **V** that he owns the private biometrics hash string S, he randomly picks a number S_t from Z_q and calculates v_t and a w_t where $v_t \leftarrow g^{S_t}$ and $w_t \leftarrow u^{S_t}$ and send them to the verifier **V**. Upon receiving v_t and a w_t, **V** generates a challenge $c \in C$ and sends it to **P**. With the challenge c, **P** calculates $S_z \leftarrow S_t + S * c$ and sends it back to **V** as the answer. Finally, **V** checks if $g^{S_z} = v_t * v_c$ and $u^{S_z} = w_t * w_c$. If the equality holds, **P** is authenticated as the holder of the biometrics hash string S. In our proposed privacy-preserving scheme, the biometrics hash string S is generated on the spot. It is not stored anywhere and there is no secret mapping anywhere. The security strength depends primarily on the cryptography strength of the Chaum-Pedersen Protocol.

IV. EXPERIMENTAL RESULTS

In this section, we present the experimental results that we have conducted for the fingerprint databases FVC2002-DB1, FVC2002-DB2, FVC2002-DB3 and FVC2004-DB2 and the iris database UBIRISv1.

In order to evaluate the performance of the classifiers used, we use the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy. To calculate these measures, we will look at the following: True Positive (**TP**), False Positive (**FP**), True Negative (**TN**), and False Negative (**FN**).

- **FAR** is the probability that the model mistakenly accepts a sample that is not from the same subject with which the model was trained. It is given as the ratio of the number of falsely accepted samples (FP) to the total number of impostor tests: $FAR = \frac{FP}{n_I}$ where n_I is the total number of impostor tests.
- **FRR** is the probability that the model mistakenly rejects a sample that is from the same subject with which the model was trained. It is given as the ratio of the number of falsely rejected samples (FN) to the total number of genuine tests: $FRR = \frac{FN}{n_G}$ where n_G is the total number of genuine tests.
- **Accuracy** is the probability that the model correctly identifies the genuine as well as the impostors. It is given as the ratio of the sum of correctly identified genuine and impostor samples to the total number of tests conducted: $Acc = \frac{TP+TN}{n_I+n_G}$.

On the other hand, we also evaluate the biometric performance using the Equal Error Rate (EER). The details on how EER is generated will be presented in the next sections.

A. CLASSIFIERS' PERFORMANCE

1) FINGERPRINT

The classification performance of the SVM classifier and the MLP classifier for the fingerprint's FVC databases is presented in the Tables 4 and 5, respectively.

As we can see from the Table 4, the binary classification models for fingerprint trained with both strategies yield a very low FAR. We could also see that using the same strategy, the lower the quality of the images in the database is, the higher the FRR becomes. On the other hand, as we apply the CFR strategy, though the FAR slightly increases, the FRR decreases sharply.

Gunasinghe and Bertino [11] employed the same concept of using SVM for biometric authentication with ECC with

TABLE 4. Fingerprint's SVM Performance (%)

	FVC2002-DB1			FVC2002-DB2			FVC2002-DB3			FVC2004-DB2		
	FAR	FRR	Accuracy	FAR	FRR	Accuracy	FAR	FRR	Accuracy	FAR	FRR	Accuracy
Traditional	0.00	11.00	99.99	0.69	0.50	99.99	0.00	13.00	99.89	0.56	6.00	99.39
CFR	0.00	1.83	99.99	0.00	1.17	99.99	0.00	4.17	99.96	0.00	9.00	99.91

TABLE 5. Fingerprint's MLP Performance (%)

	FVC2002-DB1			FVC2002-DB2			FVC2002-DB3			FVC2004-DB2		
	FAR	FRR	EER	FAR	FRR	EER	FAR	FRR	EER	FAR	FRR	EER
Traditional	0.00	1.00	0.00	0.00	3.00	0.00	0.00	10.00	2.37	0.00	29.00	2.31
CFR	0.00	1.50	0.00	0.00	0.83	0.00	0.00	4.3	2.34	0.00	7.83	2.50

TABLE 6. Iris's Performance (%)

	SVM			MLP		
	FAR	FRR	Accuracy	FAR	FRR	Accuracy
Traditional	0.41	0.00	99.59	0.00	7.47	99.97
CFR	0.39	0.00	99.61	0.00	0.21	99.99

a Zero-Knowledge Proof, which achieved 0.21% FAR along with 21% FRR when implemented with iris. However, the ECC was applied on the biometric data before it is classified by the SVM model. Moreover, in their work, a multi-class SVM was used. This means that the SVM model will output a class label based on the input data. As the class label is used as one of the secrets for key derivation, it is likely to be hard-coded in the protocol. This poses security issue that an attacker can perform a series of attacks to learn which label corresponds to a dummy label.

The performance with MLP Neural Networks is presented in Table 5.

As we compare with SVM's performance, MLP performs better in terms of recognizing the impostors when CFR is employed. SVM even though shows a slight improvement when CFR is applied, the classifiers suffer from an increase in the FAR in all databases. On the contrary, except with FVC2002-DB1, MLP shows a sharp improvement when CFR is applied in all databases while the FAR is kept at 0%.

The better performance shown by MLP can be explained by the better ability to deal with non-linear data than SVM's counterpart. Though possessing the kernel functions that can work with non-linear data, SVM's ability to classify non-linear data is limited. More importantly, The minutiae on a fingerprint are distributed naturally randomly. This results in the non-linear distribution of the bits generated by [37]. Hence, using the same method to generate fingerprint bit string, MLP with its flexibility in working with non-linearity shows a better performance.

2) IRIS

The classification results of the SVM and MLP classifier is presented in Table 6, respectively.

As we can see, UBIRISv1's SVM performance kept FRR at 0.00% in both strategies, constrasting to the MLP that maintained FAR at 0.00%. In this situation, it can be said that the CFR-based MLP performs the best by rejecting all impostors while keep the FRR as low as less than 1%.

TABLE 7. Fingerprint's EER (%)

		SVM	MLP
FVC2002-DB1	Traditional	0.54	0.00
	CFR	0.33	0.00
FVC2002-DB2	Traditional	1.00	0.00
	CFR	0.00	0.00
FVC2002-DB3	Traditional	1.00	2.37
	CFR	2.17	2.34
FVC2004-DB2	Traditional	1.00	2.31
	CFR	2.47	2.50

TABLE 8. Iris's EER (%)

		SVM	MLP
UBIRISv1	Traditional	1.24	2.07
	CFR	0.41	0.0017

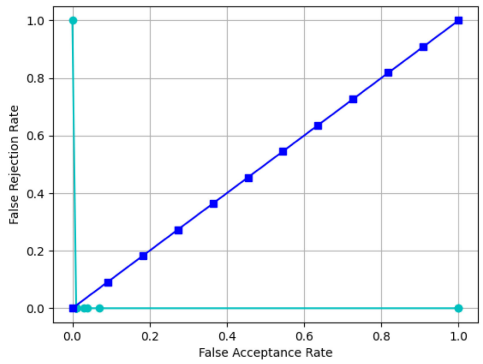
B. BIOMETRIC PERFORMANCE

We have looked at the classifier's ability in classifying the fingerprints. In this section, we will evaluate the biometric performance of these classifiers using the EER, which is the rate when FAR equals FRR. Kindly note that the FAR and FRR used to generate the EER are not the same as the ones mentioned in the previous section. Previously, the classifier generate two probabilities: one for the positive class and one for the negative class. To make a decision, the classifier chooses the class with the higher probability. Consequently, the FAR and the FRR are generated based on this decision. On the contrary, multiple thresholds will be set to determine the corresponding pair of FAR and FRR. By changing the thresholds, we can generate the EER.

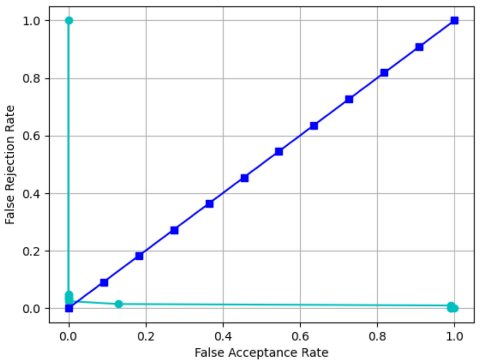
1) FINGERPRINT

The fingerprint recognition performance in terms of EER using different classifiers is presented in the Table 7. In addition, some of the Detection Error Tradeoff (DET) curves are shown in Fig. 4.

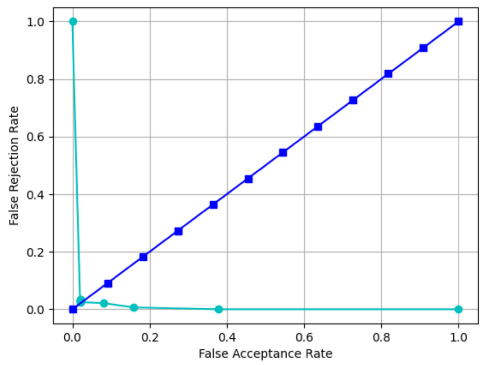
In terms of biometric performance, overall, both of the classifiers perform well in all cases with very low EER. Within the same database, the MLP classifier even shows unnoticeably higher EER than the SVM. On the other hand, it can be concluded that both the SVM and MLP classifier deliver good biometric performance. This is due to the stable binary representation from [37] decreasing the intraclass variation of the fingerprint. As a result, when applying the CFR, the



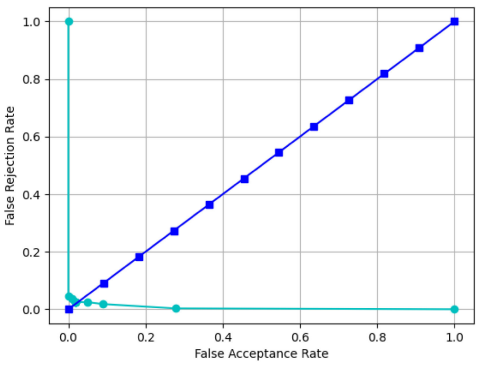
(a) SVM with Traditional Strategy implemented in FVC2004-DB2



(b) MLP with Traditional Strategy implemented in FVC2004-DB2

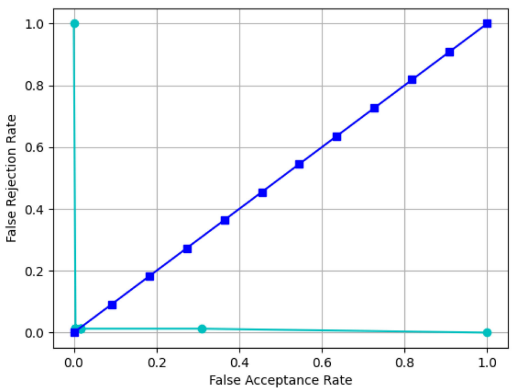


(c) SVM with CFR applied in FVC2004-DB2

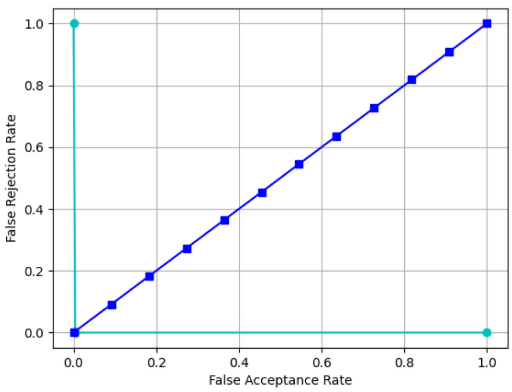


(d) MLP with CFR applied in FVC2004-DB2

FIGURE 4. **Fingerprint's DET curves.**



(a) SVM with Traditional Strategy for Iris Recognition



(b) SVM with CFR Strategy for Iris Recognition

FIGURE 5. **Iris's DET curves.**

newly generated binary representation will have less bit '1,' resulting in lower probability score. Consequently, at the same threshold, the FRR increases while FAR is not affected.

2) IRIS

Similar to the fingerprint's counterpart, iris's recognition performance with different classifiers is shown in Table 8. The DET curves for different classifiers under different strategy are presented in Fig. 5.

It can be seen that in this case, the CFR strategy performs better than the traditional strategy in both cases. This is related to the pHash feature that is used to represent each iris image: pHash is a 64-bit string that represents the features of the media file. This means that pHash was not originally devised for biometrics but instead for the generic recognition of the content in a file. Hence, pHash being the main features for iris recognition limits the discriminativeness of the iris's characteristics. Therefore, CFR contributes to lower the FRR

while the FAR is kept at a lower level at the same threshold, leading to a decrease in the EER.

V. CONCLUSION

In this paper, we have proposed a Composite Feature Retrieval scheme and evaluated its effectiveness with different AI-based classifiers. The biometric data is extracted with both the traditional and the CFR strategy. After being authenticated by a classifier, the bitstring is applied with an (n, k) RSC in order to produce the exact same hashed string, which is used in a Zero-Knowledge-Proof Protocol. We have evaluated our proposed scheme with four of the public fingerprint datasets FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2 and the UBIRISv1 dataset for iris. The results prove this method's reliability.

For the future research work, there are still ways to make a better templateless biometric authentication: First, we need to evaluate the safety of using the biometric model (i.e. if compromised, can a hacker rebuild a genuine sample from the model). Second, we should assess if the parity bits expose any information about the actual biometric data to ensure that the attacker cannot construct the original biometric data. Third, the use of pHash heavily influences both the classifier's performance and the biometric recognition performance. Hence, a more reliable bitstring for iris is much desired. Last but not least, although the SVM and MLP have shown a good performance for verification, finding another machine learning technique in which a model can be trained with a low amount of data is an interesting research topic.

REFERENCES

[1] C. Shepherd *et al.*, "Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis," *Comput. Secur.*, vol. 111, 2021, Art. no. 102471.

[2] E. Maiorana, G. E. Hine, and P. Campisi, "Hill-climbing attacks on multibiometrics recognition systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 900–915, May 2015.

[3] Q. N. Tran, B. P. Turnbull, and J. Hu, "Biometrics and privacy-preservation: How do they evolve?," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 179–191, Mar. 2021, doi: 10.1109/OJCS.2021.3068385.

[4] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, 2017.

[5] Q. N. Tran and J. Hu, "A multi-filter fingerprint matching framework for cancelable template design," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2926–2940, Jan. 2021, doi: 10.1109/TIFS.2021.3069170.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[7] J. B. Kho, J. Kim, I.-J. Kim, and A. B. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognit.*, vol. 91, pp. 245–260, 2019.

[8] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi, "A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template," *Pattern Recognit. Lett.*, vol. 42, pp. 137–147, 2014.

[9] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[10] C. Li and J. Hu, "Attacks via record multiplicity on cancelable biometrics templates," *Concurrency Computation: Pract. Experience*, vol. 26, no. 8, pp. 1593–1605, 2014.

[11] H. Gunasinghe and E. Bertino, "Privacy preserving biometrics-based and user centric authentication protocol for mobile devices," in *Proc. Netw. Syst. Secur.*, 2014, pp. 15–16.

[12] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 3, pp. 402–412, Mar. 2002.

[13] K. Jonsson, J. Kittler, Y. Li, and J. Matas, "Support vector machines for face authentication," *Image Vis. Comput.*, vol. 20, nos. 5/6, pp. 369–375, 2002.

[14] H.-A. Park and K. R. Park, "Iris recognition based on score level fusion by using svm," *Pattern Recognit. Lett.*, vol. 28, no. 15, pp. 2019–2028, 2007.

[15] F. Wang and J. Han, "Multimodal biometric authentication based on score level fusion using support vector machine," *Opto- Electron. Rev.*, vol. 17, no. 1, pp. 59–64, 2009.

[16] F. Wang and J. Han, "Robust multimodal biometric authentication integrating iris, face and palmprint," *Inf. Technol. Control*, vol. 37, no. 4, pp. 326–332, 2008.

[17] B. J. Kang and K. R. Park, "A new multi-unit iris authentication based on quality assessment and score level fusion for mobile phones," *Mach. Vis. Appl.*, vol. 21, no. 4, pp. 541–553, 2010.

[18] P. S. Vanthana and A. Muthukumar, "Iris authentication using gray level co-occurrence matrix and Hausdorff dimension," in *Proc. IEEE Int. Conf. Comput. Commun. Inform.*, 2015, pp. 1–5.

[19] H. F. Liau and D. Isa, "Feature selection for support vector machine-based face-iris multimodal biometric system," *Expert Syst. Appl.*, vol. 38, no. 9, pp. 11105–11111, 2011.

[20] A. Bansal, R. Agarwal, and R. Sharma, "SVM based gender classification using iris images," in *Proc. IEEE 4th Int. Conf. Comput. Intell. Commun. Netw.*, 2012, pp. 425–429.

[21] Y. Yao, P. Frasconi, and M. Pontil, "Fingerprint classification with combinations of support vector machines," in *Proc. Int. Conf. Audio-Video-Based Biometric Person Authentication*, 2001, pp. 253–258.

[22] A. K. Jain, S. Prabhakar, and L. Hong, "A multichannel approach to fingerprint classification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 21, no. 4, pp. 348–359, Apr. 1999.

[23] T. Kristensen, "Fingerprint identification–a support vector machine approach," in *Proc. Int. Conf. Agents Artif. Intell.*, vol. 1, pp. 451–458, 2010.

[24] C.-J. Chen, T.-W. Pai, and M. Cheng, "A support vector machine approach for truncated fingerprint image detection from sweeping fingerprint sensors," *Sensors*, vol. 15, no. 4, pp. 7807–7822, 2015.

[25] N. A. Alias and N. H. M. Radzi, "Fingerprint classification using support vector machine," in *Proc. IEEE 5th ICT Int. Student Project Conf.*, 2016, pp. 105–108.

[26] T.-N. Do, "Training neural networks on top of support vector machine models for classifying fingerprint images," *SN Comput. Sci.*, vol. 2, no. 5, pp. 1–12, 2021.

[27] M. Hejazi, S. Al-Haddad, S. J. Hashim, A. F. A. Aziz, and Y. P. Singh, "Non-fiducial based ECG biometric authentication using one-class support vector machine," in *Proc. IEEE Signal Process.: Algorithms, Architectures, Arrangements, Appl.*, 2017, pp. 190–194.

[28] T. Eude and C. Chang, "One-class SVM for biometric authentication by keystroke dynamics for remote evaluation," *Comput. Intell.*, vol. 34, no. 1, pp. 145–160, 2018.

[29] M. L. Ali and C. C. Tappert, "Pohmm/SVM: A hybrid approach for keystroke biometric user authentication," in *Proc. IEEE Int. Conf. Real-Time Comput. Robot.*, 2018, pp. 612–617.

[30] W. Leung, S. Leung, W. Lau, and A. Luk, "Fingerprint recognition using neural network," in *Proc. IEEE Neural Netw. Signal Process. Workshop*, 1991, pp. 226–235.

[31] V. B. Semwal, M. Raj, and G. C. Nandi, "Biometric gait identification based on a multilayer perceptron," *Robot. Auton. Syst.*, vol. 65, pp. 65–75, 2015.

[32] V. Mai, I. Khalil, and C. Meli, "ECG biometric using multilayer perceptron and radial basis function neural networks," in *Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc.*, 2011, pp. 2745–2748.

[33] P. Gawande and S. Ladhake, "Artificial neural network based electrocardiogram classification for biometric authentication," *Int. J. Comput. Appl.*, vol. 109, no. 2, pp. 6–9, 2015.

[34] H. Kikuchi, K. Nagai, W. Ogata, and M. Nishigaki, "Privacy-preserving similarity evaluation and application to remote biometrics authentication," *Soft Comput.*, vol. 14, no. 5, pp. 529–536, 2010.

[35] H. Gunasinghe and E. Bertino, "PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 1042–1057, Apr. 2018.
[36] W. Liu, X. Wang, and W. Peng, "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things," *IEEE Access*, vol. 8, pp. 8754–8767, 2019.
[37] J. B. Kho, A. B. Teoh, W. Lee, and J. Kim, "Bit-string representation of a fingerprint image by normalized local structures," *Pattern Recognit.*, vol. 103, 2020, Art. no. 107323.
[38] E. Klinger and D. Starkweather, *The open source perceptual hash library*. Dec. 2021, Accessed: 2010. [Online]. Available: http://phash.org/
[39] C. Zauner, "Implementation and benchmarking of perceptual image hash functions," Master's thesis, Austria, 2010.
[40] K. P. Bennett and E. J. Bredensteiner, "Duality and geometry in SVM classifiers," in *Proc. Int. Conf. Mach. Learn.*, 2000, pp. 57–64.
[41] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*. 2020.

QUANG NHAT TRAN received the B.S. degree majoring in computer science from New Mexico Highlands University, Las Vegas, NM, USA, in 2012, and the Master of Science degree by Research in 2017 from the University of New South Wales, Canberra, NSW, Australia, where he is currently working toward the Ph.D. degree. In 2013, he became a Lecturer of the Department of Computer Science and Technology, Posts and Telecommunication Institute of Technology in Hanoi, Vietnam. His research interests include computer security, biometric template protection, biometric cryptography, blockchain technology and applications.

BENJAMIN PETER TURNBULL received the bachelor degree in information technology (Software Engineering ((Honors) from University of South Australia, 2003 and Ph.D. degree in information technology from the University of South Australia, Canberra, NSW, Australia, 2007. He is an Associate Professor with the Australian Centre for Cyber Security, University of New South Wales, Sydney, NSW, Australia. His research interests include cyber-resilience, cyber-kinetic impact analysis and novel methods for network analysis. He previously worked for the Australian Defence Force.

MIN WANG (Member, IEEE) received the Ph.D. degree in computer science in 2020 from the University of New South Wales, Canberra, NSW, Australia, where she is currently a Postdoctoral Research Fellow. Her research interests include pattern recognition, machine learning, brain biometrics, and biocryptography.

JIANKUN HU (Senior Member, IEEE) received the B.E. degree from Hunan University, Changsha, China, in 1983, the master's degree by Research in computer science and software engineering from Monash University, Clayton, VIC, Australia, in 2000, and the Ph.D. degree in control engineering from the Harbin Institute of Technology, Harbin, China, in 1993. He is currently a Full Professor with the School of Engineering and Information Technology, University of New South Wales, Canberra, NSW, Australia. He was with Ruhr University, Bochum, Germany, on the prestigious German Alexander von Humboldt Fellowship 1995–1996, and from 1998 to 1999, he was a Research Fellow with Melbourne University, Melbourne, Australia. His main research interests include the field of cyber security, including image processing, forensics and machine learning where he has authored or coauthored many papers in high quality conferences and journals including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE. He was with the Editorial Board of seven international journals including the top venue IEEE TRANSACTIONS ON INFORMATION FORENSICS and Security and was a Security Symposium Chair of IEEE flagship conferences of IEEE ICC and IEEE Globecom. He has obtained ten ARC (Australian Research Council) grants and was with the prestigious Panel of mathematics, information and computing sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee.