Mathematical Biosciences and Engineering

MBE, 18(4): 4461–4476.
DOI: 10.3934/mbe.2021226
Received: 13 January 2021
Accepted: 22 April 2021
Published: 24 May 2021

http://www.aimspress.com/journal/MBE

Research article

Biometrics-based Internet of Things and Big data design framework

Kenneth Li-minn Ang[1,*] and Kah Phooi Seng[2]

[1] School of Science and Engineering, University of Sunshine Coast, Petrie, QLD 4502, Australia
[2] School of Engineering and Information Technology, UNSW Canberra, ACT 2612, Australia

* **Correspondence:** Email: lang@usc.edu.au.

Abstract: Application Specific Internet of Things (ASIoTs) has recently been proposed to address specific requirements for IoT. The objective of this paper is to serve as a framework for the design of ASIoTs using biometrics as the application. This paper provides comprehensive discussions for an ASIoT architecture considering the requirements for biometrics-based security, multimedia content and Big data applications. A comprehensive architecture for Biometrics-based IoT (BiometricIoT) and Big data applications needs to address three challenges: 1) IoT devices are hardware-constrained and cannot afford resource-demanding cryptographic protocols; 2) Biometrics devices introduce multimedia data content due to different biometric traits; and 3) The rapid growth of biometrics-based IoT devices and content creates large amounts of data for computational processing. The proposed BiometricIoT architecture consists of seven layers which have been designed to handle the challenges for biometrics applications and decision making. The latter part of the paper gives discussions for design factors for the BiometricIoT from four perspectives: 1) parallel divide-and-conquer (D&C) computation; 2) computational complexity; 3) device security; and 4) algorithm efficacies. Experimental results are given to validate the effectiveness of the D&C approach. The paper motivates the further research towards the research and development of ASIoTs for biometrics applications.

Keywords: Internet-of-Things; Application specific; biometric; Big data; parallel computation

1. Introduction

Due to the rapid progress in sensing, processing and cloud technology platforms, the Internet-of-Things (IoT) in recent years is increasingly becoming highly important and ubiquitous. The IoT gives the capabilities of connecting intelligent devices and objects to large networks and be accessible from

anywhere on the Internet. The market analysis from Gartner has commented that the IoT will account for 20% of new identity and access management (IAM) applications, with biometrics applications to play a key role [1]. The role of biometrics for authentication in consumer-based applications and devices is increasing rapidly. Some examples include the iPhone 8 from Apple which contains new face scanning and recognition technology, the "Aloha" video chat device from Facebook with a touchscreen and facial recognition technology [2], NEXT Biometrics fingerprint recognition technology [3], and the usage of face biometrics for driver identification and fatigue recognition [4]. The IoT together with the increasing usage of biometrics has significant potential in applications for smart homes, banking and finance, industry and manufacturing, healthcare and medicine, etc.

The rapid growth in Biometrics-based IoT (termed as BiometricIoT) leads to several challenges. A comprehensive architecture for BiometricIoT and Big data applications needs to address several challenges: 1) IoT devices are hardware-constrained and cannot afford resource-demanding cryptographic protocols—authentication and encryption of the biometric content need to be performed within the resource/power-constrained devices (a solution is to utilize lightweight cryptography protocols [5,6]; 2) Biometrics devices introduce multimedia data content due to different biometric traits [7,8]—various biometric attributes such as fingerprint, voice/speech, iris/retina, facial features, gait are not text-based or scalar data and may involve multimedia data (e.g., images captured from different types of sensors and devices which have to be authenticated on a central cloud server); and 3) The rapid growth of biometrics-based IoT devices and content creates large amounts of data for computational processing.

Biometrics authentication with the IoT architecture requires several additional functionalities to be incorporated into existing designs and implementations to handle the Challenges 1–3). Most designs and hardware for existing IoT architectures do not consider the need for multimedia attributes/features [9] or the need for transportation of multimedia data over the IoT communications network [10]. Some recent works on multimedia IoT can be found in [11–13]. If multiple biometric traits are considered at the same time (e.g., face and iris), this further increases the challenges. Big data analytics platforms or architectures to be integrated into the IoT need to consider multimodal feature extraction, analysis and decision making. Although recent years have seen advancing and major progress in the field of IoT [14,15], IoT with multimedia security requirements have not been comprehensively investigated. There is an important need for research into new designs and implementations for making IoT architectures to be more reliable and secure from the perspective of users and vendors. IoT security is essential for IoT objects to work effectively [16]. Without security, any connected object in IoT is subjected to risks and threats. There is a gap between existing research works and security solutions with biometrics which allows multimedia content and Big data computation in an IoT-based system.

In the past, some researchers have proposed three [17], four [18] and five layer [19] architectures for the IoT. These architectures might be general and not be able to fully address the need of specific applications. The concept of Application Specific Internet of Things (ASIoTs) [20] has recently been proposed. This paper addresses the challenges for an ASIoT architecture considering the specific needs for biometrics-based security, multimedia content and Big data. The novelty of this paper is the proposed Biometrics ASIoT architecture (BiometricIoT) architecture consists of seven layers. The seven layers in the architecture are: 1) Biometrics Identification Layer; 2) Biometrics Object Layer; 3) Biometrics Device Elements Layer; 4) Biometrics Communication Layer; 5) Biometrics Cloud Services Layer; 6) Big Biometrics Data Computation Layer; and 7) Biometrics Application Layer. The

additional layers in the BiometricIoT are proposed to deal with the specific requirements for biometrics applications. For example, the benefits of the Biometrics Object Layer are that it considers the physical objects which can be the biometrics sensors to produce multimedia contents due to the biometric traits with different modalities. The Big Biometrics Data Computation Layer is designed specifically to consider Big data including data computations for biometrics. This layer can accommodate various kinds of data including multimedia content such as video, image and audio generated by biometrics objects. The authors in [20] discussed several categories and types of ASIoTs, where a brief sketch of a biometrics IoT was one of the examples used for illustration. This paper provides comprehensive discussions for an ASIoT architecture considering the requirements for biometrics-based security, multimedia content and Big data applications.

Motivated by the aforementioned challenges, the work in this paper aims to serve as a full and comprehensive design framework for ASIoT using biometrics as the application. The security issues are also discussed for each layer in the BiometricIoT. Furthermore, the paper also gives discussions for various design factors for the BiometricIoT from four perspectives: 1) parallel divide-and-conquer (D&C) data computation; 2) computational complexity; 3) device security; and 4) algorithm efficacies. This paper is structured as follows: Section 2 discusses the BiometricIoT and seven-layer architecture. Section 3 gives discussions on the important design factors to be considered for the BiometricIoT. This section also gives theoretical discussions and experimental results to validate the algorithm efficacies. Section 5 gives some concluding remarks and suggests challenges and some potential research for the proposed framework.

2. Application-specific IoT (ASIoT) architecture for biometrics framework

This section discusses the Biometrics-based ASIoT (BiometricIoT) architecture. Figure 1 shows the BiometricIoT and its seven layers and an overview of the components for the different layers. This section also discusses the proposed Big Biometrics Computation Layer to consider Big data computations for biometrics. The architecture of the BiometricIoT is application-specific and can be contrasted with other works on the general IoT architectures which can be found in [21–23].

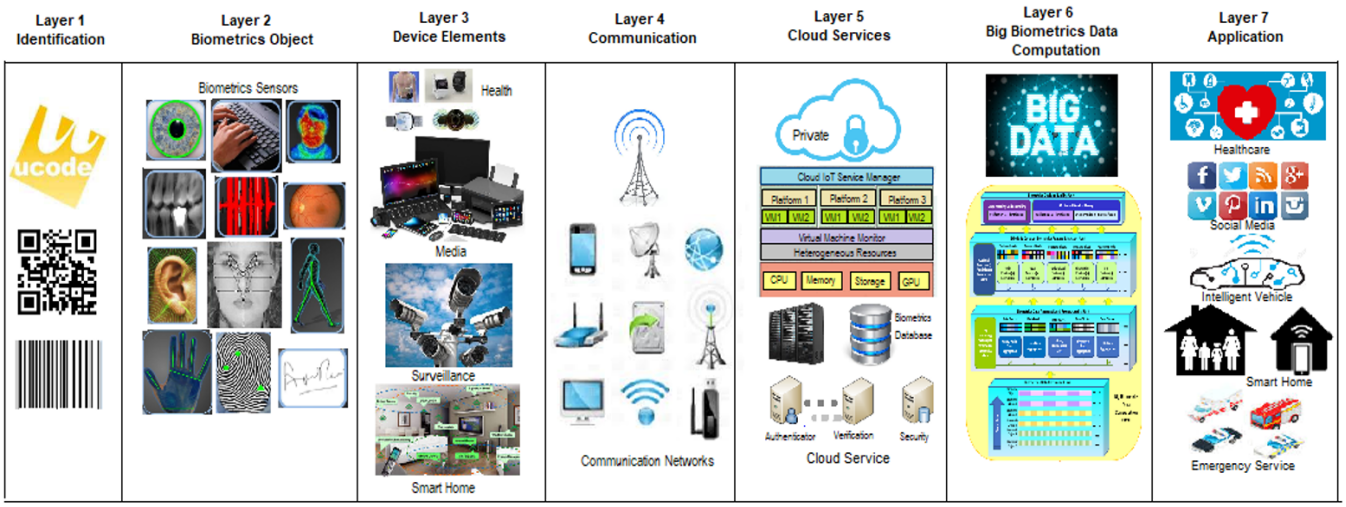

Figure 1. The proposed seven-layer BiometricIoT architecture and overview of components.

2.1. Layer 1: Biometrics Identification Layer

The Biometrics Identification Layer supplies the biometrics objects or things with a unique digital identifier which is permanent and global for the lifetime of the object. This unique identifier can then be used to refer to the biometrics object/thing with its characteristics and information history. The identifier can make use of available naming codes being used by manufacturers (e.g., EPC—electronic product codes, uCodes—ubiquitous codes) and addressing schemes such as IP addresses (e.g., IPv6). A combination of naming codes together with addressing schemes creates a unique identifier for the biometrics object.

2.2. Layer 2: Biometrics Object Layer

The Biometrics Object Layer performs the data collection from the biometric sensors and objects in the network. This could include sensing devices from fingerprint, voice/speech, iris/retina, facial features, gait features, or other biometric modalities. It is important to implement security and protection measures at this layer to mitigate against attacks conducted against the physical sensors. For example, side channel attacks [24,25] based on power consumption, timing information or electromagnetic leaks may reveal to an attacker useful information to retrieve secret keys. The physical IoT sensors are usually left out in the open and not stored in physically secure locations. Thus, an adversary can get in close proximity to launch the side-channel attacks. The author in [26] commented that existing physical layer security techniques may not be suitable for IoT applications compared to mobile devices (phones and tablets). This is particularly the case for biometrics IoT sensors due to its limited hardware, processing, storage, and energy resources. These important aspects for physical layer security for biometrics sensors have so far received limited attention in the literature. Further issues and potential attacks for this layer are jamming attacks [27,28] and tampering [29,30] of the biometric devices.

2.3. Layer 3: Biometrics Device Layer

The Biometrics Device Layer consists of wireless devices, nodes or motes which have the capability to send the captured biometrics data to other parts of the network. This could form part of the implementation for body sensor networks or other wearable devices. The wireless transmission of the biometrics data gives an opportunity for adversaries and attackers. It is important to implement security and protection measures at this layer to mitigate against attacks conducted against the data transmission. However, the implementation of these security protocols has to be designed to meet the requirements for IoT devices which are hardware-constrained. Biometric devices would have low computational power, storage capacity, and limited energy resources. A solution would be to use low-complexity encryption methods and lightweight cryptographic protocols to secure the biometrics data before transmission [5,6]. Further issues on design factors for device security are given in Section 3.

2.4. Layer 4: Biometrics Communication Layer

The Biometrics Communication Layer consists of three sub-layers: 1) Link Sub-Layer; 2) Network Sub-Layer; and 3) Transport Sub-Layer. The Link Sub-Layer has the responsibility for the

medium access control (MAC) protocols in the BiometricIoT. To meet the hardware constraints, a consideration is to implement and deploy MAC protocols with low-cost and/or low-power consumption wireless networks such as given in the IEEE 802.15.4 specification [31]. The IEEE 802.15.4 includes three security modes which can be utilized depending on the level of security required [32,33]: 1) Unsecured mode—this mode provides no security services and is not suitable for high security applications like the BiometricIoT; 2) ACL mode—this mode utilizes an access control list (ACL) and provides a limited amount of security services to reject transmission frames which do not originate from registered devices contained in the ACL. This mode does not provide encryption or cryptographic services; and 3) Secured mode—this mode provides several security suites including cryptographic protocols. These suites employ the advanced encryption standard (AES) in various modes of operations. An important security issue at this sub-layer is termed the backoff manipulation attack [34] where an attacker attempts to use its nodes to maximize its access to the medium by deliberately selecting a small backoff window, and thus deprive or reduce the legitimate node's access to the medium. The authors in [34] investigated this potential attack on IEEE 802.11 networks. The authors in [35] gave a study of potential attacks on the IEEE802.15.4 for a wireless body area network (WBAN) application, finding that a sophisticated backoff detection scheme successfully detected the backoff attacks.

The Network Sub-Layer has the responsibility for the routing and connectivity in the BiometricIoT. The IEEE 802.15.4 specification proposes the RPL (Routing over Low Power and Lossy Networks) protocol. Security issues at this sub-layer include network congestion, network traffic disruption and route changes when an adversary introduces false packets or routing details into the network. An example is the rank attack [36] when an adversary creates false nodes and violates the rank rule in RPL to create longer routing paths for data transmission. This has the effect of decreasing the overall performance of the network (e.g., delay and throughput) and consumes extra energy to deplete the network resources. Other possible routing attacks aim to reduce network performance by spoofing, misdirecting, packet dropping, generating routing loops, or injecting false error messages into the network. Several authors have considered these potential attacks which include Black Hole, Gray Hole, Worm Hole, Hello Flood, and Sybil. Further details for these attacks at the Network sub-layer can be found in [21].

The Transport Sub-Layer has the responsibility for the flow and congestion controls in the BiometricIoT. Two protocols which can be utilized at this sub-layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is a connection-oriented protocol and suffers from a high amount of data overheads for the communications. UDP is a connectionless protocol and does not guarantee packets to be delivered. However, authors in [37] have shown that techniques using UDP and application layer retransmission control could give an effective trade-off between transmission reliability and energy efficiency. Security issues at this sub-layer include de-synchronization attacks and flooding [38]. In de-synchronization attacks, an adversary aims to spoof messages in the network to cause retransmission of missing frames or report errors in reception. This misinforms the host node and causes it to re-transmit the data frames which will subsequently lead to depleting the node resources. A solution to this is to apply end-to-end authentication between communicating nodes so that the adversary cannot spoof the messages. Flooding is a resource exhaustion attack where an adversary repeatedly initiates a large number of new connection requests and blocks legitimate requests from being serviced.

2.5. Layer 5: Biometrics Cloud Services Layer

The Biometrics Cloud Services Layer consists of hardware and software architecture for the BiometricIoT. The cloud hardware architecture consists of servers, storage and network equipment and may deploy virtualization technology and parallel computational environments. The cloud software architecture consists of the services centre and the access centre. Most cloud services are powered by data centres. The data centre is the physical location which houses and run a cloud service. Some examples of cloud services are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The access centre provides the access control services to only allow authorized users. This layer could be implemented using private or public cloud components (e.g., from Amazon EC2, Google Cloud). It is important to implement security and protection measures at this layer to mitigate against attacks conducted against security and privacy attacks for cloud-based IoT [39] such as identity/location privacy, node compromise attacks, layer removing/adding attacks, and semi-trusted/malicious cloud security attacks. From these issues, one particularly relevant security issue for the BiometricIoT is the need for forward and backward security. The implications for forward security are that users which have just enrolled into the BiometricIoT should only be allowed to decipher encrypted messages which have been received after (and not before) they join the cloud services. Similarly, the implications for backward security are that revoked users should only be allowed to decipher messages which have been received before (and not after) leaving the cloud services. Further security issues are to secure end-to-end communications between the end of the Device Layer (e.g., gateway) and the Cloud Services Layer. A sub-layer can be designed to secure end to end communications between the gateway and the cloud servers without needing the control of the full communication path which is not possible for the global Internet.

2.6. Layer 6: Big Biometrics Data Computation Layer

The proposed architecture of Big Biometrics Data Computation Layer consists of four components: 1) Biometrics Centralized Unit (Bio_CU); 2) Biometrics Aggregation and Preprocessing Unit (Bio_AU); 3) Biometrics Feature Extraction Unit (Bio_FU); and 4) Biometrics Decision Making Unit (Bio_DU). The Bio_CU has the responsibility to extract the data from biometrics objects and devices. For multi-biometric data, this unit combines the biometric data from objects with the same identity which may have been transported using different routes through the network. With the integrated biometric sensors and installed plug-ins, the component devices or smart 'things' in the Device Elements Layer can send the sensed data from the biometrics objects in the Biometrics Objects Layer to the Biometrics Cloud Services Layer through a range of communication gateways in the Biometrics Communication Layer. The Bio_AU has the responsibility for the data aggregation role and performs the ordering of the data into blocks based on the identities of the blocks and biometrics modalities, and then feeds the ordered blocks into the Bio_FU. The Bio_FU makes use of divide and conquer (D&C) mechanisms for parallel computation of the biometrics data.

Section 3 gives further discussions on the D&C mechanisms using algorithm variants for PCA (principal component analysis) and LDA (linear discriminant analysis) which are suitable for large-scale D&C implementation in the BiometricIoT. The Bio_DU has the responsibility for the final decision making for the biometrics data. The Bio_DU can perform decision making for single modality and multiple modality biometric objects. The decision making for multimodal biometric objects

utilizes various fusion techniques (e.g., early fusion, late fusion) to perform the joint decision making tasks. Figure 2 shows the proposed architecture of the Big Biometrics Data Computation Layer.

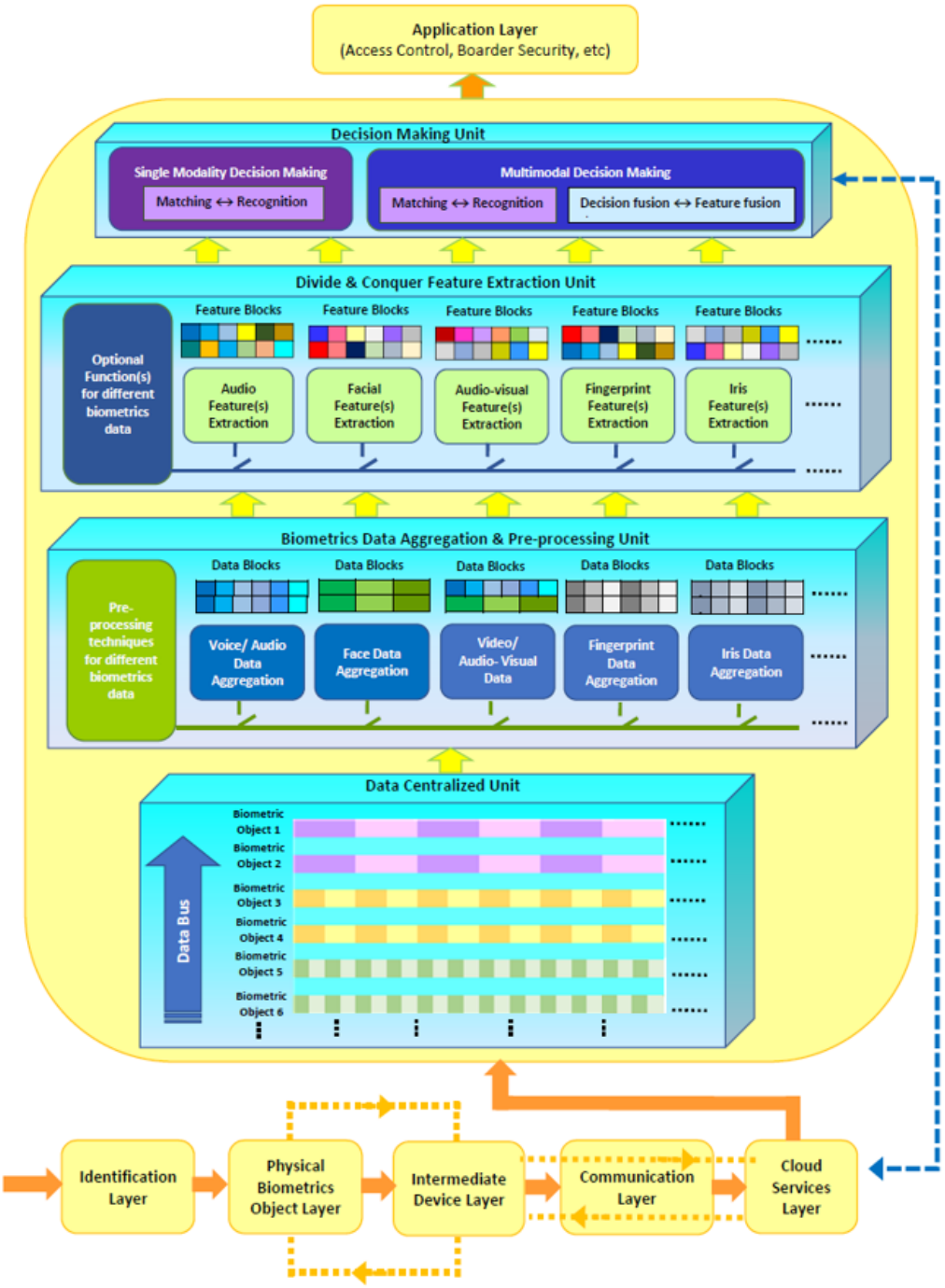

Figure 2. The proposed architecture of Big Biometrics Data Computation Layer.

2.7. Layer 7: Biometrics Application Layer

The Application Layer in the BiometricIoT has the responsibility to provide services and protocols for the various application requirements (e.g., smart homes, banking and finance, industry

and manufacturing, healthcare and medicine, etc.). The IEEE 802.15.4 specification proposes the constrained application protocol (CoAP) [40] for implementation in low power networks. Security issues at this layer should also be considered to be essential to the overall security for the BiometricIoT. The authors in [41] proposed an approach using DTLS (Datagram Transport Layer Security) and X.509 public key certificates for end to end secure communications where the IoT infrastructure does not have complete control over the communications network and channels. Besides CoAP, other application layer protocols which could utilized for the BiometricIoT include message queue telemetry transport (MQTT), representational state transfer (REST), advanced message queuing protocol (AMQP) and extensible messaging and presence protocol (XMPP) [42].

3. Design factors for biometrics IoT

Section 2 has discussed the comprehensive seven-layer framework for the BiometricIoT. This section gives discussions regarding the design factors for the biometrics IoT from four perspectives: 1) parallel Big data divide-conquer (D&C) computation; 2) computational complexity; 3) device security; and 4) algorithm efficacies. The design factors are important to develop the BiometricIoT considering the requirements for biometrics-based security, multimedia content and Big data applications.

3.1 Design factor 1: parallel Big data (D&C) computation

A first design factor for the BiometricIoT to be considered is the parallel Big data computation. This section will focus on the specific novelty for one layer and illustrate the parallel computation for the Bio_Data_FU using divide and conquer (D&C) techniques for the principal component analysis (PCA) [43] and linear discriminant analysis (LDA) [44] feature extraction approaches. A novel cascaded feature extraction technique called the Cascaded D&C PCA and LDA (Cas-D&C PCA-LDA) is proposed for Big Biometrics Data Computation Layer in the BiometricIoT. The traditional PCA and LDA algorithms incurs high computational costs due to the need to perform a SVD (singular value decomposition) on the full data matrix.

The authors in [45] proposed a split and combine technique to reduce the computational requirements for LDA to permit the deployment of parallel processing approaches using multicore architectures or graphical processing units (GPUs). In this section, we propose the full reconstructive-discriminative cascaded PCA-LDA problem on Big data for the BiometricIoT. The proposed approach uses variations of the PCA and LDA using the QR decomposition in place of the SVD. Further discussions on the PCA/QR can be found in [46]. The LDA/QR algorithm variation can be found in [47]. Equation (1) shows the LDA/QR objective function G, using the pseudoinverse operation of $(\cdot)^{(+)}$.

$$G = arg \max_{G \in \mathbf{R}^{g \times h}} trace\left((G^T S_t G)^{(+)}(G^T S_b G)\right) \tag{1}$$

Figure 3 shows the Cas-D&C PCA-LDA feature extraction architecture to be implemented in the Big Biometric Data Computation Layer and Table 1 shows a summary of the notations and terminology.

Figure 3 shows the block diagram of the Cas-D&C PCA feature extraction for the BiometricIoT. The actual algorithm of the Cas-D&C PCA feature extraction is given in Figure 4. A summary and discussion of the algorithm is given next. The algorithm inputs are the dataset, A which is stored in an $m \times n$ matrix and the class data, C which is stored in a $1 \times n$ vector. The algorithm outputs are three

matrices, A_1, A_2, A_{Test}, and three row vectors C_1, C_2, and C_{Test} where A_1 and A_2 are matrices of size $m \times n/4$, and A_{Test} is a matrix of size $m \times n/2$. This is shown as *Step 1*. In *Step 2*, the centered data matrices X_1 and X_2 are formed by subtracting the sample means from the respective datasets. *Step 3* performs the two Divide PCA in parallel. *Step 4* performs the Conquer PCA and calculates the PCA matrix ϕ. This is followed by the D&C LDA. Further theoretical discussions for the Cas-D&C LDA module can be found in [45].

Table 1. Summary of notations and terminology.

Notation	Description
$A = [a_1, a_2, \ldots, a_n]$	$\in \mathbb{R}^{m \times n}$ is a set of n biometric data samples in a m-dimensional feature space
k	number of classes
C	Class vector with biometric class labels $\Omega = [\omega_1, \omega_2, \ldots, \omega_n]$, where $\omega \in [1, 2, \ldots, k]$

Table 2. Computational costs for various divide and conquer (Cas-D&C) PCA-LDA/QR configurations.

Cas-D&C PCA/QR				
Configuration	QR matrix operations			SVD
	$(m \times n/2)$	$(m \times n/4)$	$(m \times n/8)$	$(n \times n)$
1	3	–	–	1
2	–	9	–	1
3	–	–	27	1
Cas-D&C LDA/QR				
Configuration	QR matrix operations			SVD
	$(g \times n/2)$	$(g \times n/4)$	$(g \times n/8)$	
1	3	–	–	–
2	–	9	–	–
3	–	–	27	–

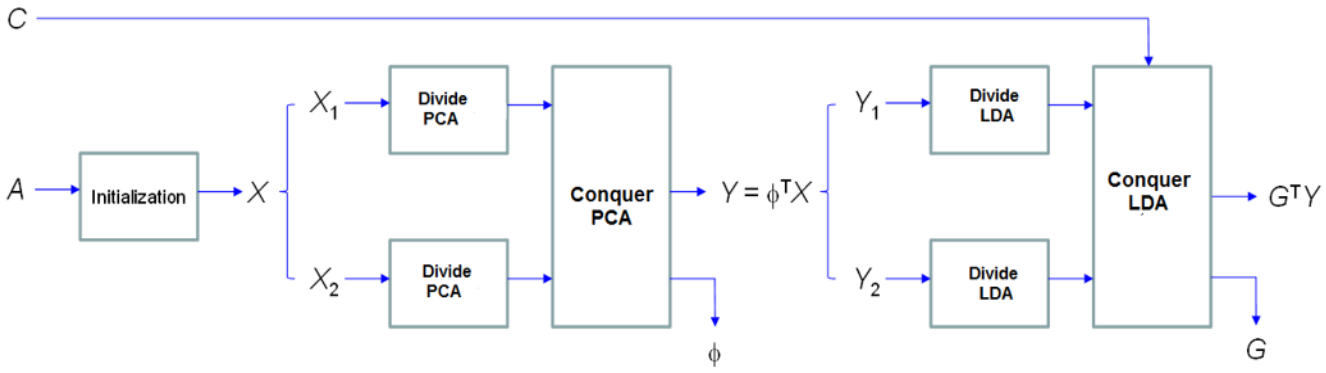

Figure 3. Block diagram of Cas-D&C PCA-LDA feature extraction architecture.

Step 1. Dividing into data sub-matrices A_1, A_2, A_{Test} and class row vectors C_1, C_2, C_{Test}.

Input: A (m×n matrix), C (1×n vector).

For i = 1 to 2 do

For j = 1 to n/4 do

1.1 Randomly select a column x from A (without replacement) and mark the selected column.

1.2 Select the corresponding column entry y from C.

1.3 Set x as the j-th column in the sub-matrix A_i.

1.4 Set c as the j-th entry in the row vector C_i.

End For

End For

1.5 Set A_{Test} to the remaining unmarked columns in C.

Output: A_1 and A_2 (m×n/4), A_{Test} (m×n/2), C_1 and C_2 (1×n/4), C_{Test} (1×n/2)

Step 2. Subtract the respective sample means from the datasets to form the centered data matrices X_1 and X_2.

Input: A_1 and A_2 (m×n/4 matrix).

2.1 Compute the centered data matrix, $X_1 = \frac{1}{\sqrt{n}}(A_1 - \mu)$.

2.2 Compute the centered data matrix, $X_2 = \frac{1}{\sqrt{n}}(A_2 - \mu)$.

Output: X_1 and X_2 (m×n/4 matrix).

Step 3. Do Divide PCA and solve sub-problems in parallel.

Input: X_1 and X_2 (m×n/4 matrix).

Do in Parallel

3.1 Compute the economic QR factorization of X_i as $X_i = Q_iR_i$ where Q_i is an orthogonal matrix of size (m×n/4) and R_i is an upper triangular matrix of size (n/4×n/4).

End Do

Output: Q_1 and Q_2 (m×n/4), R_1 and R_2 (n/4×n/4).

Step 4. Do Conquer PCA and calculate PCA matrix ϕ.

Input: Q_1 and Q_2 (m×n/4), R_1 and R_2 (n/4×n/4).

4.1 Compute Z as the matrix expression of $(X_2 - Q_1Q_1^{\mathrm{T}}(X_2))$.

4.2 Compute the economic QR factorization of Z as $Z = Q_zR_z$, where Q_z is an orthogonal matrix of size (m×n/4) and R_z is an upper triangular matrix of size (n/4 × n/4).

4.3 Construct the matrix R_{PCA} from the sub-matrices as $R_{PCA} = \begin{bmatrix} R_1 & Q_1^{\mathrm{T}}X_2 \\ 0 & R_Z \end{bmatrix}$.

4.4 Compute the svd of R_{PCA}^{T} as $R_{PCA}^{\mathrm{T}} = U\Sigma V^{\mathrm{T}}$ and retain the g largest principal components to form matrix V_g.

4.5 Compute the PCA transform ϕ as $\phi = Q_1V_g$.

4.6 Compute the dimensionality reduced dataset as $Y = \phi^{\mathrm{T}}X$.

Output: ϕ (m×g), Y (g×n/2).

Figure 4. Algorithm of Cas-D&C PCA feature extraction for BiometricIoT.

3.2 Design factor 2: computational complexity

A second design factor for the BiometricIoT to be considered is the computational complexity requirements. The computational complexity for a SVD decomposition is 14 mn^2 flops [46] whereas the computational complexity for a QR decomposition is 4 mn^2–(4/3)n^3 flops [48]. Table 2 shows a summary of the computational complexity for different Cas-D&C PCA-LDA architecture configurations. The architecture is scalable and each QR decomposition can be further split into three smaller QR decompositions to suit the computational requirements for the architecture. This becomes illustrative of the processing operations in the Big biometric data computation layer for the BiometricIoT. With a large number of computational processing units available (e.g., in a multicore or GPU architecture), the data blocks can be split until the block size reaches a threshold. In this way, a scalable architecture can be used to distribute the blocks to multiple parallel computational processing units for recombination at a later stage.

3.3 Design factor 3: device security

A third design factor for the BiometricIoT to be considered is the device security. This is particularly the case for IoT devices and applications which require significant levels of security such as biometrics identification for medical, financial and military systems. This section provides a discussion for the device security for the biometrics IoT. Device security (e.g., encryption) is required for securing the network transmission from the biometric devices/objects to the gateway. Encryption approaches that can be used includes identity-based [49,50] and pairing-based [51] methods. An advantage of identity or pairing-based approaches compared with other public-key cryptography approaches is that user-defined bit strings (e.g., derived from IP addresses, email addresses, or biometric traits) could be used as the public key. A disadvantage is that key revocation would also revoke the user identity. This is an especially important for the BiometricIoT using the biometric traits (e.g., facial identity) as the public key as the user biometric traits are permanent. A solution to this is to concatenate the identity component with a timestamp [52]. A biometrics identity breach would be limited to when the timestamp expired. Another approach proposed by [53] used a technique where nodes monitor its neighbor nodes for suspicious behavior (e.g., nodes sending invalid messages, extremely high traffic) and accumulates the information in an accusation matrix (AM). The public key is then revoked when the sum of all accusations exceeds a threshold. The authors in [54] identified a further security issue when compromised nodes attempt to transmit forged packets in the network.

3.4 Design factor 4: algorithm efficacies

A fourth design factor for the BiometricIoT to be considered is the efficacy of the algorithms. This is particularly the case for algorithms which have been initially designed for sequential implementations on traditional computer systems, and which now have to be efficiently executed on the IoT platforms. This section provides a discussion for the algorithm efficacy for the biometrics IoT. The face feature extraction and recognition procedure using the proposed Cas-D&C PCA-LDA approach is investigated and compared with traditional sequential implementations. Figures 5 and 6 show the comparison on the ORL and Yale datasets. The first two columns on the left show the algorithm performance using the traditional PCA and PCA + LDA (Fisherface [55]) approaches. The

remaining columns to the right show the algorithm performance using the Cas-D&C PCA-LDA configurations (PCA-LDA/QR). The classification was performed using the nearest neighbor classifier. As shown in Figures 5 and 6, the Cas-D&C PCA-LDA gave higher performance than the traditional and well-established Fisherface approach. This demonstrates that a parallel approach could give high algorithm efficacies without needing to compromise on performance. Figures 5 and 6 also show that the various splitting configurations gave similar algorithm efficacy. Thus, the divide-and-conquer processing can be tailored to suit the number of computational elements in the architecture.

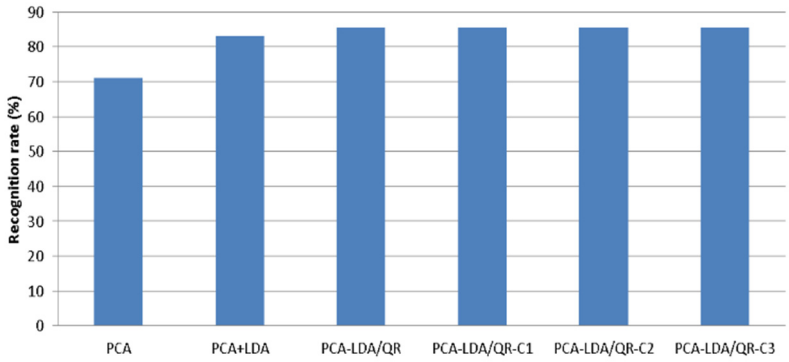

Figure 5. Performance on ORL dataset for different algorithms/configurations.

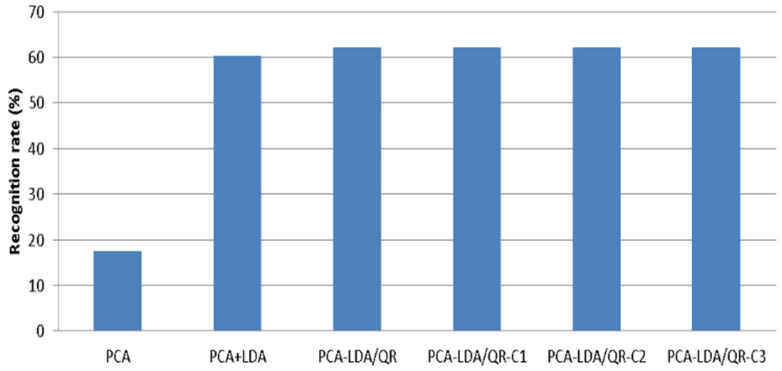

Figure 6. Performance on Yale dataset for different algorithms/configurations.

4. Conclusions

This paper has presented a seven-layer biometrics-based IoT (BiometricIoT) architecture with Big data computation and discussed various design factors for the IoT architecture. The BiometricIoT serves as an example of an ASIoT and requires additional challenges to be addressed compared with conventional IoT systems. Security issues for the different layers have also been discussed for the different layers. Some layers which are specific for the biometrics-based IoT including Big biometrics computation layer for biometrics data analytics has been introduced. In response to some of the security and processing issues raised in the architecture description, the authors have presented experimental data in support of a proposed novel cascaded feature extraction technique called Cas-D&C PCA-LDA

for Big biometrics data analytics. The approach utilizes divide-and-conquer (D&C) techniques for real-world Big data applications and have been validated with experiments on real-world datasets. The work in this paper has given a comprehensive framework for the design of ASIoTs using biometrics as the application, and has the objective to encourage researchers/practitioners towards the research and development of ASIoTs. It is expected that the integration of biometric technology to IoT connected devices to be happen over the next few years. This area will continue to grow as businesses look to tackle the potential threats caused by unsecured IoT devices on their network. For future research, some aspects such as security and threats, multimedia content and Big data can be further researched and strengthen making the proposed framework more reliable, secure and can meet the need of Big data applications. For example, security may be considered as a transverse layer which crosses the other seven system layers.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. Planet Biometrics, Gartner: Internet of Things will redefine identity management. Available from: http://www.planetbiometrics.com/article-details/i/2534/.
2. Business insider, Facebook Making Big Push Into Smart Home, IoT Device Market. Available from: https://mobileidworld.com/facebook-smart-home-iot-device-market-008252/.
3. Find biometrics, Arrow Electronics Signs On for IoT-Focused Distribution Agreement with NEXT. Available from: https://findbiometrics.com/arrow-electronic-next-408221.
4. Find biometrics, Baidu's Apollo Smart Car Program Depends on Face Biometrics. Available from: https://findbiometrics.com/baidus-apollo-smart-car-program-depends-face-biometrics/.
5. O. G. Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J. T. Arce, A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO, in *International Symposium on Algorithms and Experiments for Wireless Sensor Networks*, (2015), 112–128.
6. T. Guneysu, T. Oder, Towards lightweight identity-based encryption for the post-quantum-secure Internet of Things, in *2017 18th International Symposium on Quality Electronic Design (ISQED),* (2017), 319–324.
7. S. Dargan, M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, *Exp. Syst. Appl.*, **143** (2020), 113114.
8. N. Yusuf, K. A. Marafa, K. L. Shehu, H. Mamman, M. Maidawa, A survey of biometric approaches of authentication, *Int. J. Adv. Comput. Res.*, **10** (2020), 96–104.
9. J. K. P. Seng, K. L. M. Ang, Multimodal emotion and sentiment modeling from unstructured Big data: Challenges, architecture, & techniques, *IEEE Access*, **7** (2019), 90982–90998.
10. S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, W. Mahmood, Internet of multimedia things: Vision and challenges, *Ad Hoc Networks*, **33** (2015), 87–111.
11. K. P. Seng, L. M. Ang, A big data layered architecture and functional units for the multimedia Internet of Things, *IEEE Trans. Multi-Scale Comput. Syst.*, **4** (2018), 500–512.

12. A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, S. W. Kim, Multimedia Internet of Things: A comprehensive survey, *IEEE Access*, **8** (2020), 8202–8250.
13. L. M. Ang, K. P. Seng, L. W. Chew, L. S. Yeong, W. C. Chia, *Wireless multimedia sensor networks on reconfigurable hardware*, Springer, Heidelberg, 2013.
14. J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, B. Fang, A survey on access control in the age of Internet of Things, *IEEE Int. Things J.*, **7** (2020), 4682V4696.
15. G. K. Ijemaru, K. L. M. Ang, J. K. P. Seng, Mobile collectors for opportunistic Internet of Things in smart city environment with wireless power transfer, *Electronics*, **10** (2021), 697.
16. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E. K. Markakis, A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues, *IEEE Commun. Surv. Tutorials*, **22** (2020), 1191–1221.
17. D. Miorandi, S. Sicari, F. de Pellegrini, I. Chlamtac, Internet of Things: vision, applications and research challenges, *Ad Hoc Networks,* **10** (2012), 1497–1516.
18. M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, A. Alamri, Toward end-to-end biometrics-based security for IoT infrastructure, *IEEE Wireless Commun.,* **23** (2016), 44–51.
19. O. Said, M. Masud, Towards Internet of Things: survey and future vision, *Int. J. Comput. Networks,* **5** (2013), 1–17.
20. K. L. M. Ang, J. K. P. Seng, Application specific Internet of Things (ASIoTs): Taxonomy, applications, use case and future directions, *IEEE Access*, **7** (2019), 56577–56590.
21. A. Mosenia, N. K. Jha, A comprehensive study of security of Internet-of-Things, *IEEE Trans. Emerging Top. Comput.*, **5** (2017), 586–602.
22. L. Atzori, A. Iera, G. Morabito, The Internet-of-Things: a survey, *Comput. Networks,* **54** (2010), 2787–2805.
23. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, *Future Gener. Comput. Syst.*, **29** (2013), 1645–1660.
24. A. Zankl, H. Seuschek, G. Irazoqui, B. Gulmezoglu, Side-channel attacks in the Internet of Things: threats and challenges, in *Research Anthology on Artificial Intelligence Applications in Security,* (2021), 325–357.
25. L. A. Tawalbeh, T. F. Somani, More secure Internet of Things using robust encryption algorithms against side channel attacks, in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, IEEE, (2016), 978–983.
26. A. Mukherjee, Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints, *Proc. IEEE*, **103** (2015), 1747–1761.
27. N. Namvar, W. Saad, N. Bahadori, B. Kelley, Jamming in the Internet of Things: a game-theoretic perspective, in *2016 IEEE Global Communications Conference (GLOBECOM)*, (2016), 1–6.
28. W. Xu, K. Ma, W. Trappe, Y. Zhang, Jamming sensor networks: attack and defense strategies, *IEEE Network*, **20** (2006), 41–47.
29. I. E. Bagci, U. Roedig, I. Martinovic, M. Schulz, M. Hollick, IoT: using channel state information for tamper detection in the Internet of Things, in *Proceedings of Annual Computer Security Applications Conference,* (2015), 131–140.
30. C. Hota, R. K. Shrivastava, S. shipra, Tamper-resistant code using optimal ROP gadgets for IoT devices, in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, IEEE, (2017), 570–575.

31. IEEE Computer Society LAN MAN Standards Committee, Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs), *ANSI/IEEE Std.*, **802** (1999).
32. J. Granjal, E. Monteiro, J. S. Silva, Security for the Internet of Things: a survey of existing protocols and open research issues, *IEEE Commun. Surv. Tutorials,* **17** (2015), 1294–1312.
33. Y. Xiao, H. Chen, B. Sun, R. Wang, S. Sethi, MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks, *EURASIP J. Wireless Commun. Networking*, **2006** (2006), 1–12.
34. S. Radosavac, A. A. Cardenas, J. S. Baras, G. V. Moustakides, Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: robust strategies against individual and colluding attackers, *J. Comput. Secur.*, **15** (2007), 103–128.
35. S. Saleem, S. Ullah, K. S. Kwak, A study of IEEE 802.15.4 security framework for wireless body area networks, *Sensors*, **11** (2011), 1383–1395.
36. A. Le., J. Loo, A. Lasebae, A. Vinel, Y. Chen, M. Chai, The impact of rank attack on network topology of routing protocol for low-power and lossy networks, *IEEE Sensors J.,* **13** (2013), 3685–3692.
37. P. Sethi, S. R. Sarangi, Internet of Things: architectures, protocols, and applications, *J. Electr. Comput. Eng.*, **2017** (2017), 9324035.
38. C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, *Ad Hoc Networks,* **1** (2003), 293–315.
39. J. Zhou, Z. Cao, X. Dong, A. V. Vasilakos, Security and privacy for cloud-based IoT: challenges, countermeasures, and future directions, *IEEE Comms. Mag.,* **55** (2017), 26–33.
40. C. Bormann, Z. Shelby, K. Hartke, B. Frank, Constrained application protocol (CoAP), *Int. Eng. Task Force*, 2014.
41. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, DTLS based security and two-way authentication for the Internet of Things, *Ad Hoc Networks,* **11** (2013), 2710–2723.
42. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: a survey on enabling technologies, protocols, and applications, *IEEE Commun. Surv. Tutorials*, **17** (2015), 2347–2376.
43. I. Jolliffe, Principal component analysis, *Princ. Compon. Anal.*, (2002), 167–198.
44. A. J. Izenman, Linear discriminant analysis, in *Modern Multivariate Statistical Techniques*. Springer, (2013), 237–280.
45. J. K.P. Seng, K. L. M. Ang, Big feature data analytics: split and combine linear discriminant analysis (SC-LDA) for integration towards decision making analytics, *IEEE Access*, **5** (2017), 14056–14065.
46. A. Sharma, K. K. Paliwal, S. Imoto, S. Miyano, Principal component analysis using QR decomposition, *Int. J. Mach. Learn. Cybern.*, **4** (2013), 679–683.
47. D. Chu, L. Z. Liao, M. K. P. Ng, X. Wang, Incremental linear discriminant analysis: A fast algorithm and comparisons, *IEEE Trans. Neural Network Learn. Syst.*, **26** (2015), 2716–2735.
48. G. W. Stewart, Matrix Algorithms: Volume 1: Basic Decompositions, in *Society for Industrial and Applied mathematics*, 1998.
49. B. S. Adiga, M. A. Fajan, R. Shastry, V. L. Shivraj, P. Balamuralidhar, Lightweight IBE scheme for wireless sensor nodes, in *2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS),* IEEE, (2013), 1–6.

50. S. Sankaran, Lightweight security framework for IoTs using identity-based cryptography, in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* IEEE, (2016), 880–886.
51. X. Xiong, D. S. Wong, X. Deng, Tinypairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks, in *2010 IEEE Wireless Communication and Networking Conference,* IEEE, (2010), 1–6.
52. D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in *Annual International Cryptology Conference,* (2001), 213–229.
53. K. Hoeper, G. Gong, Key revocation for identity-based schemes in mobile ad hoc networks, in *International Conference on Ad-Hoc Networks and Wireless,* (2006), 224–237.
54. R. J. Hwang, Y. Z. Huang, Secure data collection schemes for wireless sensor networks, in *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, IEEE, (2017), 553–558.
55. P. N. Belhumeour, J. P. Hespanha, D. J. Kriegman, Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection, in *European Conference on Computer Vision*, (1996), 43–58.

AIMS Press