Biometric Cryptosystem to Secure Smart Object Communications in the Internet of Things

Abdallah Meraoumia, Mohammed Amroune*, Lakhdar Laimeche, Hakim Bendjenna

Laboratory of Mathematics, Informatics and Systems (LAMIS)
University of Larbi Tebessi, Tebessa, ALGERIA
**Corresponding author: mohmed.amroune@univ-tebessa.dz*

Abstract

Smart cities are viewed as one of the strengths of developed countries. Despite its novelty, It has attracted a lot of attention, prompting major tech companies to invest in various aspects related to their design. In fact, the Internet of Things is the most important pillar of these cities, as it allows almost everything, including machines, animals, and people, to be connected to the Internet and interact with one another. Like any electronic application, the security aspect is one of the most difficult challenges in the creation and design of such networks. As a result, in this paper, we proposed a secure IoT framework based on cloud computing. In this study, we focused on the security aspect of connecting people to their objects using biometric cryptosystems. Our proposed cryptosystem uses the concepts of a chaotic system combined with hand-palm biometrics, and uses the oriented Basic Image Features (oBIF) as a feature extraction method. The user message is then encrypted using the AES algorithm, while the user template is encrypted by a proposed algorithm.

Keywords: Internet security; Cryptosystem; Cryptography; Biometrics; chaotic maps; Palmprint; Palmvein; Data fusion

1. Introduction

Humans instinctively strive to create an environment that improves their sense of happiness and health using whatever means are available. There have been many little successes in this search over the years until the sudden emergence of digital technologies accelerating this pace of success. This amazing human evolution provides comfort and luxury by creating machines that reward humans for everything they need luxury (Pelton *et al.* 2019). However, humans are still looking to improve the services of these machines by implementing smart cities that can manage themselves and meet endless human demands. Indeed, smart cities are innovative cities that use ICTs to improve life quality, the efficiency of urban processes and services, and competitiveness (Rahul *et al.* 2016). In these cities, you can work and run your business anywhere with technologies that helps improve resource efficiency, improve living standards, provide timely and quality services, provide a safe and less polluted environment. All of this indicates that you live in a city that has the main appearance of smart cities.

Data is the most important element in transforming a city into a smart city (Mochizuki *et al.* 2018). Today, cities are full of objects that receive, collect, and transmit data, even simple things like smartphones, smart traffic lights, air pollutants, and even garbage. It collects all the data from relevant digital sensors to create new products that improve the city's infrastructure, equipment, services, and more. from the city. All of these sensors are connected to form what is called the Internet of Things (IoT) (Yasunori *et al.* 2017) which is used to provide the ability to connect to the Internet for devices and different objects, in addition to the ability to communicate with each other through network and cloud services (Qasem *et al.* 2019) to exchange information so that each party can perform its mission. Devices and objects include everything you can think of, from televisions, refrigerators, and surveillance cameras to our body's organs (Alsbou *et al.* 2019). Thus, the important part of this architecture is not the machine or the object but rather the sensors that collect the data of the environment of the machine or the object.

One of the biggest challenges of IoT is security and privacy (Shah *et al.* 2017). Unfortunately, in this structure, devices and objects, that use sensors, collect very sensitive data about us in this structure. He hears what we say and knows what we do at home. In addition, most devices and objects can be private and are likely to be attacked because they are connected to the internet (Yahyaoui *et al.* 2020). Therefore, maintaining the confidentiality of this data and monitoring illegal access to objects is essential to gain the trust of consumers. Therefore, as a humble suggestion, this paper proposes a new tool that enables users to create secure communications over unsecured channels with their things. The proposed cryptosystem allows users to exchange their messages and biometric templates via the Internet with high security. Since the feature extraction method should be light, it is advisable to use an efficient handcrafted method to extract a distinct feature vector capable of differentiating between different users. Fortunately, the oriented Basic Image Features (oBIF) can do this for two reasons. Firstly, its promising results which have been shown in pattern analysis, and secondly, its excellent ability to extract line traits which are the main features of the biometric modalities used. In order to harden the proposed system against attacks on the biometric template and as well as on user messages, we have adopted a cryptographic approach to reduce the number of security breaches because failure to do so will result to insufficient security, making the system vulnerable to attack. To solve security problems, the power of chaotic systems has been used as one of the most effective methods due to its simplicity, speed, and high security. Experimental results show that the proposed system provides a very high level of security to protect the biometric templates and user messages making the user objects safe from attacks, naturally increasing confidence in being involved in such networks.

The rest of the paper is organized as follows: Section 2 provides an overview of IoT, where we focused on their security framework. The concept of biometric cryptosystem and some preliminary work have been covered in Section 3. Section 4 highlights the general scheme of cloud-based IoT and how to secure communication between a person and their things. In this section, the proposed biometric cryptosystem is presented. Section 5 aims to describe the proposed methodology. In section 6, the experimental results, before and after the fusion, are given and commented. This section evaluates the system performance and analyzes cryptographic security. Section 7 presents a comparative study. Finally, conclusion and further work are presented in section 8.

2. Internet of things

Internet of Things (IoT), as an extension of of the classical Internet network, is the network of physical objects or things rooted with sensor software and network connectivity (Ishaq *et al.* 2013). The IoT is seen as a technological and monetary wave in the post-Internet global information industry. It is an intellectual network, which combines everything with the Internet to enable seamless communication and information exchange through sensing devices according to an agreed protocols.

Day by day, the number of devices connected to the Internet is increasing. Basically, devices connected to the Internet are personal computers and smartphones which generally require human intervention. Nowadays, almost all electronic objects can be connected to the Internet. As an example (Joshy *et al.* 2017), modern technology has succeeded in connecting different household appliances like refrigerators, washing machines, air conditioners, doors, and windows, as well as all goods and products on the shelves of shops. They are also extended to animals in farms and seas, to trees in forests, etc. Therefore, this technology can be used in several fields such as medicine, economics, social fields, education, public safety, and sport.

2.1 IoT Revolution

The Internet revolution has produced spectacular results. In 1990, one billion electronic devices were connected to the Internet, the majority of these devices being personal computers. In 2000, that number exceeded over six billion, due to the remarkable development of the mobile device and smart device industry (Krotov *et al.* 2017). Nowadays, there are more mobile devices than people, and according to the World Economic Forum, there will be 2.5 billion users connected to social networks by the end of 2020. In addition, these users can access 50 billion connected things. So this hyperconnectivity or IoT can inject nearly $ 65 trillion into world trade. According to several indicators, such as IoT adoption rates, economic trends, and demographics, the annual economic impact of IoT could be between $ 3.9 trillion and $ 11.1 trillion in 2025. Probably, in the next years, factories will have the biggest impact on IoT with up to $ 3.7 trillion per year. The expected economic impact of IoT technology can come from humans, homes, offices, and vehicles of all kinds, cities, shops and factories (Lee *et al.* 2015).

2.2 Security Requirements

The benefits of IoT are undeniable, but the reality is that security does not keep pace with in- novation. In addition, IoT faces many challenges, such as heterogeneity of things, protocol inter-operability, and network scalability. As the IoT is an extended notion of the Internet network, it is vulnerable to various attacks such as Man-In-The-Middle (MITM), Sniffing/Spoofing, Denial-of-Service (DoS), Distributed DoS (DDoS), brute force, etc. Therefore, the security requirements should include (Atwady *et al.* 2017), (Azarmehr *et al.* 2017):

- **Authentication:** Identity verification of an entity, whether it is a person or a thing.
- **Identification:** Identify the entity, this provides an answer to the question: "who/what is the entity?"
- **Privacy (Confidentiality):** Ensure that information is only accessible to those who have been authorized, which requires that data and information be encrypted.
- **Integrity:** There should be no be any alterations or destruction of information.
- **Availability:** Information must be available upon request.
- **Freshness:** The information is constantly and indefinitely updated.
- **Forward/backward secrecy:** The changing of network entity's number has no effect on the communication.

Authentication in IoT is about things, smart devices, and people. There are two types of human authentication: non-biometric and bio- metric. As a subclass in the first, we find: *i)* what we know? Such as password, code number, etc. *ii)* what do we have? Such as token, e-card, etc. (Mohan 2017), (Abdur *et al.* 2017). For the biometric class, we find two subclasses: *i)* what we are? It means morphological or physiological features such as fingerprint, palmprint, finger-knuckle-print, face, ear, iris, retina, electrocardiography (ECG), etc. *ii)* how we do? This means behavioral characteristics such as voice, gait, dynamic or static signature, handwriting, dynamic keystroke (Mohan 2017).

In addition to authenticating and identifying a user, biometrics can be used to ensure the confidentiality of securely sharing the secret key. These schemes are In addition to authenticating and identifying a user, biometrics can be used to ensure the confidentiality of sharing the secret key securely. These schemes are called a biometric cryptosystem. the cryptographic key (symmetric cryptographic with a random key) and the biometric feature (template) are confused in these systems. This is known as the key-binding principle (Abdur *et al.* 2017).

2.3 IoT Security Framework

The IoT now plays an important role in all aspects of our daily lives. The widespread adoption of IoT applications is based on a critical factor: security, which refers to the protection of devices and networks linked in the IoT (Ling *et al.* 2017). As a result, the field of IoT security is an important area of research that generates many challenges that necessitate a great deal of attention and investigation on the part of researchers. However, because the security aspect of IoT is still relatively, it frequently fails to respect the security principle in the design of IoT-oriented products. In this subsection, we present a brief description of the well-known IoT security frameworks (Mahmoud *et al.* 2018).

1) Amazon Web Services IoT: Amazon Web Services (AWS) (Amazon iot) is an IoT cloud platform provided by Amazon. It aims to make smart devices more accessible while also ensuring secure interaction with the AWS Cloud and other connected devices. This framework is easy to use and utilizes various AWS services such as Amazon Machine Learning (Amazon ML), Amazon DynamoDB (Amazon dynamodb), Amazon S3, and others. Furthermore, AWS IoT enables applications to talk to devices even when they are offline. The architecture of this framework is based on four main components: Device Gateway, Rules Engine, Registry, and Device Shadows. The first, which employs the MQTT protocol, serves as an intermediary between connected devices and cloud services. Second, the rules engine helps to support the received posted messages by delivering them to other subscribed devices or AWS cloud services, as well as to non-AWS services through AWS Lambda for further processing or analysis. The third component, the registry, on the other hand, assigns a unique ID to each connected device, regardless of device type, vendor, or method of connection. It also stores metadata (such as device name, ID, attributes, etc.) for connected devices in order to provide traceability.

2) ARM mbedIoT: ARM mbedIoT uses ARM micro-controllers (ARM plt) to develop applications for IoT. It includes an operating system, cloud services, tools, and developer ecosystem to develop standalone or networked IoT applications (ARM mbed). ARM mbedIoT is a platform that aims to provide a scalable, connected, and secure environment for IoT devices by integrating mbed tools and services, ARM micro-controllers, mbed OS, mbed Device Connector, and Mbed Cloud. This framework stands out by offering a common operating system foundation for IoT development. It supports the most widely used communication protocols for device interconnection and Device/Cloud connection. It is worth noting that it supports automatic power management in order to provide solutions to the power consumption issue. The architecture of this framework is built around five components mbed OS, mbed client library, mbed cloud, mbed device connector, and hardware devices based on ARM microcontrollers.

3) Azure IoT Suite: This framework is proposed by Microsoft (Microsoft azure), it offers several services to end-users. In this context, Azure IoT Suite allows the user to communicate with their IoT devices, receive data from them, perform various operations on the data, and visualize them in a suitable way for business. The Azure IoT Suite sees the challenge of having a complete IoT framework as a combination of three different sub-issues: scaling, telemetry models, and big data. This framework is compatible with a wide range of hardware devices, operating systems, and programming languages. The main component of the Azure IoT architecture is the predefined cloud gateway that enables IoT devices to interact with the Azure cloud. Data sent by devices is stored in the cloud for further processing and analysis by Azure cloud services. Among these services are Azure Machine Learning and Azure Stream Analytics, to name a few. The data can also be immediately made available to specific services for real-time analysis. The output of both tracks is presented and visualized in a customized way that matches the customers? desires and their business. The second component is the Azure IoT Hub (Azure hub). It is a web service that provides two-way communication between devices and cloud backend services while also addressing all security concerns.

4) Brillo/Weave: Google's contribution to the security of the IoT domain is the Brillo/Weave platform for the rapid implementation of IoT applications. The platform contains two main components: Brillo and Weave (Google Weave). Brillo is an Android-based operating system designed for the development of embedded low power devices; however, the Weave is used to act as a communication shell for interactions and message-passing purposes. These components allow a device to be registered in the cloud and send/receive commands remotely. The two components interact together in a policy that is complementary to the IoT framework.

5) Calvin: Ericsson created this platform, which is an open-source IoT platform (Ericsson calvin) designed for the creation and management of a distributed application that provides inter-device communication. It is a framework that employs the Flow-based Computing (FBP) paradigm methodologies on the well-defined actor model. Calvin's architecture is made up of six layers structured like a stack (hardware, OS, platform-dependent runtime, platform-independent runtime, actor instance, and application). The Hardware is the bottom layer and the application is the top layer of Calvin architecture.

Finally, it is important to note that other platforms exist, such as: Home Kit developed by Apple (Apple smarter), Kura is an Eclipse IoT, and Smart Things project developed by Samsung (Smart doc).

3. Biometric cryptosystem

In recent years, emerging electronic applications (*e*-applications) have played a critical role in the rapid and continuous growth of development in a number of countries around the world (Fhatuwani *et al.* 2018). Several online applications can be integrated into this area, such as *e*-commerce, *e*-banking, *e*-voting, *e*-learning and *e*-government. Reliable *e*-applications must ensure the security of shared information, which is becoming increasingly common and poses new challenges for all applications. The information exchanged is generally sensitive and must be protected. Furthermore, the identity of the users who transmit this information must be accurately authenticated on the recipient's side. Indeed, using biometric cryptosystems is a simple way to meet these requirements (Kuo 2018).

3.1 Biometrics in cryptography

In general, identifying the user's identity in the majority of *e*-application schemes is a necessary step before providing the required services. For this purpose, the recipient uses two main procedures, on the one hand, to recover the cryptographic key from the encrypted template and, on the other hand, to accurately identify the user. To be successful at this stage, the template extracted from the biometric modality must accurately represent the user. This requirement is met adequately by employing an appropriate feature extraction method, which can be difficult at times (Jingjin *et al.* 2017).

A biometric cryptosystem combines biometrics and cryptography to generate cryptographic keys linked to biometric templates. Therefore, biometric cryptosystems provide solutions for the secure management of cryptographic keys as well as the protection of biometric templates. Based on how helper data is derived, biometric cryptosystems approaches can be divided into two categories: key-binding and key generation types (Jain *et al.* 2018). In the first category, a secure key can be bound to the biometric data to obtain a so-called secure sketch from which no information about the biometric data or the key can be re-covered. In key-binding schemes, two well-known examples of these systems are the fuzzy commitment (Sha *et al.* 2018) and the fuzzy vault (Sweedle *et al.* 2018). Based on a cryptographic key, the first scheme secures biometric templates as binary vectors, while the second secure them as an unordered set of points. In a key generation scheme, the helper data is derived only from the biometric template so that the cryptographic key is directly generated from the helper data and a given biometric template.

3.2 Relate work

In this context, there have been a number of research efforts aimed at addressing the issues related to biometric cryptosystems. *Soutar et al.* (Soutar *et al.* 1998) proposed one of the first biometric cryptosystems that used key binding. In this method, a key binding algorithm in an optical correlation-based fingerprint matching system has been proposed. This algorithm binds a cryptographic key with the user's fingerprint images at the time of enrollment. The key is then retrieved only upon successful authentication. The algorithm begins by generating a correlation filter function with amplitude and phase components. The design criteria for this function include both distortion tolerance as well as discriminability. The algorithm also calculates an output by convolution/correlation of the training fingerprint images with the correlation filter function. Then, the complex conjugate of the phase component of the correlation filter function is multiplied by a randomly generated only phase array of the same size.

Lifang Wu et al. (Lifang *et al.* 2010) developed a biometric cryptosystem based on face biometrics. During encryption, the 128 dimensional principal component analysis (PCA) feature vector is initially obtained from the facial image. Then, using thresholding, a 128 bit binary vector is obtained. The author then chose distinct bits to create a bio-key. In addition, an Error correcting code is produced using the Reed-Solomon algorithm.

Li et al. (Li *et al.* 2010) proposed a fuzzy vault scheme, that combines two local structures, the minutiae descriptor and minutia local structure. By using three fusion approaches, the two transformation-invariant local structures are integrated into the proposed scheme.

Hybrid approaches that use both key generation schemes and key binding concepts have also been proposed. In (Yi *et al.* 2010), the authors propose a hybrid approach that takes advantage of both the biometric cryptosystem and the transformation-based approach. A three-step hybrid algorithm is designed and developed based on random projection, discriminability-preserving (DP) transformation, and fuzzy commitment scheme. Cancellability is provided by random projection. The DP transform is developed to convert real-valued cancelable templates to binary templates while preserving discriminability, allowing it to be easily encrypted in the fuzzy commitment scheme. *Xi et al.* (Xi *et al.* 2011) proposed a fuzzy extractor using a local dual-layer structure. In this system, fuzzy extractors are based on error- correcting codes. A cryptographic key is encoded with an error-checking code, then the encoded bit sequence is integrated with the biometric template which are calculated using the data of the training sample. This process produces an open string. While the authenticated person presents the biometric data, the data is computed with the open string using *XORing* process. The process yields a key release with wrong bits corrected.

In (Liu *et al.* 2017), *Liu et al.* used l_1-minimization to protect fingerprint templates and store them as ciphertext. Fingerprint matching is performed in the encrypted domain and authentication is successful only when the query fingerprint is close enough to the fingerprint template. As the template is generated from the Minutia Cylinder-Code (MCC) (Cappeli *et al.* 2010) with the appropriate design of the secure algorithm, the proposed system achieves high security and recognition accuracy.

In order to provide a more accurate error correction decoding in an iris-based fuzzy commitment scheme, which approaches a theoretical limit obtained by *Bringer et al.* (Bringer *et al.* 2008), the authors apply a two-dimensional iterative min-um decoding. In their approach, a matrix is created where the rows, as well as the columns, are formed by two different Reed-Muller binary codes. *Sarkar et al.* (Sarkar *et al.* 2018) proposed the generation of cryptographic keys from fingerprint templates. Different keys with a length of 128 *bits* can be generated by canceling and re-issuing different fingerprint templates. This reduces the possibility that the same secret key that existed with both the recipient and the sender will be leaked after negotiation.

Alam et al. (Alam *et al.* 2018) put forward a biometric cryptosystem that incorporates the discrete Fourier transform (DFT) and random projection-based cancelable technique to enhance security. In the proposed system, polar grid-based fingerprint features are transformed by using DFT and random projection, creating a non-invertible template. Furthermore, to improve template security, a bit-toggling strategy is used to inject noise into the generated template.

4. Secure management of IoT objects

The main objective of this paper is to design and develop a secured IoT scheme. The proposed scheme allows the user to freely access his things using his biometric traits. For security reasons, this scheme must be designed to withstand well known attacks such as replay and forgery. In order to accomplish this, we have included a security procedure in our scheme that is based on the biometric identification and the message cryptography principle. The proposed IoT scheme based on biometrics technologies and cloud computing is shown in 1. Two bidirectional connectivity (two links) must be secured: user-server connectivity and server-object connectivity. As a result, the security process in each connectivity is described in detail in the following two subsections.

4.1 Cloud/Objects connectivity

In our scheme, users' data (template and queries) is secured in both links. First and foremost, the server must identify things for each user. The gateways track or localize things (especially moving ones) at any time and with the help of their IDs. Then, the information obtained is transmitted to the server which connects the user to his things and vice versa. Users can connect to their objects even when they are in motion by using this protocol. Let k_{t-1} and k_t be two encryption keys transmitted by the user at times t and $t-1$ (two successive connections). At time t, the server and the gateways know the key k_{t-1}. At this time, the server encrypts the users' queries with the k_t key. In addition, the key k_t is encrypted with k_{t-1}. Finally, these two encrypted messages are transmitted to gateways. On the side

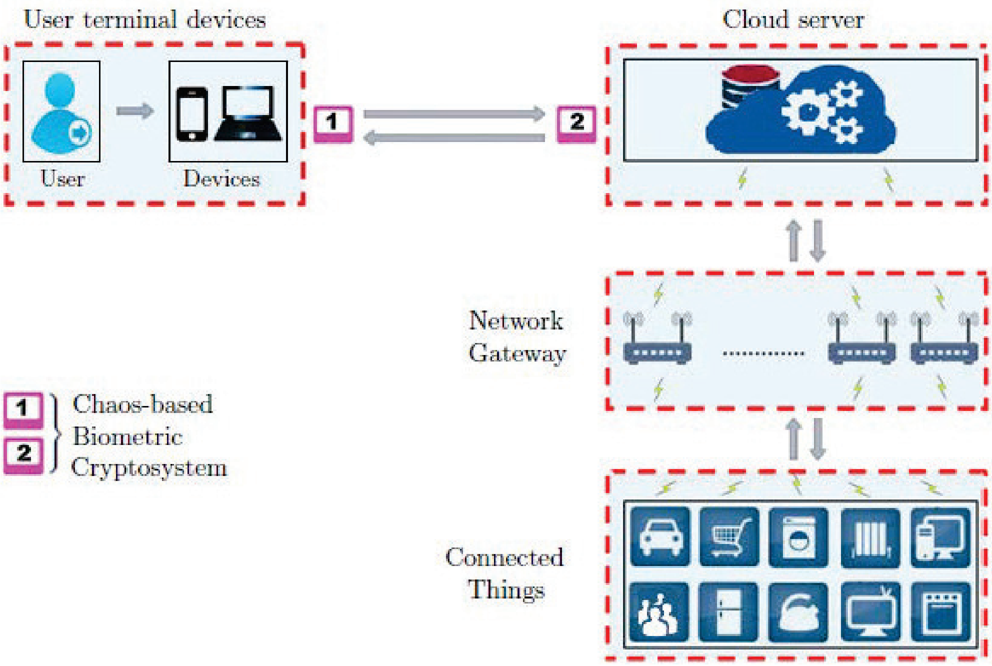


Fig. 1. Communication security of smart objects based on a biometric cryptosystem

of the gateway, the key k_t is extracted using the previously-stored k_{t-1}. Now gateways can decrypt and process user queries. In the case of gateway-server communication, the message is encrypted with the last key stored in the gateways.

4.2 User/cloud connectivity

This link is secured by a biometric cryptosystem. In the proposed cryptosystem (see Fig. 2), several chaotic systems (Logistic maps and Arnold's Cat map) are combined. Indeed, the first logistic system ($\mathcal{L}^0$), controlled by $\mathcal{N}_0$, is used to determine the location in which we insert two integer values $\mathcal{N}_k$ and $\mathcal{N}_s$ (16-bits each) into the binary templates (feature vectors) of the PLP and PLV modalities. These values are used as follows: $\mathcal{N}_k$ generates a cryptographic key used by the AES algorithm to encrypt the message data. While $\mathcal{N}_s$ is used to substitute $\mathcal{N}_0$ in which in two transmission attempts, the locations (x, y) of $\mathcal{N}_k$ and $\mathcal{N}_s$ in the biometric templates become different.

To generate the AES key (see Fig. 3), three logistic maps ($\mathcal{L}^m$, $\mathcal{L}^{m_1}$, $\mathcal{L}^{m_2}$), controlled by $\mathcal{N}_k$, are used. In addition, in order to encrypt the user's templates, two logistic maps ($\mathcal{L}^1$, $\mathcal{L}^2$), controlled by $\mathcal{N}_1$ and $\mathcal{N}_2$, and an Arnold's Cat map ($\mathcal{C}^1$) are used. The role of $\mathcal{L}^1$ is to change the control parameters (a, b) for the $\mathcal{C}^1$, while $\mathcal{L}^2$ is to generate an orthogonal pseudo-random matrix (using the Gram Schmidt algorithm) from which the template, at a predefined $\mathcal{C}^1$-iteration, is projected.

In the key generation procedure (see Fig. 3), the binary codeword ($\mathcal{N}_k$) is divided into two parts (k_1 and k_2). The first part (k_1) determines the initial state of $\mathcal{L}^m$ while the second part (k_2) makes it possible to set the length of the encryption key (variable key length). This variation increases the security level of our system. Also, k_1 is divided into two subparts (k_{11} and k_{12}) which are used, after transformation into integer values, to determine the initial states of $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$. Each of $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$ establishes a sequence of real values ($\in [0, 1]$). After the normalization process ($\in [0, 255]$), the two chaotic sequences are concatenated and transformed into a binary format to form an encryption key.

5. Proposed Methodology

Basically, the process of personal identification is critical to ensuring the security of physical/logical access (Pietro *et al.* 2016). Biometrics has recently emerged as one of the most powerful technologies for recognizing a person's identity (Bilgehan *et al.* 2016). Among many biometric traits, those

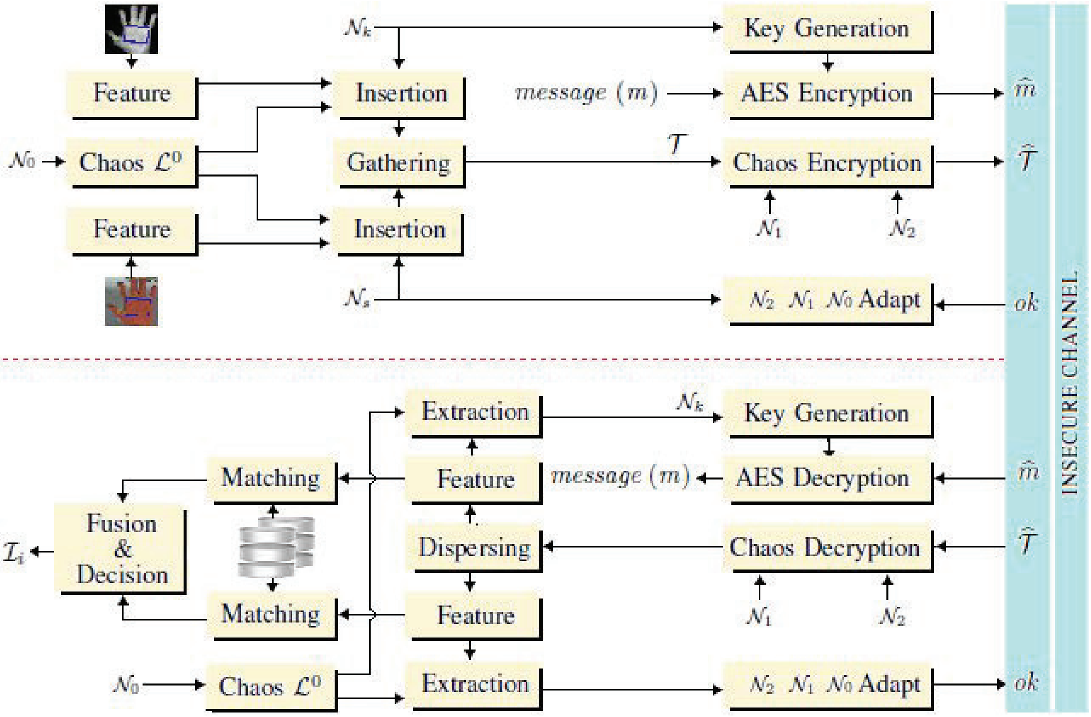


Fig. 2. Proposed remote identification system based on PLP and PLV biometric modalities.

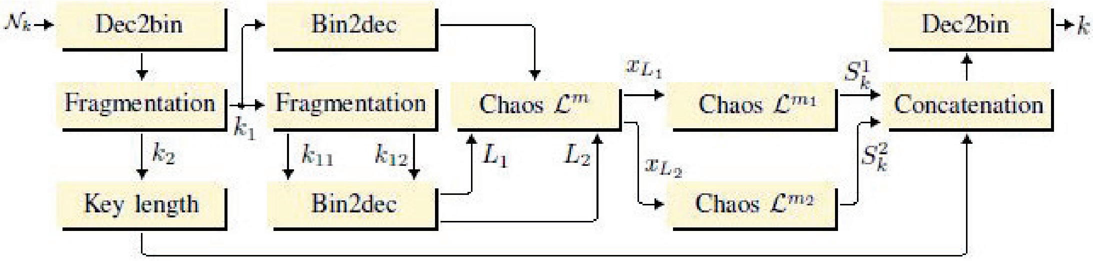


Fig. 3. Proposed AES key generation scheme.

extracted from the human hand have been systematically used to make the biometric system easier to use (Jyotismita *et al.* 2019). In fact, users still prefer manual access systems because hand information, except for fingerprints, is not considered private information such as iris or retina. It is therefore more practical to use them than other biometric modalities. In addition, the simplicity of acquisition, processing and the stability of their features make this technology very suitable for many uses. For these reason, our proposed cryptosystem scheme employs two commonly used hand biometrics: palmprint (PLP) (Nabil *et al.* 2017) and palm-vein (PLV) (Yiding *et al.* 2017).

5.1 Preliminary knowledge required

The objective of this study is to develop a reliable method of remotely identifying users in order to provide secure electronic applications. Our proposed biometric cryptosystem reduces the risk of attempted fraud significantly. In this system, we investigate chaotic sequences to establish its superiority for biometric cryptosystems. Furthermore, all issues related to the final design of the biometric systems are generally related to the feature vector extraction task. In this subsection, the feature vector extraction method, as well as the chaotic systems used in our design, are discussed.

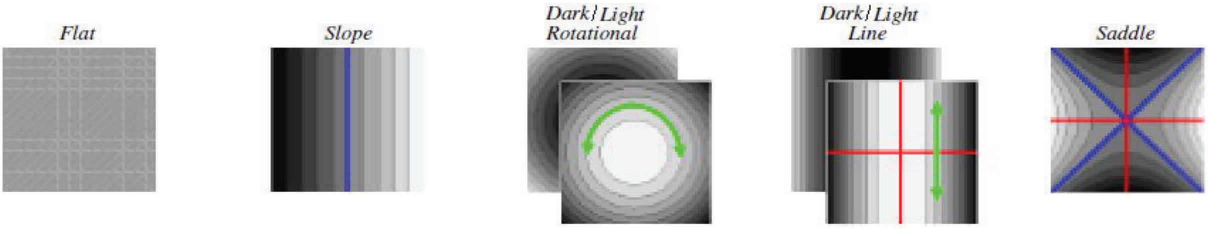


Fig. 4. Basic image features.

5.1.1 Chaotic Systems

As security and reliability have improved in recent years, chaotic systems have become more and more popular in digital communication technology (Adel *et al.* 2017). In fact, chaos is a dynamic system characterized by chaotic properties such as non-periodicity, sensitivity and pseudo-randomness. Compared to traditional methods, the chaotic encryption algorithm offers several advantages, such as simplicity of implementation, ample cryptographic key space, robustness and speed. Indeed, many chaotic systems based on various principles have been proposed. Among these, Arnold's Cat system ($\mathcal{C}$) and Logistic map system ($\mathcal{L}$) have been commonly used for several data encryption applications.

- *Arnold's Cat Map:* Arnold's cat map (Arnold *et al.* 1968) is a two dimensional discrete chaotic map allows to transform the original pixel positions of the an image. This transformation is invertible in which the original image can be reappeared after a sufficient number of iteration. Let I be an image of $N \times N$ pixels, their 2D cat map is determined by the following formula:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \mathcal{F}(\begin{bmatrix} x_n \\ y_n \end{bmatrix}) = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ N) \tag{1}$$

where $x_n, y_n \in [0, N-1]$ are the pixel coordinates, the two positive integers a, b represent two control parameters and $x_{n+1}, y_{n+1} \in [0, N-1]$ are the new pixel positions when the Arnold's cat map is done once. In this system, the number of iterations ($\mathcal{C}$ period denoted by τ_{cat}) depends on the control parameters a, b and the size of the original image ($N \times N$). Thus, in our biometric cryptosystem, we can use the control parameters a, b as a secret key.

- *Logistic map:* the logistic map (Robert M. 1976) is one-dimensional discrete chaotic system defined by the following recurrence relation:

$$x_{n+1} = \mathcal{F}(x_n) = \mu\, x_n(1 - x_n) \tag{2}$$

where x_n is the state of the chaotic system (for $n = 0, 1, 2, \cdots$) and μ is the control parameter. This map generates pseudo-random sequences by means of an initial state x_0 and a fixed control parameter μ. In this generator, the states obtained x_i are between 0 and 1. For a chaotic behavioral, x_0 and μ must belong respectively to the intervals $[0, 1]$ and $[3.57, 4]$. In our biometric cryptosystem, these two parameters (x_0 and μ) have been used as secret keys.

5.1.2 Feature Extraction

The efficient extraction of the salient features of an image is an essential task in any pattern recognition system. Therefore, the extracted features must adequately represent the overall information contained in the image, because good results are directly related to the uniqueness and variability of these features, which allow different patterns to be distinguished (Suresh *et al.* 2018). Using different feature extraction methods, various features in the image can be extracted and then used as a vector to distinguish the image models, which can be divided into three main categories: hand-crafted methods, learned hand-crafted methods, and deep learning methods. Unfortunately, the last two categories require devices that are powerful in terms of memory and speed. So, since this scheme is intended to work in weak devices (like Smartphones or smart tablets), hand-crafted methods become very appropriate.

In fact, hand-crafted methods require an expert to determine the appropriate method depending on the work context. In our biometric cryptosystem, we use PLP and PLV modalities which have their own oriented lines. Thus, to effectively represent this image, it is necessary to use an efficient method for optimal representation of these lines. Currently, oriented Basic Image Features (oBIF) (Ardelio *et al.* 2017) provide strong capabilities to obtain a lot of information about an image texture, including their lines. In this method, each location in the image is classified according to some local properties, such as symmetry type and orientation, using a bank of Gaussian Derivative (DtG) filters.

• *Gaussian Derivative Filters:* DtG filters have been shown to be effective in many computer vision applications as one of the most successful image analysis methods. This type of filter has been successful in areas such as optimal edge detection, localization of curved edges, measurement of local anisotropy and orientation in an image are some examples where this type of filters has been successful. The 1D Gaussian filter (Ardelio *et al.* 2017) is defined by:

$$G_\sigma(x) = \frac{1}{\sigma\sqrt{2\pi}}\, e^{\frac{-x^2}{2\sigma^2}} \tag{3}$$

where σ denotes the standard deviation (scale).

Because this function is exponential, repeated derivation (along x) yields a pattern that resembles an increasing order polynomial, multiplied by the original Gaussian function. For example, hereafter we show the first four derivatives of the order 0 (*i.e.* no differentiation) to 3 ($G_\sigma^{(n)}(x) = \frac{d^n}{dx^n} G_\sigma(x)|_{n=0}^3$):

$$\begin{cases} G_\sigma^{(0)}(x) = G_\sigma(x) \\ G_\sigma^{(1)}(x) = (\frac{-x}{\sigma^2}) \cdot G_\sigma(x) \\ G_\sigma^{(2)}(x) = (\frac{x^2-\sigma^2}{\sigma^4}) \cdot G_\sigma(x) \\ G_\sigma^{(3)}(x) = (\frac{x^3-3\sigma^2 x}{\sigma^6}) \cdot G_\sigma(x) \\ \vdots \quad \vdots \quad \vdots \qquad \vdots \\ G_\sigma^{(n)}(x) = P_n(x) \cdot G_\sigma(x) \end{cases} \tag{4}$$

From Equation 4, it is clear that the order of the polynomial ($P_n(x)$) has the same order as the derivative associated with it ($\frac{d^n}{dx^n}$). These polynomials are the Hermite polynomials, which come from the following definition:

$$\frac{d^n e^{-x^2}}{dx^n} = (-1)^n H_n(x) e^{-x^2} \tag{5}$$

where the function $H_n(x)$ denotes the n^{th} Hermite polynomial. The relationship between the function $G_\sigma(x)$ and its derivatives can be obtained by substituting $x \rightarrow \frac{x}{\sigma\sqrt{2}}$, which gives the following formula::

$$G_\sigma^{(n)}(x) = (-1)^n \frac{1}{(\sigma\sqrt{2})^n} H_n(\frac{x}{\sigma\sqrt{2}}) \cdot G_\sigma(x) \tag{6}$$

and, then

$$P_n(x) = (-1)^n \frac{1}{(\sigma\sqrt{2})^n} H_n(\frac{x}{\sigma\sqrt{2}}) \tag{7}$$

The Gaussian filter is a function that is released along the major axis, so multiplication results in a higher DtG. Thus, the 2D DtG filter can be constructed as the product of two 1D DtG filters:

$$G_\sigma^{(m,n)}(x, y) = G_\sigma^{(m)}(x) G_\sigma^{(n)}(y) \tag{8}$$

To summarize, we can say that DtG filters are produced from a polynomial function (Hermit polynomial) and a Gaussian kernel. Hermite polynomials are characterized by many interesting recursive relations which make these filters very suitable for analytical treatment.

• *Oriented Basic Image Features:* By utilizing the symmetry sensitivities of DtG filters in image, a set of local texture descriptors known as Basic Image Features (BIF) can be produced. To that end, the following inner products must be computed, which measure the filter responses to a DtG filter of order (m, n), must be calculated:

$$c_{mn} = \langle G_{\sigma}^{(m,n)} | \mathcal{I} \rangle \tag{9}$$

where $G_{\sigma}^{(m,n)}$ is the set of DtG filters and $\mathcal{I}$ the analyzed image. Typically, a family of DtG filters with a certain order is used (*e.g.* 2^{nd} order family: $0 \leq m+n \leq 2$). Thus, using scale-normalized filter responses (Equation 10), the BIF method classifies the pixels in the image into one of seven classes according to the structure of local zero, first order, or second-order.

$$s_{mn} = \sigma^{m+n} c_{mn} \tag{10}$$

Based on s_{mn} $(m+n \leq 2)$, we calculate the following quantities:

$$\lambda = s_{20} + s_{02}, \quad \gamma = \sqrt{(s_{20} + s_{02})^2 + 4s_{11}^2} \tag{11}$$

Finally, the resulting classes are: *flat* (εs_{00}), *dark rotational* (λ), *light rotational* $(-\lambda)$, *dark line* $(\frac{\gamma+\lambda}{\sqrt{2}})$, *light line* $(\frac{\gamma-\lambda}{\sqrt{2}})$, *slope* $(2\sqrt{s_{10}^2 + s_{01}^2})$ and *saddle* (γ). These seven BIFs are illustrated in the Fig. 4. In general, the only free parameters to adjust in the BIF system are the filter scale σ and ε which controls the amount of image classified as flat ($\varepsilon = 0.05$ is an effective default).

In pattern recognition systems, local orientation is one of the distinguishing features to take into account. Therefore, it is desirable to combine local symmetry with local orientation, resulting in oriented Basic Image Features (oBIF) which is an extension of the BIF system. Indeed, the orientations that can be assigned depend on the type of local symmetry. So, due to the rotational symmetry of the dark or light rotational and the flat classes, no orientation is assigned (0 quantisable orientation). For the classes of dark lines, light lines, saddle, a possible orientation can be assigned (3 quantisable orientations of the three classes). Finally, two possible orientations can be attributed to the slope class (2 signed quantisable orientations). So if the number of unsigned orientations is n_{φ}, we can get $5n_{\varphi}$ + 3 different types of oBIF. Several works show that n_{φ} = 4 (23 oBIF types) is sufficient to obtain an optimal performance. once the type of BIF has been determined, the following formulas are evaluated to determine possible orientations: $\arctan(\frac{2s_{11}}{s_{02}-s_{20}+\gamma})$ for dark line, light line and saddle, and $\arctan(\frac{s_{01}}{s_{10}}) \pm \pi$ for slope.

Our scheme uses binary templates, for that, to extract the lines of the image, the *oBIF*-response $(\mathcal{A}_{oBIF})$ must be coded “0” or “1” according to the predefined binarization threshold (T_{th}). Therefore, the binary vector, $V_{oBIF}(i,j)$, is represented by the following inequalities:

$$\mathcal{V}_{oBIF}(i,j) = \begin{cases} 1, & \text{if} \quad \mathcal{A}_{oBIF}(i,j) \geq T_{th} \\ 0, & \text{if} \quad \mathcal{A}_{oBIF}(i,j) < T_{th} \end{cases} \tag{12}$$

The value of the binarization threshold is given as follows:

$$T_{th} = k_{th} \cdot \rho \tag{13}$$

where ρ indicates the mean value of the response $(\mathcal{A}_{oBIF})$ and the k_{th} is a constant value. Finally, it is important to note that the value of k_{th} is chosen (empirically) maximize the identification rate.

5.2 System Framework

The proposed system can be used in several network-related tasks such as *e*-commerce, *e*-banking and *e*-voting. These applications are divided into two parts: the user terminal and the central system. Also, in a biometric system, the user must be enrolled in the system database before any use. To understand the activities taking place at each stage of our cryptosystem, the most important steps are described below.

5.2.1 Enrolment Phase

During the enrollment phase, the user's feature vectors (or biometric templates) are extracted from his biometric (PLP and PLV) data using the oBIF method and stored in the system database with all of the user's ID objects for later use in the identification process. Besides, a random integer value ($\mathcal{N}_0$) must be generated and stored as a variable user ID. This value is used for security purposes (template encryption) and during operation; this value is automatically modified (substitution with $\mathcal{N}_s$, which is previously embedded into the template) with each transmission. This process can be run online by passing the key $\mathcal{N}_0$ to the user over the phone. In this case, $\mathcal{N}_0$ is directly modified when the user is enrolled in the system database.

5.2.2 Identification Phase

In all e-application transmission, the application consists of two parts. One for the user terminal, and the other other for the central server (administration). The user's request is sent over the network in an encrypted data format (the message data and their template). Thus, the administrator (central server) must decrypt the template (using $\mathcal{N}_0$) and identify the user using the feature matching. If it accepts, the system retrieves $\mathcal{N}_k$, generates the key, decrypts the message data (using the AES algorithm), extracts $\mathcal{N}_s$, substituting $\mathcal{N}_0$ by $\mathcal{N}_s$, and sends a confirmation to the user terminal to also replace $\mathcal{N}_0$ by $\mathcal{N}_s$. The following algorithm is executed at the user terminal (at the transmitter).

- ▷ Perform the Region of Interest (ROI) extraction method on the original PLP and PLV images. This task is performed automatically during the acquisition process. The program intended for acquisition is designed to capture the ROI by placing the points of the two corners of the rectangle displayed on the Smartphone screen on the two specific points of the user's palm, which are the point between the little and the ring fingers and the other between the middle and index fingers.
- ▷ On the basis of the oBIF method, generate, from the PLP and PLV ROI sub-images, 2D binary vectors, designated respectively by $\mathcal{V}^{PLP}_{oBIF}$ and $\mathcal{V}^{PLV}_{oBIF}$.
- ▷ Compares the user-entered key and PIN code. If they are not equal, go to the end (no entry).
- ▷ Generate two random integer values ($\mathcal{N}_k$ and $\mathcal{N}_s$) and convert them to 16-bit binary codewords.
- ▷ Based on $\mathcal{N}_0$ and $\mathcal{L}^0$, generate an integer sequence to determine the locations used to embed $\mathcal{N}_k$ (in $\mathcal{V}^{PLP}_{oBIF}$) and $\mathcal{N}_s$ (in $\mathcal{V}^{PLV}_{oBIF}$), see subsection 5.3.1;
- ▷ Gather both biometric templates ($\mathcal{V}^{PLP}_{oBIF}$ and $\mathcal{V}^{PLV}_{oBIF}$) in a one biometric template designated by $\mathcal{V}^{U}_{oBIF}$, see subsection 5.3.3;
- ▷ Based on $\mathcal{N}_k$ value, generate the AES encryption key (k), see subsection 5.3.2;
- ▷ Encrypt the message (m) with the key k, which gives an encrypted message denoted by $\widehat{m}$.
- ▷ Based on $\mathcal{N}_1$, $\mathcal{N}_2$ values and $\mathcal{L}^1$, $\mathcal{L}^2$ and $\mathcal{C}^1$ chaotic systems, encrypt the biometric template ($\mathcal{V}^{U}_{oBIF}$) which is denoted by $\widehat{\mathcal{V}}^{U}_{oBIF}$, see subsection 5.3.3;
- ▷ Send both the encrypted message $\widehat{m}$ and the encrypted biometric template $\widehat{\mathcal{V}}^{U}_{oBIF}$;
- ▷ If a confirmation, from the central server (administration), has been received, replace $\mathcal{N}_0$ with $\mathcal{N}_s$.

Upon receipt (at the recipient level), the administrator must execute the following algorithm to retrieve the key and authenticate the transmitted user.

- ▷ For each user stored in database, use its $\mathcal{N}_1$, $\mathcal{N}_2$, $\mathcal{L}^1$, $\mathcal{L}^2$ and $\mathcal{C}^1$ to decrypt template ($\widehat{\mathcal{V}}^{U}_{oBIF}$).

- ▷ Disperse the two biometric templates $\mathcal{V}_{oBIF}^{PLP}$ and $\mathcal{V}_{oBIF}^{PLV}$ from $\mathcal{V}_{oBIF}^{U}$, then reshape original templates;
- ▷ Run the feature matching process (using $\mathcal{V}_{oBIF}^{PLP}$ and/or $\mathcal{V}_{oBIF}^{PLV}$) to identify the user;
- ▷ If there is a genuine, using its $\mathcal{N}_0$ and $\mathcal{L}^0$, generate an integer sequence to determine the locations used to retrieve $\mathcal{N}_k$ (from $\mathcal{V}_{oBIF}^{PLP}$) and $\mathcal{N}_s$ (from $\mathcal{V}_{oBIF}^{PLV}$), see subsection 5.3.1;
- ▷ Based on $\mathcal{N}_k$ value, generate the AES encryption key (k), see subsection 5.3.2;
- ▷ Decrypt the message ($\widehat{m}$) using the key k, which gives the original message (m).
- ▷ Replace the $\mathcal{N}_0$ value with the $\mathcal{N}_s$ value and send a confirmation to the terminal user.

If the connection is lost prior to confirmation, the user (after referring to this) requests the secret key by sending his identity and one of his ID objects (encrypted with a key being sent for this request), or by re-accessing using the last two keys.

5.3 Proposed encryption method

The biometric cryptosystem proposed in our work uses chaotic systems to: *i)* determine the locations used to embed integer values (in 16-*bit* binary representation) in the biometric template (Insertion of $\mathcal{N}_k$ and $\mathcal{N}_s$); *ii)* generate the cryptographic key for the AES algorithm, and *iii)* encrypt the user's biometric template ($\widehat{\mathcal{V}}_{oBIF}^{U}$).

5.3.1 Determination of embedding locations

Our algorithm uses the chaotic system $\mathcal{L}^0$ to determine the locations used to embedding the $\mathcal{N}_k$ and $\mathcal{N}_s$ values (two integers of 16 *bits* each) into the biometric template. The parameters of the chaotic system $\mathcal{L}^0$ (control parameter and initial state) are defined as follows:

$$\begin{cases} u_{00} = u_0^0 + (4 - u_0^0)\frac{\mathcal{N}_0}{2^{16}},\ u_0^0 \in [3.57, 4[\\ x_{00} = x_0^0 + (1 - x_0^0)\frac{\mathcal{N}_0}{2^{16}},\ x_0^0 \in [0, 1[\end{cases} \tag{14}$$

Thus, the chaotic system generates a sequence ($\mathcal{S}_0$) in which their components are between [0,1]. So, to normalize it to $[1, N]$, the following equation is applied:

$$\widetilde{\mathcal{S}}_0 = \lfloor 10^5 \cdot \mathcal{S}_0 \rfloor \pmod N \tag{15}$$

where $\widetilde{\mathcal{S}}_0$ is an integer sequence obtained from $\mathcal{L}^0$ and $N \times N$ is the size of biometric templates $\mathcal{V}_{oBIF}^{PLP}$ and $\mathcal{V}_{oBIF}^{PLV}$. Since the length of $\mathcal{N}_k$ (or $\mathcal{N}_s$) is 16 *bits*, the length of $\widetilde{\mathcal{S}}_0$ must be equal to 16×2 = 32 components (each of the two components represents a coordinate (x, y) in the biometric template). The vector $1{\times}32$ found is reshaped into a $2{\times}16$ vector so that the bit i of $\mathcal{N}_k$ (or $\mathcal{N}_s$) is embedded into the $\mathcal{V}_{oBIF}^{PLP}(\widetilde{\mathcal{S}}_0(1, i), \widetilde{\mathcal{S}}_0(2, i))$ (or $\mathcal{V}_{oBIF}^{PLV}(\widetilde{\mathcal{S}}_0(1, i), \widetilde{\mathcal{S}}_0(2, i))$). It should be noted that the 16 coordinates found must be checked so that they do not repeat and the embedded process is performed by a simple substitution of Least Significant Bit (LSB) (ARM mbed) of the pixel $\mathcal{V}_{oBIF}^{PLP}(\widetilde{\mathcal{S}}_0(1, i), \widetilde{\mathcal{S}}_0(2, i))$.

5.3.2 AES cryptography key generation

The integer $\mathcal{N}_k$ is converted to a 16-*bits* binary codeword. Its first 4 *bits* (k_2) are reserved for defining the length of the AES cryptographic key (16 possibilities), while the 12 *bits* (k_1) are also decomposed into two other binary codewords (k_{11} and k_{12}), each of six bits. Then, the three binary codewords (k_1, k_{11} and k_{12}) are converted into decimal values ($\mathcal{N}_{k_1}$, L_1 and L_2). The initial state of the chaotic system

$\mathcal{L}^m$ is defined as in $\mathcal{L}^0$ using $\mathcal{N}_{k_1}$ (instead of $\mathcal{N}_0$), while L_1 and L_2 are used to determine the initial states of the chaotic systems $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$ as follows:

$$x_{0m1} = x_{L_1} = \mathcal{S}_m(L_1), \quad x_{0m2} = x_{L_2} = \mathcal{S}_m(L_2) \tag{16}$$

where $\mathcal{S}_m$ denotes the sequence generated by the chaotic system $\mathcal{L}^m$. Finally, the sequences obtained by the chaotic systems $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$ are normalized between [0, 255], which gives S_k^1 and S_k^2, then concatenated to get a unique sequence S_k. Thus, to obtain the AES cryptographic key (k), the sequences S_k must be converted into binary codewords, then selecting a subsequence of length defined by k_2.

5.3.3 Biometric template encryption/decryption

The template encryption method used in our work is based on the transformation principle. Before starting the encryption process, the two biometric templates (binary format) must be combined into one biometric template (decimal format).

$$\mathcal{V}_{oBIF}^{U} = \mathcal{F}_{\text{DEC}}(\mathcal{V}_{oBIF}^{PLP}, \mathcal{V}_{oBIF}^{PLV}) \tag{17}$$

where $\mathcal{F}_{\text{DEC}}$ denotes the decimal conversion function. This step reduces the amount of data, in which the binarized templates are converted to an integer-valued template. So each $H \times W$-sized template is divided into four parts (each part size is $\frac{H}{2} \times \frac{W}{2}$). The parts of the two templates are then grouped together in a tensor ($\mathcal{T}_{oBIF}^{PV}$) of size $\frac{H}{2} \times \frac{W}{2} \times 8$. Finally, the string of 8-bit around each location ($x = [1, \frac{H}{2}]$ and $y = [1, \frac{W}{2}]$) is converted using the following decoding polynomial (binary to decimal conversion process):

$$\begin{gathered} \mathcal{V}_{oBIF}^{U}(x, y) = \sum_{i=1}^{8} 2^i \cdot \mathcal{T}_{oBIF}^{PV}(x, y, i) \\ x \in [1, \frac{H}{2}], \quad y \in [1, \frac{W}{2}] \end{gathered} \tag{18}$$

Now the encryption operation can start by executing the following algorithm in the user terminal (the sender).

1. The integer value $\mathcal{N}_2$ is used by the chaotic system $\mathcal{L}_2$ to generate a sequence $\mathcal{S}_2$. The initial state x_{02} of the chaotic system $\mathcal{L}_2$ is equal to x_0^2 + $(1 - x_0^2)\frac{\mathcal{N}_2}{2^{16}}$. After normalization ([0, 255]), $\mathcal{S}_2$ is reshaped into matrix $\mathcal{M}$ of size $b_l \times b_l$;

2. Decomposition of matrix $\mathcal{M}$ by orthogonal decomposition, as follows:

$$\mathcal{M} = \mathcal{Q} \cdot \mathcal{R}, \text{ with } \mathcal{Q}^{-1} = \mathcal{Q}^T \tag{19}$$

3. Decomposition of the biometric template $\widehat{\mathcal{V}}_{oBIF}^{U}$ into n blocks (B) of size $b_l \times b_l$;

4. The integer value $\mathcal{N}_1$ is used by the chaotic system $\mathcal{L}_1$ to generate a sequence $\mathcal{S}_1$ of n pairs. The initial state x_{01} of the chaotic system $\mathcal{L}_1$ is equal to x_0^1 + $(1 - x_0^1)\frac{\mathcal{N}_1}{2^{16}}$. After normalization ([0, 100]), each pair of components is used as control parameters (a, b) for Arnold's cat system (for each block);

5. For each block, B_i, do

   5.1 Use control parameters a, b, and the block size b_l to calculate the Arnold's Cat period (τ_{cat});

   5.2 Apply the Arnold's cat algorithm on the block (B_i) τ_{cat}/2 times, which gives $B_i^{\tau_{cat}/2}$;

   5.3 Project the transformed block ($B_i^{\tau_{cat}/2}$) in $\mathcal{Q}$

$$\widetilde{B}_i^{\tau_{cat}/2} = B_i^{\tau_{cat}/2} \cdot \mathcal{Q} \tag{20}$$

5.4 Apply the Arnold's cat algorithm on the resulting block ($\widetilde{B}_i^{\tau_{cat}/2}$) τ_{cat}/2 times.

6. Arrange the blocks as an image.

Upon receipt (at the recipient level), the administrator must execute the decryption algorithm to retrieve the biometric template. Indeed, the decryption algorithm is the same as that of the encryption, except step 5.3 which must be modified as follows:

5.3 Project the transformed block ($B_i^{\tau_{cat}/2}$) in $\mathcal{Q}^{-1}$

$$\widetilde{B}_i^{\tau_{cat}/2} = B_i^{\tau_{cat}/2} \cdot \mathcal{Q}^{-1} = B_i^{\tau_{cat}/2} \cdot \mathcal{Q}^T \tag{21}$$

After decryption of $\mathcal{V}_{oBIF}^{U}$, the two templates ($\mathcal{V}_{oBIF}^{PLP}$ and $\mathcal{V}_{oBIF}^{PLV}$) can be recovered by using the reverse operation of $\mathcal{F}_{\text{DEC}}$.

$$(\mathcal{V}_{oBIF}^{PLP}, \mathcal{V}_{oBIF}^{PLV}) = \mathcal{F}_{\text{BIN}}(\mathcal{V}_{oBIF}^{U}) \tag{22}$$

where $\mathcal{F}_{\text{BIN}}$ denotes the binary conversion function.

5.4 Effectiveness of the methodology

Most biometric cryptosystems use the face, iris, signature and fingerprint as biometric traits. Indeed, these traits have advantages and disadvantages:

1) Iris and fingerprint based systems can provide high accuracy, users find them unacceptable. In the case of the iris-based system, the user makes every effort to avoid exposing his eye to the sensor while the fingerprint is considered very sensitive (legal) information.

2) Signature and face based-system have high user acceptability but low accuracy due to the high intra-class variability.

Recently, hand-palm biometrics modalities (palmprint/palm-vein) have recently emerged as powerful alternative modalities. When compared to several other modalities, the palmprint and palm-vein have many advantages, the most important of which are their high acceptability by users, the stability of their biometric feature, and the high accuracy, as result, these modalities have recently piqued the interest of many researchers. In addition to the use of these two biometric modalities in our scheme, which are in themselves an important advantage, our proposal has advantages over many biometric cryptosystems in the literature through the following points:

1) Our scheme works in a variety of AES key lengths. So, a system in two different transmissions can be operated with two keys of different length, which will certainly increase the security level.

2) Biometric templates are automatically discontinued each time you submit. This means that the system can work with two different models in two different presentations, which will definitely improve user integrity.

3) Use of the concept of multibiometric where two biometric templates (extracted from the PLP and the PLV) are effectively combined into one small template.

4) Without sharing the hash key (without sending any key information or just without sending $h(c)$). Therefore, the key is extracted from the biometric template after successful authentication.

5) The security key (message encryption key and template protection) is generated from a small 16-bit string. This length was chosen because it does not affect the template much upon insertion, and for this reason it is possible to insert a specific copy of this key to increase noise resistance (the template size is much larger than the size of the key). Furthermore, the main advantages of the proposed cryptosystem scheme can be seen in its implementation in existing communication devices. Smartphone, tablets, and personal computers have recently been widely and conveniently used by users to communicate via real-time online communication. The majority of these devices now have cameras that can capture, process, encrypt, and transmit biometric data. Because of its memory capacity and impressive speed, the world of Smartphones has advanced to the point where it can now implement sometimes complex programs.

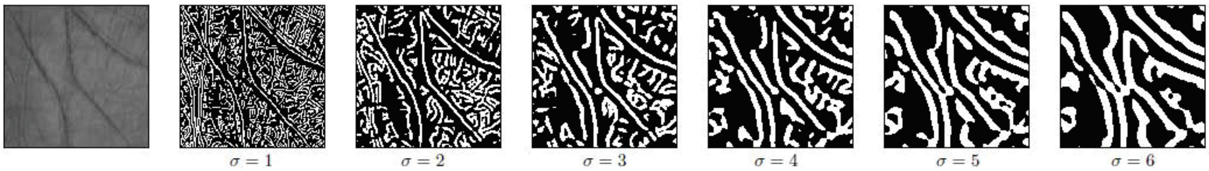


Fig. 5. An example of the binary features of the palmprint image under different filter scale values (σ)

6. Experimental Results and Discussion

In our experiments, we need a multibiometric dataset is needed to test and validate the robustness and effectiveness of the proposed scheme, which, unfortunately, was not available. For this, we use an accessible and publicly available multispectral palmprint dataset (Hong Kong Polytechnic University (PolyU) (PolyU Hong Kong))) to form a synthetic multibiometric data set. Thus, in our dataset, the palmprint modality is represented by the grayscale image that is built using three spectral bands (*blue*, *green*, *red*), whereas the palm-vein modality is represented by a spectral band near infrared. However, the obtained palmprint and palm-vein datasets contain images captured with a palm image acquisition device developed at the Hong Kong Polytechnic University. In general, the palm images for these databases were collected from volunteers among the students and staff of this university. Images of the palm with significant intra-class deformation, such as different hand poses and different lighting conditions, can be found in these databases. Also, these images were collected in two separate sessions. At each session, each person is asked to provide six images that are captured in four spectral bands. The experimental results in our work are divided into two parts. The proposed bio- metric system is tested and evaluated in the first part using the database described above. This part can also be divided into two subparts, the first of which presents the unimodal system (PLP and PLV), while the second subpart deals with the multimodal system (PLP and PLV fusion). In the second part, we examine key security as well as template encryption security. To assess the performance of our proposed biometric system, we use a dataset of 300 people and select three samples at random from a total of 12 samples for each modality (PLP or PLV) to create the system database (enrolment phase). The remaining nine samples were set aside for testing. Thus, we can obtain the genuine experiences by comparing nine test samples to the corresponding class in the database. Therefore, a total of 2700 scores were generated. Similarly, we can obtain the impostor's experiences by comparing these samples to all classes in the database (except their class. As a result, a total of 403650 scores were generated.

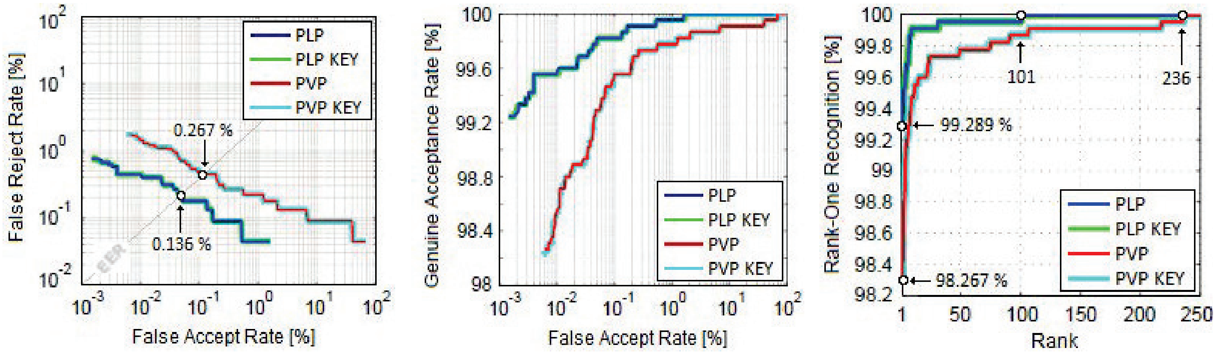
6.1 Biometric System Test Result

In a biometric system, the feature extraction task has a significant impact on the biometric identification rate. Because our feature extraction method (oBIF) depends not only on the binarization threshold, but also on the Gaussian filter scale (σ), we ran a series of experiments with the modalities PLP and PLV to find the best parameters (filter scale). So if σ changes, you can get multiple feature vectors, as a result; You can choose the appropriate empirical σ, that can effectively improve the vector accuracy of the feature vector by varying it each time and choosing the best that gives the best performance. An example of a feature vector (template) for a palmprint image obtained in this way with a binarization threshold $T_{th} = \rho$ ($k_{th} = 1.00$) is shown in Fig. 5. From this figure, for example, if $\sigma = 3.00$, the resulting feature vector contains several non-discriminant features that result in a higher correlation between inter-classes. For that, objective tests are done to choose σ, and the results show that six (σ = 6.00) is sufficient to achieve good accuracy. Henceforth, we select this σ to conduct several experiments to compare the effectiveness of the PLP and PLV based biometric systems.

The purpose of the next part is to evaluate the performance of the biometric system using the parameters already selected ($\sigma = 6.00$, $k_{th} = 1.00$). Therefore, the result of the identification test is divided into two parts. First, we present the performance of a nonlinear biometric system, and the results of the second part aim to evaluate the performance of a multimodal biometric system.

TABLE 1 : PERFORMANCE OF THE UNIMODAL BIOMETRIC SYSTEMS

MODALITY	OPEN-SET IDENTIFICATION				CLOSED-SET IDENTIFICATION			
	WITHOUT KEY		WITH KEY		WITHOUT KEY		WITH KEY	
	T_o	EER [%]	T_o	EER [%]	ROR [%]	RPR	ROR [%]	RPR
PALMPRINT	0.2878	0.1360	0.2878	0.1366	99.2889	101	99.2889	101
PALM-VEIN	0.2760	0.2670	0.2784	0.2754	98.2667	236	98.2667	236



(a) (b) (c)

Fig. 6. Performance comparison of the unimodal *open-set/closed-set* identification systems using PLP and PLV biometric modalities (with and without embedded key). *(a)* DET curves, *(b)* ROC curves, and *(c)* ROC curves.

6.1.1 Unimodal biometric system

The performance of the biometric system was evaluated in this series of tests by using the information provided by each modality (PLP and PLV). Indeed, the biometric system must be tested in both cases, without $\mathcal{N}_x$ (raw template) and with $\mathcal{N}_x$ ($\mathcal{N}_k$ embedded in $\mathcal{V}_{oBIF}^{PLP}$ and $\mathcal{N}_s$ embedded in $\mathcal{V}_{oBIF}^{PLV}$). It is important to note that $\mathcal{N}_x$ is a binary vector with 16 *bits*; the difference between the raw template and the template after the embedding of $\mathcal{N}_x$ is equal to 16 *bits* (maximum difference). Thus, using the normalized Hamming distance, the distance produced between two templates for the same person is 0.000977, which has no effect on the accuracy of the system. To see the performance of the open/closed-set identification systems, we plot the results of the PLP and PLV modalities in Fig. 6. In this figure, it is clear that, first, the system performs nearly identically with or without $\mathcal{N}_x$ for both modalities. Second, the obtained accuracy is very acceptable, reflecting the efficiency of the feature extraction method.

To chose the best modality in both identification modes (open-set and closed-set), a table of results, expressed as the lowest Equal Error Rate (EER) as a function of the threshold (T_o) and the Rank-One Recognition (ROR) according to the Rank of Perfect Recognition, is generated (see Table 1). In the case of the open-set identification mode, the results obtained from this table show that the performance of PLP modality is better than that of PLV modality. Thus, when compared to the PLV modality, the PLP modality shows a 49% improvement. Thus, the system can give an EER of 0.137 % (T_o = 0.2878) and 0.2754 % (T_o = 0.2784) for PLP and PLV, respectively. A comparison between these modalities is drawn in the form of Receiver Operating Characteristics (ROC) and Detection Error Trade-off (DET) curves in Fig. 6.*(a)* and Fig. 6.*(b)*, respectively.

Similarly, it can be seen in Table 1 that closed-set identification performance is generally improved when using the PLP modality. These results show that the performance of the PLP outperforms the PLV and can effectively improve the performance of the biometric system of a ROR equal to 99.289% and an RPR equal to 101 instead of 98.267% (RPR = 236). One figure compares the two performances (PLP and PLV) in the form of a Cumulative Match Curves (CMC) is illustrated in 6.*(c)*. A careful examination of all the obtained results leads to the conclusion that, in general, the unimodal system performances are significantly improved as a result of the feature extraction method used.

6.1.2 Multimodal biometric system

The When a single biometric trait is used, the performance of the biometric system produces some errors (Maryam *et al.* 2019). Thus, it is preferable to use the data fusion principle to improve its performance (Gurjit *et al.* 2018). Because our proposed cryptosystem is already based on two modalities, the identification task must evaluate when these modalities are fused. Thus, in this context, PLP and PLV operate independently, and their results are combined using a score level fusion scheme. Moreover, in this part, it is imperative to evaluate the performance of the identification system in both cases, without $\mathcal{N}_x$ (raw template) and with $\mathcal{N}_x$ ($\mathcal{N}_k$ embedded in the template $\mathcal{V}_{oBIF}^{PLP}$ and $\mathcal{N}_s$ embedded in the template $\mathcal{V}_{oBIF}^{PLV}$).

Because of its simplicity, efficiency, and ease of implementation, the fusion at matching score level (Nanang *et al.* 2019) is the most commonly used approach In our study, we use the rule-based fusion technique to test sum-score (SUM), sum-weighting-score (WHT), min-score (MIN), max-score (MAX), and mul-score (MUL) to find the rule that optimizes the system accuracy. To demonstrate the effectiveness of the PLP and PLV data fusion, the results of open-set/closed-set identification tests at the EER point and the ROR point are shown in Table 2 and Table 3. This Table 2 clearly shows that our open-set identification biometric system offers the best possible accuracy in all fusion rules. However, this biometric system can work with a minimum EER (EER = 0.098 % at T_o = 0.1014) in the case of the MUL rule when we use the raw template (without $\mathcal{N}_x$). Thus, a slight degradation of 7.15 % can be obtained if we use a template with $\mathcal{N}_x$, in which case the biometric system operates with an EER equal to 0.105 % at a threshold T_o = 0.1093. Fig. 7 depicts the obtained results in the form of graph DET and graph ROC comparing the two cases.

To further validate our idea, we performed additional tests for the closed-set identification mode, and the results in Table 3 also demonstrate the effectiveness of data fusion. In this case, the biometric identification system works very well (according to the WHT rule) with a ROR equal to 99.689 % and a minimum RPR equal to 36. It should be noted that the inclusion of $\mathcal{N}_x$ in both biometric templates has no effect on the identification result. Finally, in Fig. 7.*(c)*, we plot the closed-set identification performances (CMC curve) for the two cases (with and without $\mathcal{N}_x$).

6.2 Security Analysis

A secure *e*-application must be resistant to all types of cryptanalysis attacks (Vei *et al.* 2019). This subsection is dedicated to examining the level of security of our proposed cryptosystem. Assuming the attacker is aware of the cryptosystem's architecture, the key space must be large enough to render his attack impossible to execute within an acceptable time interval (Chengqing *et al.* 2018). Furthermore, a minor change in the cryptoraphy key should result in completely different encrypted data.

6.2.1 Key Space Analysis

In our scheme, two encryption algorithms are used, the first is based on the AES encryption algorithm to encrypt the user's data, while the second is a proposed algorithm using to encrypt the user's template. We give below an analysis of the two key spaces.

• *AES Key Space Analysis:* in the generation of AES encryption keys, our scheme uses three coupled 1D logistic maps ($\mathcal{L}^m$, $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$) to generate three sequences respectively (S_m, S_{m_1} and S_{m_2}). Thus, in our experimental tests, we empirically fixed the control parameter (u_α) at 3.65, 3.75 and 3.95 for $\mathcal{L}^m$, $\mathcal{L}^{m_1}$ and $\mathcal{L}^{m_2}$, while we choose their initial states as follows:

$$\begin{cases} x_0^m = 0.34 + 0.66 \cdot \frac{k_1}{2^{16}} \\ x_0^{m_i} = \frac{0.28}{i} + (1 - \frac{0.28}{i}) \cdot \mathcal{S}_m(L_i), \quad i = 1, 2 \end{cases} \tag{23}$$

where L_i ($i = 1, 2$) are two integer values derived from $\mathcal{N}_k$ by a simple binary-to-decimal transformation, this variable nature allows our system to generate two different keys for the same person. It is

TABLE 2 : PERFORMANCE OF THE MULTIMODAL OPEN-SET IDENTIFICATION SYSTEMS

KEY	SUM		WHT		MIN		MAX		MUL	
	T_o	EER	T_o	EER	T_o	EER	T_o	EER	T_o	EER
No	0.3255	0.111	0.3430	0.133	0.2259	0.120	0.3816	0.214	0.1014	0.098
Yes	0.3283	0.114	0.3447	0.133	0.2259	0.120	0.3841	0.218	0.1039	0.105

TABLE 3 : PERFORMANCE OF THE MULTIMODAL CLOSED-SET IDENTIFICATION SYSTEMS

KEY	SUM		WHT		MIN		MAX		MUL	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
Yes	99.689	82	99.689	36	98.711	86	99.644	232	98.711	65
No	99.689	82	99.689	36	98.711	86	99.644	233	98.711	65

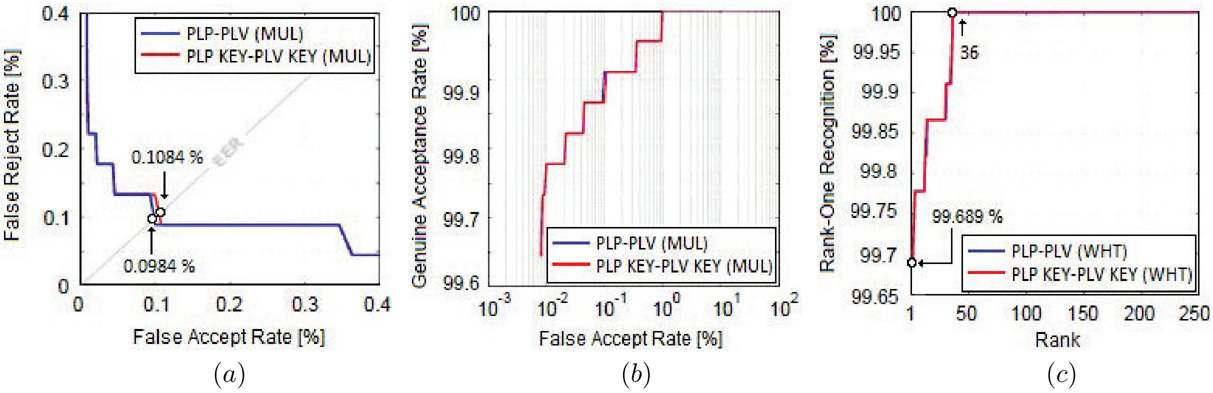


Fig. 7. Multimodal *open/closed-set* identification test results. *(a)* DET curves, *(b)* ROC curves and *(c)* CMC curves.

important to note that our cryptosystem can operate with different key lengths (also fixed with $\mathcal{N}_k$ in each transmission), which is an attractive property that adds the most stringent security requirements to our system. According to *G. Bhatnagar et al.* in (Gaurav *et al.* 2012), the key space is calculated by using all mean absolute errors between two generated sequences, $\mathcal{S}_\alpha$ and $\widetilde{\mathcal{S}}_\alpha$ (for each chaotic systems $\mathcal{L}^\alpha$, $\alpha = m, m_1, m_2$).

$$\text{MAE}(\mathcal{S}_\alpha, \widetilde{\mathcal{S}}_\alpha) = \frac{1}{L_\alpha} \sum_{j=1}^{L_\alpha} |\mathcal{S}_\alpha(j) - \widetilde{\mathcal{S}}_\alpha(j)| \tag{24}$$

where $\mathcal{S}_\alpha$ is a chaotic sequence with length L_α, generated by the chaotic system $\mathcal{L}^\alpha$ having the initial state x_0^α and $\widetilde{\mathcal{S}}_\alpha$ is a sequence generated by the same chaotic system but with an initial state $x_0^\alpha + d_\alpha$. Thus, the key space for x_0^α, called s_α, is equal to $1/d_{0\alpha}$, where $d_{0\alpha}$ is the value of d_α for which MAE = 0. In our scheme, the values of $d_{0\alpha}$ are equal to 1.323×10^{-16}, 1.573×10^{-16} and 1.715×10^{-16} for respectively, x_0^m, $x_0^{m_1}$ and $x_0^{m_1}$ and 1.218×10^{-16}, 1.433×10^{-16} and 1.510×10^{-16} for respectively u_m, u_{m_1} and u_{m_2}. Therefore, the obtained total key space for AES encryption process (s_{AES}) is

$$s_{\text{AES}} = \prod_{i=0}^{2} \frac{1}{d_{0\alpha_i}} \cdot \prod_{i=0}^{2} \frac{1}{d_{u\alpha_i}} = 0.1060 \times 10^{64} \approx 10^{63} \tag{25}$$

Our system can work with a large key space, which allows it to resist different attacks. Finally, this space is also multiplied by the possible number of key length that is 2^4 = 16 possibilities (4 *bits* of $\mathcal{N}_k$ were reserved for the key length). It is important to note that our system works with multi-factor identification because each user has their own key. This means two basic points: the first is that the identification rate increases to $\simeq$ 100% and the second is that the system does not accept the key if the person is an impostor, and therefore that person cannot access the objects of the other person.

- *Template Encryption Key Space Analysis:* In the template encryption, two logistic maps ($\mathcal{L}^1$ and $\mathcal{L}^2$)

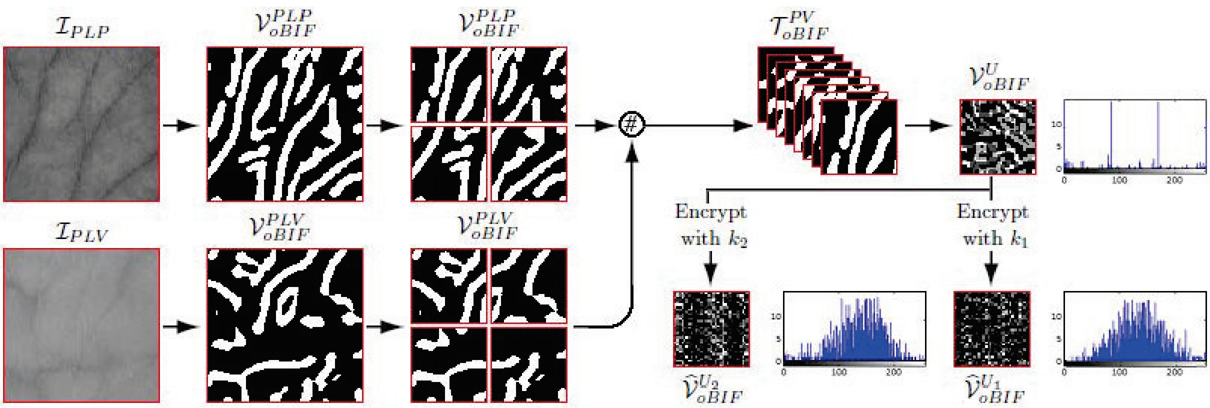

$\mathcal{I}_{PLP}$
$\mathcal{V}^{PLP}_{oBIF}$
$\mathcal{V}^{PLP}_{oBIF}$
$\mathcal{T}^{PV}_{oBIF}$
$\mathcal{V}^{U}_{oBIF}$
$\mathcal{I}_{PLV}$
$\mathcal{V}^{PLV}_{oBIF}$
$\mathcal{V}^{PLV}_{oBIF}$
#
Encrypt with k_2
Encrypt with k_1
$\widehat{\mathcal{V}}^{U_2}_{oBIF}$
$\widehat{\mathcal{V}}^{U_1}_{oBIF}$
10
5
0
0
100
200

Fig. 8. Biometric template encryption process.

and a one Cat map ($\mathcal{C}^1$) are used. The key space is calculated as in the AES key space. Thus, after simulation, we obtain 1,013$\times10^{-16}$, 1,002$\times10^{-16}$, 1,147$\times10^{-16}$ and 1,033$\times10^{-16}$ for x_{01}, x_{02}, u_{01} and u_{02}. Therefore, the total key space obtained for temlate encryption (s_{TEM}) is 0.831$\times$ $10^{64} \approx 10^{64}$ which is sufficient for a secure system. It should be noted that the template encryption process is performed in the middle of the $\mathcal{C}^1$ System period ($\tau_{cat}/2$), so this location can also be varied to increase the key space.

Finally, the user can only interact with his objects if it is precisely identified (*i.e.* identify his identity and the key used to encrypt his message). According to this condition, the global keys space (s_{GLO}) becomes:

$$\begin{aligned} s_{\text{GLO}} &= s_{\text{AES}} \times s_{\text{TEM}} \\ &= 0.106 \times 10^{64} \times 0.831 \times 10^{64} \\ &= 0.088 \times 10^{128} \approx 10^{127} \end{aligned} \tag{26}$$

The results obtained show that the proposed scheme provides a large keys space that enables it to effectively resist probable attacks.

6.2.2 Key Sensibility Analysis

The key sensitivity is the slight difference between cryptography keys that produces completely different encrypted data (Noura *et al.* 2015). It can be calculated as follows:

$$K_s = \frac{1}{H \times W}\left[\sum_{i=1}^{H}\sum_{j=1}^{W} \widehat{\mathcal{V}}^{U_c}_{oBIF}(i,j) \otimes \widehat{\mathcal{V}}^{U_w}_{oBIF}(i,j)\right] \tag{27}$$

where $\widehat{\mathcal{V}}^{U_c}_{oBIF}$ and $\widehat{\mathcal{V}}^{U_w}_{oBIF}$ are the encrypted data using correct and wrong keys, $H \times W$ indicate the template size and $\widehat{\mathcal{V}}^{U_c}_{oBIF}(i,j) \otimes \widehat{\mathcal{V}}^{U_w}_{oBIF}(i,j)$ is equal to 1 if $\widehat{\mathcal{V}}^{U_c}_{oBIF}(i,j) = \widehat{\mathcal{V}}^{U_w}_{oBIF}(i,j)$ and 0 otherwise. In general, if K_s is greater than 75% (Otheila *et al.* 2018), it means that the cryptosystem has good performance. In our tests, three different initial states for the first chaotic system ($\mathcal{L}^1$), which are x_{01} (correct key) and two wrong keys ($x_{01} + 10^{-16}$ and $x_{01} + 10^{-15}$) are examined. The obtained experimental results show that our scheme has the best performance with a K_s equal to 99.6277 % at the $x_{01} + 10^{-15}$ and 99.6521 % at $x_{01} + 10^{-16}$. Therefore, it is clear that the obtained values demonstrate the highly sensitive to the keys, and it is comparable with several kinds of research in literature. Fig. 8 depicts two subjective examples, which include the test templates and their corresponding encrypted templates by the correct and two incorrect keys. Based on this figure, we can conclude that the proposed cryptosystem is very sensitive to any minor modification of the initial state of $\mathcal{L}^1$, allowing us to completely change the encryption biometric templates.

TABLE 4 : PARAMETERS AND RESULTS OF OUR EXPERIMENTS

Feature extraction	PLP PLP	oBIF	$(\sigma, \kappa_{th}) = (6, 1.00)$	
Key insertion	$\mathcal{N}_0 = 1E6D_h$	$\mathcal{L}^0$	$(u_0^0, u^0) = (3.87, 3.8855)$	Sequence of 64 integer components
			$(x_0^0, x^0) = (0.32, 0.4008)$	
AES key generation	$\mathcal{N}_k = A025_h$ $k_1 = 8C7_h$	$\mathcal{L}^m$	$(u_{0L_m}, x_{0L_m}) = (3.65, 0.3626)$	$x_{L_{m1}} = 0.26(L_1 = 43)$ $x_{L_{m2}} = 0.31(L_2 = 29)$
		$\mathcal{L}^{m1}$	$(u_{0L_{m1}}, x_{0L_{m1}}) = (3.75, 0.6832)$	
		$\mathcal{L}^{m2}$	$(u_{0L_{m2}}, x_{0L_{m2}}) = (3.95, 0.4066)$	
Template protection	$\mathcal{N}_1 = 211B_h$	$\mathcal{L}^1$	$(u_0^1, x_0^1) = (3.710, 0.4556)$	$(b_1 \times b_2) = (32 \times 32)$
	$\mathcal{N}_2 = 2CD7_h$	$\mathcal{L}^2$	$(u_0^2, x_0^2) = (3.981, 0.4256)$	
Biometric system performance	PLP	With key	EER = 0.1366 %	Degradation of 0.44%
		Without key	EER = 0.1360 %	
	PLV	With key	EER = 0.2754 %	Degradation of 0.15%
		Without key	EER = 0.2750 %	
	PLP-PLV	With key	EER = 0.105 %	Degradation of 7.14%
		Without key	EER = 0.098 %	
Security analysis	Key space	$S_{AES} \simeq 10^{63}$	Sensitivity : K_s	$> 99.6200\%$
		$S_{TEM} \simeq 10^{64}$		
		$S_{GLO} \simeq 10^{64}$		

6.2.3 Template Histogram Analysis

In image encryption, another evaluation parameter may be used to evaluate the performance of the cryptographic algorithm, namely the histogram analysis (Sovan *et al.* 2019). For an ideal algorithm, the histogram of the encrypted image should be uniform and very different from the histogram of the original image. Fig. 8 also shows the histograms of the biometric template and its version encrypted using two correct keys (k_1 and k_2). Analysis of the figure shows that the inhomogeneity of the encoded template histogram is related to insignificant changes in the pixel amplitude of the original template (we can say that the histogram is practically homogeneous). Second, when we compare the two histograms produced by k_1 and k_2, we can see the most significant difference between them, implying that the proposed biometric cryptosystem is efficient.

6.2.4 Robustness against quantum attacks

Many users have recently expressed concern about the security of encryption algorithms owing to quantum computers, which provide a very fast way to solve the discrete-log problem and the problem of factoring large integers. The adversary can break all key exchange methods by using such quantum computers. So, in our approach, we considered this type of attack with three basic points:

1) The AES-256 symmetric encryption used in our method is ineffective against quantum computers if the key sizes are large enough.

2) The variability of the generated keys length. It is important to note that our system works with keys of different lengths, which means that the length of the key is changed in each transmission. Therefore, the adversary must necessarily try with all lengths ($\sum_{i=1}^{N} 2^{n_i}$, n_i = keys length, and N: number of lengths).

3) The sensitivity of the generated keys. The proposed cryptosystem demonstrates that it is extremely sensitive to even minor changes in the chaotic system's initial state, allowing for complete modification of the biometric templates.

Finally, Table 4 summarizes all of the experiments performed, including the values of all the control parameters for each of the feature extraction method, message encryption and template protection.

6.3 Biometric Cryptosystem Complexity

The complexity of the proposed biometric cryptosystem can be calculated as the sum of the complexity of each algorithm used, including the AES algorithm, the oBIF feature extraction method and the logistics map (LM) algorithm. For the different steps such as insertion, matching, concatenation and fragmentation, they have constant complexity $O(1)$. Thus, the complexity of the proposed cryptosystem can be given by:

$$C_{BCS} = C_{AES} + C_{LM} + C_{oBIF} \tag{28}$$

• Firstly, based on the complexity parameters of AES algorithm which are the block size and the message size, the AES algorithm complexity is computed as follows:

As most cryptographic algorithms (*i.e.* AES, DES, Triple DES, Blowfish) only work on a fixed block size, they take approximately the same time regardless of input, so they are $O(1)$. Also, for any message, the number of calls to the AES encryption/decryption algorithm is a linear function, so it has a complexity of $O(m)$, where m is the size of the message, because we have $O(m)$ blocks of data to be encrypted.

• Likewise, the complexity class of the logistics map depends on the complexity parameter which is the initial value of iteration x_0. Computational space complexity is measured as the loss of precision rate $k = m/N$, where m is the mantissa length needed to represent the initial value x_0 and N is the number of iterations. Thus, a complexity of about $O(K)$ is reached.

• Likewise, the complexity class of the oBIF feature extraction method is based on the six derivatives of Gaussian filters that computes the n^{th} order derivatives of the image in x and y. Raw 2D convolution between a square *N*×*N*-sized image and a square *M*×*M*-sized filter is implemented using two for loops to iterate through each output pixel and two additional for loops to perform the 2D convolution at that pixel's location. Therefore, a total of 4 nested for loops are required; a complexity of $O(N^2 \times M^2)$.

• Finally, a total complexity of about $O(m)+O(K)+O(N^2\times M^2) \simeq O(N^2\times M^2)$ is reached. From the last equation, we can notice that the complexity of our proposal is mainly linked to the feature extraction method, which is only done in the user's terminal (PC or Smartphone). This complexity decreases rapidly to reach the max ($O(m)$, $O(k)$) at the objects level of IoT, which is acceptable by recent hardware. Also, we can replace the AES algorithm by the LSFR algorithm to reduce this complexity.

7. Comparative study

In this section, we will provide an important comparison with modern schemes mentioned in the literature to prove the efficiency of the proposed scheme. Additionally, we will highlight the most significant differences between our scheme and PKI models.

7.1 Comparison with state-of-the-arts

To demonstrate the effectiveness of our proposed method in comparison to other methods, we will conduct a comparative study with some recent works in the literature. Thus, Table 5 summarizes the main works using different biometric modalities. The efficiency of the proposed system is clear from this table, as it outperforms all of the systems mentioned in the table in terms of authentication accuracy (99.895%) and security level ($10^{127} \simeq 2^{421}$), which allows it undoubtedly to be used in applications requiring a high level of security.

7.2 PKI models

The main difference between our proposed cryptosystem and the Public Key Infrastructure (PKI) models lies in the way the keys are generated and managed. PKI is a system that can prove the relationship between public key and user identity, with digital certificates created by an independent Certificate Authority (CA) that acts as a third party for the identity of the owner. Thus, within PKI systems, the generation of private and public keys is managed under various constraints:

• The public key is generated at the same time as the private key,

TABLE 5 : PERFORMANCE COMPARISON TO SOME WORKS IN THE STATE-OF-THE-ARTS

Authors	Biometrics	Security	Feature	GAR [%]	Key space
(Rathgeb *et al.* 2015)	Face and Iris	Adaptive Bloom filters	Local Gabor	99.510	$\simeq 10^{78}$
(Veeru *et al.* 2017)	Face and Iris	Error-correction coding	DNN	92.500	$\simeq 10^{82}$
(Jindal *et al.* 2018)	Face	SHA-3 512	VGG-Face CNN	96.530	$\simeq 10^{77}$
(Li *et al.* 2018)	Iris	RS error correcting code	CNN	98.960	$\simeq 10^{77}$
(Sujitha *et al.* 2019)	Fingerprint and palmprint	Fuzzy vault	Crossing number and bottom-hat filtering	95.000	$\simeq 10^{42}$
(Jang *et al.* 2019)	Face	Deep Table-based Hashing (DTH)	CNN	96.040	$\simeq 10^{72}$
(Jae *et al.* 2019)	Iris	Alignment-free	IrisCode	99.470	$\simeq 10^{89}$
(Wendy *et al.* 2020)	Signature	Fuzzy Vault	Pen-down-time and total-signature-time	94.630	$\simeq 10^{15}$
(Li *et al.* 2020)	Palmprint	Randomized cuckoo hashing and MinHash	Anisotropic filter	95.000	$\simeq 10^{68}$
Proposed	Palmprint and Palm-vein	Transformation (Chaotic systems)	oBIF	99.895	$\simeq 10^{127}$

• The keys are generated before the production of a certificate. The validity of the link between the public and private keys must be verified by the CA before issuing the certificate,

• The public key is either generated at the CA or by a process that the client deems reliable,

• The public key is usually the result of a process that uses a random secret input to generate public and private keys.

Unfortunately, PKI is complex in terms of keys management and revocation, and since connecting a person to their things does not necessitate all this complexity in creating and managing keys, the proposed method can effectively reduce this complexity by developing an alternative security scheme for applications that do not require a very high security level. Therefore, our main idea is based on:

• Unlike PKI which usually uses asymmetric encryption, our scheme uses a symmetric encryption scheme which is efficient in terms of decryption speed and which is a requirement for our application (real-time).

• Key generation can be performed by any user on their device, and there is no need to involve a third party to establish the relationship between the user's identity and their key, which can be verified with its biometric feature.

• Security keys can be generated at different time and do not need to build different digital certificates,

• Key revocation does not rely on a certificate, which is one of the main difficulties encountered by implementers of PKI systems.

8. Conclusion and Further Works

Nowadays, the internet of things (IoT) has proven its efficiency and practicality in the design of smart cities. Such cities, in fact, are unimaginable without an IoT network. Just like the classic Internet, the security aspect is the major challenge in any IoT-framework. Thus, strengthening this security will increase customer confidence, and thus generalize such applications, inevitably leading to an indirect adaptation of citizens to smart cities.

In this paper, we propose a secure cloud-based IoT framework to secure the interaction of the person with his own objects. The main idea of this study is to enhance the security and privacy of users/object information by developing a biometric-based cryptosystem.

Our proposed cryptosystem uses the concepts of a chaotic system combined with PLP and PLV biometrics. In this study, a hand-crafted feature extraction method (oBIF) was used due to its simplicity and speed. Subsequently, the user's requests are encrypted using the AES algorithm, while the user's biometric template is encrypted by a transformation-based encryption algorithm.

In our scheme, the Chaos system was adopted to generate AES encryption keys used to encrypt user messages on the one hand and projection matrices to encrypt biometric templates on the other. Experimental results obtained with a multi-biometric dataset of 300 users show the effectiveness of the proposed to achieve the two goals of the system (privacy and security). In terms of privacy, our biometric system works with an excellent recognition rate (99.895 %), which can be perfect when using multi-factor recognition. In terms of security, a very large keys space has been obtained ($\simeq 10^{127}$) which can be increased further by increasing the number of chaotic systems used.

In the future, we intend to use lightweight deep learning techniques to improve the recognition rate in large databases, as well as hyper-chaotic systems. In addition to using other IoT architectures that are not cloud-based computing.

. Acknowledgements

This work would not have been possible without the financial support of the Directorate General for Scientific Research and Technological Development (DGRSDT). Thus, this research was carried out as part of the PRFU project (Grant: A01L08UN120120180001) of the Department of Electrical Engineering, University of Laarbi Tebessi, Tebessa. The authors also appreciate the invaluable and profound comments from the unknown referees.

. References

Abdur-Razzaq, M., Sheikh, R.A., Baig, A. & **Ahmad, A. (2017)**. Digital image security: Fusion of encryption, steganography and watermarking, In: International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 5.

Adel, O., Giuseppe, G., Ahmad, T.A., Ahmed, G.R., Christos, V., Viet-Thanh, P., Toufik, Z., Ioannis, M.K. & **Ioannis, N.S. (2017)**. Dead-beat synchronization control in discrete-time chaotic systems, In: IEEE 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, pp. 1-4.

Alam, B., Jin, Z., Yap, W.S. & **Goi, B.M. (2018)**. An alignment-free cancelable fingerprint template for bio-cryptosystems, In: J. Netw. Comput. Appl., Vol. 115, PP. 20–32.

Alsbou, N., Chen, K.H.S. & **Afify, M. (2019)**. Smart IoT In Car Life Detector System to Prevent Car Deaths, In: Issarny V., Palanisamy B., ZhangLJ. (eds) Internet of Things ICIOT 2019. Lecture Notes in Computer Science, vol 11519. Springer, Cham.

Amazon dynamodb, In: *https://aws.amazon.com/dynamodb.*

Amazon iot. Awsiot framework, In: *https://aws.amazon.com/iot.*

Amazon ML. Amazon machine learning, In: *https://aws.amazon.com/machine-learning*

Amazon s3. In: *https://aws.amazon.com/s3.*

Apple. The smart home just got smarter. In: *http://www.apple.com/ios/home/.*

ARM plt. Arm mbediot device platform In: *http://www.arm.com/products/iot-solutions/mbed-iotdevice-platform.*

, **ARM**, mbed device connector

Abdeljalil, G., Chawki, D., Youcef, C. & **Imran, S. (2017)**. Oriented Basic Image Features Column for isolated handwritten digit, In: International Conference on Computing for Engineering and Sciences (ICCES17), Istanbul, Turkey, pp. 13-18.

Ardelio, G., Giulio, G., Livia, M. & **Diego, P. (2017)**. An algorithm for Gaussian recursive filters in a multicore architecture, In: Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic , 2017.

Arnold, V.I. & **Avez, A. (1968)**. Ergodic Problems of Classical Mechanics (Advanced Book Classics). W. A. Benjamin, New York.

Atwady, Y. & **Hammoudeh, M.A. (2017)**. Survey on authentication techniques for the internet of things, In: Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS17, New York, NY, USA. ACM.

Azarmehr, M., Ahmadi, A. & **Rashidzadeh, R. (2017)**. Secure authentication and access mechanism for iot wireless sensors, In: IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–4.

Azure, M., Azure iot hub, In: *https://azure.microsoft.com/en- us/services/iot-hub/*

Bilgehan, A., Ezgi, Y., Burcin, A. & **Seref S. (2016)**. Security Perspective of Biometric Recognition and Machine Learning Techniques, In: 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, pp. 492-497.

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B. & **& Zémor, G.(2008)**. Theoretical and practical boundaries of binary secure sketches, In: IEEE Transactions on Information Forensics and Security Vol. 3: PP. 673-683.

Cappelli, R., Ferrara, M. & **Maltoni, D. (2010)**. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition, In: IEEE Trans. Pattern Anal. Mach. Intell., Vol. 32, PP. 2128–2141.

Chengqing, L., Dongdong, L., Bingbing, F., Jinhu, L. & **Feng, H. (2018)**. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy, In: IEEE Access, Vol. 6, pp. 75834-75842.

Ericsson.Open source release of iot app environment calvin, In: *https://www.ericsson.com/research-blog/cloud/open-source-calvin/*

Nada, F.M., Majid, J.J. & **Suhad A.A.(2020)**. Biometric-based medical watermarking system for verifying privacy and source authentication. Kuwait J. Sci. 47 (3) pp. 2-13.

Fhatuwani, V. M., Tranos, Z. & **Martin, A. (2018)**. Users' Perceptions on Security of Mobile Computing for Adoption of e-Applications in South Africa, In: IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, pp. 1-8.

Gaurav, B., & **Jonathan, W.Q.M. (2012)**. Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission, In: IEEE Transactions On Instrumentation And Measurement, Vol. 61, No. 4, pp. 876-887.

Google. Weave, In: *https://developers.google.com/weave/*.Online; accessed: April 2017.

Gurjit, S.W., Shivam, R., Rajesh, A., Aarohi, K. & **Anjana, G. (2018)**. Secure multimodal biometric system based on diffused graphs and optimal score fusion, In: IET Biometrics, Vol. 8, Issue 4, pp. 231-242.

Ishaq, I. ,Carels, D., Teklemariam, G.K., Hoebeke, J., Abeele, F.V., Poorter, E.D., Moerman, I. & **Demeester, P.(2013)**. IETF Standardization in the Field of the Internet of Things (IoT): A survey, In: Journal of Sensor and Actuator Networks. Vol. 2, pp. 235–287.

Jae, Y.J. & **Rae J. (2019)**. Efficient Cancelable Iris Template Generation for Wearable Sensors. Security and Communication Networks, Hindawi, Vol. 2019, pp. 1-13.

Jain, A. K., Nandakumar, K. & **Nagar, A. (2018)**. Biometric template security, In: EURASIP J. Adv. Signal Process,: 1–17.

Jang, Y.K. & **Cho, N.L. (2019)**. Deep Face Image Retrieval for Cancelable Biometric Authentication. Proceedings of the 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2019.

Jindal, A.K., Chalamala, S. & **Jami, S.K. (2018)**. Face Template Protection using Deep Convolutional Neural Network‘¨ In: IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).

Jingjin, G., Lizhen, L., Wei, S., Chao, D. & **Xinlei, Z. (2017)**. The study of image feature extraction and classification, In: IEEE International Conference on Progress in Informatics and Computing (PIC), Nanjing, China, pp. 147-178.

Joshy, A. & **Jalaja, M. J. (2017)**. Design and implementation of an IoT based secure biometric authentication system, In: IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kollam, pp. 1–13.

Jyotismita, C., Nilanjan, D., Fuqian, S. & **Simon, S.R. (2019)**. Pattern Mining Approaches Used in Sensor- Based Biometric Recognition: A Review, In: IEEE Sensors Journal, Vol. 19, Issue 10, pp. 3569-3580.

Krotov, V.(2017). The Internet of Things and new business opportunities, In: Business Horizons, Vol. 60, No. 6, pp. 831–841.

Kuo-Hui Y. (2018). A Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments, In: IEEE Systems Journal, Vol. 12, Issue 2, pp. 2027-2038.

Lee, I. & **Lee, K. (2015)**. The Internet of Things (IoT): Applications, investments, and challenges for enterprises, In: Business Horizons, Vol. 58, No. 4, pp. 431–440.

Li, H., Qiu, J. & **Teoh, A.B.J. (2020)**. Palmprint template protection scheme based on randomized cuckoo hashing and MinHash. Multimed Tools Appl 79, 11947-1971.

Li, P., Yang, X., Cao, K., Tao, X., Wang, R. & **Tian, J.** An alignment-free fingerprint cryptosystem based on fuzzy vault scheme, In: J. Netw. Comput. Appl. Vol. 33, PP. 207–220.

Li, X., Jiang, Y., Chen, M. & **Li, F. (2018)**. Research on iris image encryption based on deep learning. EURASIP Journal on Image and Video Processing, no 126.

Lifang, W., Xingsheng, L., Songlong, Y. & **Peng X.A.(2010)**. Novel key generation cryptosystem based on face features, In: IEEE 10th IC on Signal Processing, pp:1675–1678.

Ling, Z. , Luo, J. , Xu, Y. , Gao, C. , Wu, K. & **Fu, X. (2017)**. Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System, In: IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1899–1909.

Liu, E. & **Zhao, Q. (2017)**. Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with l1minimization, In: Neuro computing, Vol. 259, pp. 3–13.

Mahmoud, A., Gionanni, R. & **Bruno, C. (2018)**. Inernet of Things: A survey on the security of IoT frameworks, In: Joirnal of Information Security and Application, Vol. 38, pp. 8-27.

Maryam, E. & **Omid S. (2019)**. Effect of face and ocular multimodal biometric systems on gender classification, In: IET biometrics, Vol. 8, Issue 4, pp. 243-248.

Microsoft.Tap into the internet of your things with azure iot suite, In: *https:// www.microsoft.com/en-us/cloud- platform/internet-of-things-azure-iot-suite.* Online; accessed: April 2017.

Mochizuki, Y. (2018). Global Perspective for Data-Leveraged Smart City Initiatives, In: *NEC Technical Journal*, vol. 13, no. 1, pp. 14–18.

Mohan A. (2017). Cyber security for personal medical devices internet of things, In: IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE, 2014, pp. 372-374.

Nabil, H. & **Abdelhani, B. (2017)**. Multimodal biometric recognition using human ear and palmprint, In: IET Biometrics, Vol. 6, Issue 5, pp. 351-359.

Nanang, S., Raymond, V., Luuk, S. & **Chris, K. (2019)**. Semiparametric likelihood-ratio-based biometric score-level fusion via parametric copula, In: IET Biometrics, Vol. 8, Issue 4, p. 277-283.

Hassan, N., Soran, H., Steven, M., Lila, B. & **Khaldoun, A.A.E. (2015)**.: An efficient and robust data integrity algorithm for mobile and wireless networks, In: IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, pp. 1-6.

Otheila, C., Hakim, B. & **Abdallah, M. (2018)**. Can Chaos System Provide Secure Communication over Insecure Network? Online ATM services as a case study, In: Journal of Electronic Imaging, Vol. 27, No. 3, 033045.

Pelton, J.N. & **Singh, I.B. (2019)**. The Coming Age of the Smart City. In: Smart Cities of Today and Tomorrow, In: Copernicus, Cham.

Pietro, R., Giuseppe, C., Giovanni, L.M. & **Enrico, G. (2016)**. Accessing Cloud Services through Biometrics Authentication, In: IEEE 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Fukuoka, Japan, pp. 38-43.

PolyU. The Hong Kong Polytechnic University (PolyU) palmprint Database, In: *http://www.comp.polyu.edu.hk/ $\sim$ biometrics*.

Mohammed, Q. & **Hussain, M.J.A. (2019)**. An efficient deception architecture for cloud-based virtual networks. Kuwait J. Sci. 46 (3) pp. 40-52.

Rahul, R., Pankaj, K.S., Banshidhar, M. & **Sambit B. (2016)**. Direction Estimation for Pedestrian Monitoring System in Smart Cities: An HMM Based Approach, In: *IEEE Access*, Vol. 4, pp. 5788– 5808.

Rami, A.H. (2020). Deep learning autoencoder approach: Automatic recognition of artistic Arabic calligraphy types. Kuwait J. Sci. 47 (3) pp. 2-13.

Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J. & **Fierrez, J. (2015)**. Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. 3rd International Workshop on Biometrics and Forensics (IWBF).

Robert, M. (1976). Simple mathematical models with very complicated dynamics, In: Nature. 261 (5560): pp. 459-67.

Sarkar, A. & **Singh, B.K. (2018)**. Cryptographic key generation from fingerprint templates, In: Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 15–17 March, pp. 1-6.

Sha, S., Jia, C., Xin-Li, Z., Yang, L., Jing-Liang, G., & **Yun-Jiang, W. (2018)**. Fingerprint Recognition Strategies Based on a Fuzzy Commitment for Cloud-Assisted IoT: A Minutiae-Based Sector Coding Approach, In: IEEE Access, Vol. 7, pp. 44803-44812.

Shah, T. & **Venkatesan, S.A. (2017)**. Method to Secure IoT Devices Against Botnet Attacks, In: Issarny V., Palanisamy B., Zhang LJ. (eds) Internet of Things ICIOT 2019. Lecture Notes in Computer Science, vol 11519. Springer, Cham.

Smart Things. Smart things documentation, In: *http://docs.smartthings.com/en/latest/.*

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. & **Kumar, B. V. (1998)**. Biometric encryption: enrollment and verification procedures, In: Proceedings of SPIE, Optical Pattern Recognition IX 3386, PP. 24–35.

Sovan, T. & **Isara, A. (2019)**. Robust Image Encryption Method With Cipher Stream Chaining Process, In: IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, Singapore, pp. 283-288.

Sujitha, V. & **Chitra, D. (2019)**. A Novel Technique for Multi Biometric Cryptosystem Using Fuzzy Vault. Interna- tional Journal of Medical Systems, vol. 43, no 112

Suresh, D. & **Priyanka, T. (2018)**. Feature Extraction By Using Deep Learning: A Survey, In: IEEE Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 1795-1801.

Sweedle, M., Prajyoti, D., Snehal, D., Supriya, S. & **Priya, C. (2018)**. Securing ATM Pins and Passwords Using Fingerprint Based Fuzzy Vault System, In: IEEE Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, India, pp. 1-6.

Veeru, T., Matthew C.V. & **Nasser M.N. (2017)**. Multibiometric secure system based on deep learning. IEEE Global Conference on Signal and Information Processing (Global SIP).

Wei, F., Yigang, H., Hongmin, L. & **Chunlai, L. (2019)**. Cryptanalysis and Improvement of the Image Encryption Scheme Based on 2D Logistic-Adjusted-Sine Map, In: IEEE Access, Vol. 7, pp. 12584-12597.

Wendy, P.H., Ramon, B.G., Judith, L.J. & **Raul, S.R. (2020)**. Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification. eIEEE Access, Vol. 8, pp. 11152-11164.

Xi, K., Hu, J. & **Han, F.(2011)**. An alignment free fingerprint fuzzy extractor using near-equivalent Dual Layer Structure Check (NeDLSC) algorithm, In: Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), Beijing, China, 21-23 June, pp. 1040–1045.

Hamdi, Y., Jumana, E.Q. & **Mohamed, A. (2020)**. Specification and recognition of service trust behaviors. Kuwait J. Sci. 47 (1) pp. 33-41.

Yasunori, M. (2017). AI and IoT for Social Value Creation, In: *IEEE Asian Solid-State Circuits Conference (A-SSCC)*, Macau, Macao.

Yi, C.F. & **Pong, C. Y. (2010)**. A Hybrid Approach for Generating Secure and Discriminating Face Template, In: IEEE transactions on information Forensics and security, Vol. 5, no. 1.

Yiding, W. & **Shan, D. (2017)**. Dorsal Hand Vein Recognition Based on Improved Bag of Visual Words Model, In: Chinese Conference on Biometric Recognition, Part of the Lecture Notes in Computer Science book series (LNCS, volume 10568), pp. 203-212.

Submitted	:03/12/2020
Revised	:26/04/2021
Accepted	:27/04/2021
DOI	:10.48129/kjs.11169