An Improved Framework for Biometric Database's Privacy

Ahmed EL-YAHYAOUI[1], Fouzia OMARY[2]

[12]Mohammed V University in Rabat, Morocco

Abstract: Security and privacy are huge challenges in biometric systems. Biometrics are sensitive data that should be protected from any attacker and especially attackers targeting the confidentiality and integrity of biometric data. In this paper an extensive review of different physiological biometric techniques is provided. A comparative analysis of the various sus mentioned biometrics, including characteristics and properties is conducted. Qualitative and quantitative evaluation of the most relevant physiological biometrics is achieved. Furthermore, we propose a new framework for biometric database privacy. Our approach is based on the use of the promising fully homomorphic encryption technology. As a proof of concept, we establish an initial implementation of our security module using JAVA programming language.

Keywords: Performance, Biometrics, physiological traits, improved FHE, privacy, database security, noise-free, encryption**.**

1. Introduction

Biometrics or biometric identifiers refers to the use of different identification techniques in relation with human behaviour and physiology characteristics. It allows to establish and verify the identification of an individual. In this sense, there are several Biometric recognition techniques like face recognition, fingerprint recognition, retina recognition, iris recognition, hand geometry recognition, voice recognition, signature recognition, gait recognition etc. The use of biometrics offers safer authentication compared to traditional techniques such as secret password, PIN number, ID cards and driver's licenses. In fact, Secret passwords and PIN number could be forgotten while ID cards and driver's licenses could be lost, stolen or forged by an adversary. In the other hand, biometric techniques are highly resistant to alteration or unchangeable and cannot be forgotten, misplaced, or transferred to another person which overcomes all previous disadvantages and gives biometric systems an advantage over other verification and identification systems.

Biometrics are measurable and relatively easy to capture by biometric automated systems. Generally, Biometric systems include five main components:

- **A sensor device**: a material or hardware that allows to gather and digitize biometric data. It is employed to capture the necessary verification data from an individual. For example, in fingerprint biometrics applications, an optical sensor is used to produce an image of the ridge structure at a fingertip. This captured image serves as the basis for further access control activity.
- **Data Quality Assessment**: it allows to form the biometric template by following several steps. First of all, the biometric data captured by the sensor device are evaluated to gauge whether it is suitable for processing. Then, an algorithm for signal processing is applied to the data for the purpose of improving its quality. Finally, a specific set of features is selected from the overall data set to form the biometric template.
- **A data storage unit**: is the biometric system database that stores all the information needed for processing biometric templates. The biometric template is input into the database, sometimes just as biographical information related to the user in order to improve security issues.
- **A matching algorithm**: After the biometric template has been extracted from the gathered data, it allows to compare new templates to those previously recorded and stored in the system database as it permits to match it with any identical points. The number of matching points between the input and the template provides a match score, this score can fluctuate between readings depending on the quality of collected data.
- **A decision process**: It allows to use the results of the matching algorithm to accept or reject a new individual. A decision-making apparatus relies on the match score to either confirm an individual's identity or to determine the identity by correlating the score to a ranked list of possible identities stored in the database.

Biometric systems can identify or verify the identity of a person. A system used for identification recognizes the individual's biometric template by comparison to the templates of users stored in its database. A verification system matches an individual's biometric template to a previously stored example of that individual's template.

Currently, various applications of biometrics exist. It could be used in law enforcement, in government, and in civilian applications. In general, law enforcement uses biometrics to identify the suspect of a crime, governments use biometrics to verify the identity of people entering the country. Companies and organizations use biometric systems to restrict access to sensitive information or areas. These applications could be classified into three main categories:

- **Law enforcement applications**: forensic applications, computer access, immigration, national identity, physical access, prisons, telecommunications…
- **Government applications**: national ID cards, border-passport control, driver's license, correctional facility, social security …
- **Civilian applications**: physical access control, Cellular phones, credit cards, computer network login, Automated Teller Machines (ATMs), electronic data security, internet access, medical records management, distance learning…

Biometric systems have some risks and challenges that should be taken into consideration. The first challenge is that biometric sources are not private. In fact, our ears, eyes, fingers, faces… etc are exposed. We reveal our eyes whenever we look at things. With fingerprint recognition we leave fingerprints everywhere we go. With voice recognition, someone is recording our voice when speaking to him via phone. Essentially, there's easy access to all these identifiers. The second challenge is the security and protection of biometric data. In fact, biometrics are hackable either from a database where they are stored or from an illegal collection. For example, a hacker can collect a picture of someone's ear, eye, or finger, therefore he can easily gain access to their personal accounts.

In this paper, we will provide an extensive study of biometric techniques. We will explore biometrics area as one of the most optimistic trends in authentication and identification systems. Actually, a significant attention is given to authentication and identification steps in many authorization contexts. To gain access to a specific resource we should know who are you? (identification) and be sure that the identity you dare is really you (Authentication). We will discover how biometrics could present a suitable, adequate and satisfactory response. We will also provide a security study of biometric systems. Our study will focus on security issues for biometric databases and its related attacks. Databases privacy is a relevant subject for biometrics. Taking into consideration this problematic, we will introduce a new framework for biometric databases privacy in the last section. Our solution is noise-free FHE based. Its objective is data encryption and processing encrypted biometrics without any prior decryption.

1.1. Motivation

Nowadays, biometric systems are widely spread with a large number of applications like legal applications, government applications, commercial applications and so on. The architecture of any biometric system contains a database component for templates storage. Most of those systems store templates in clear which expose privacy of biometrics to internal and external hackers.

Unfortunately, if the security of the biometric database is compromised then the identification and authentication process ensured by the system will be questioned. What could happen exactly when we store biometrics in clear? What happens to system users if a non-trusted third part gain a successful access our biometric database? Clearly, the attackers will have the possibility to bypass the established security by the biometric system and impersonate user's identities.

Our new framework will allow to preserve biometric database privacy even if an attack take place. Currently, we believe that biometric databases need a new framework for data privacy that allows encryption and processing of data for comparison and decision purposes. This obligation will require rethinking biometric technologies and constructing new solutions with biometric data privacy and security in mind. Hopefully, we stand at the edge of a new phase of processing with encrypted data. After more than 10 years of scientific research, there have been significant advances in the fields of homomorphic encryption and processing of encrypted data, resulting in the disclosure of a new technology—known as the fully homomorphic encryption—which has the capacity to allow computation over encrypted data without any prior decryption. In this paper, we exploit the reliability guarantees provided by this encouraging technology to build a privacy framework for biometric databases.

1.2. Contribution

This paper is an extension of our prior works [1], [2], [3]. In these works, we proposed improved cryptographic methods for searching and computation over encrypted data. Our contribution in today's paper is to present an improved version and a significant application of our noise-free fully homomorphic encryption scheme to biometric databases. We will begin by a deep classification of physiological traits. Why physiological traits? Most of security systems based on biometrics are using physiological ones. Behavioural biometrics are rarely used in comparison to physiological biometrics. The well-known spread biometrics are fingerprint, face and retina recognitions. They are, all, physiological biometrics.

Actually, unlike existing systems, our framework allows to store encrypted biometrics in database and use it without decryption. It is relied on the main following properties. Computing with ciphertexts: data issued from a fully homomorphic encryption algorithm could be treated as it is in clear. In fact, we can evaluate any function on it and especial comparison of encrypted data which is the desired operation in biometric systems. Cloud computing outsourcing: This property could be exploited to outsource biometric databases to cloud computing and benefit from its unlimited storage and computation capacities.

1.3. Related work

Several efforts have been put into improving biometric databases privacy. The usage of homomorphic encryption technology has already been introduced by Bringer et al [4]. In this article the authors propose to exploit the homomorphic property of GM encryption scheme [5] for secure biometric-based authentication. Their protocol allows to hide, from an adversary, the user that is trying to authenticate himself in the system.

Yasuda et al [6] suggest to compute the Hamming distance on encrypted data using a somewhat homomorphic encryption scheme based on ideal lattices. This Hamming distance is used to compare two biometric feature vectors. In addition, Drozdowski et al [7] address to subject of privacy of facial recognition databases by using homomorphic encryption. The authors propose an architecture of a biometric identification system in the encrypted domain, as well as providing an implementation using some existing homomorphic encryption schemes.

Recently, Catak et al [8] propose a biometric authentication system based on hash expansion and fully homomorphic encryption features. Authors solved the runtime complexity of FHE schemes by parallelization of the matching algorithm and provided a proof of concept implementation of their system with fingerprint biometrics.

The drawback of homomorphic encryption schemes is its overhead and runtime complexities. In fact, currently known FHE schemes consume a lot of time and memory space to perform operations on encrypted data. In this paper, we address this problem by using a promising category of FHE schemes. We will use noise-free FHE [1].

1.4. Organization

The rest of this paper is organized as follows: Section 2 proposes a classification physiological biometrics. Section 3 introduces some security issues related to biometric technologies. It presents some notions of security in relation with biometric identification and authentication, then it explains how biometric technologies work and it ends by an extensive review of security attacks related to biometric systems. Therefore, we provide a new framework for biometric database's privacy in section 4, while section 5 concludes the paper.

2. Classification of Physiological Biometrics: Analysis and Evaluation

Over the past several years, an increasing number of biometric technologies have been proposed. In modern approach, biometric characteristics can be classified in two main categories: physiological and behavioural traits. Biometric technologies for identification and authentication have been developed based on these characteristics.

Physiological traits (called also passive traits) are related to enduring or fixed human characteristics, such as fingerprints, fingers, hands, ears, shape and geometry of face, the pattern of veins, irises, retina, teeth, as well as samples of DNA. Physiological traits are generally available on every person and are permanent and distinctive, except if genetic defects, aging, illnesses or accidents, have modified or broken them.

Behavioural traits (called also active traits) are derived from human characteristics represented by skills, actions or functions performed by an individual. These include voice, gait, key-stroke and signature dynamics. It is important to note that the time dimension is incorporated as an essential metric of a behavioural biometric. Indeed, the measured behaviour has a starting, middling, and ending time.

It should be recalled that the behavioural/physiological distinction is somewhat artificial. Behavioural biometric technologies are related in part on physiology, such as the dexterity of hands and fingers (signature dynamics) or the shape of the vocal cords (voice). Physiological biometrics are similarly acquainted by user behaviour, such as the way in which a user looks at a camera or presents a finger. Nevertheless, the behavioural/physiological distinction is a useful tool in comprehension of how biometrics work and how they can be put in an application for the real world.

2.1. Physiological traits

Physiological biometrics are derived from a direct measurement of a part or a feature of human body that we were born with. They mainly are determined by our genetics. Fingerprints authentication systems are the oldest systems; it has been used for more than 100 years. Other examples are hand geometry, iris image, retina, face, odour, ear, vascular pattern, DNA, and many other distinguished features of human body that can be collected, recorded and measured through an automatic process.

2.1.1. Biometrics from Butt

Butt recognition: In 2011, Engineers from the Advanced Institute of Industrial Technology in Tokyo have developed a novel biometric that can recognize a person by the backside when he takes a seat [9]. It is possible to identify a person by the unique shape of his butt. They developed a system that can perform a precise measurement of the person's posterior, its contours and the way the person applies pressure on the seat. It is an automotive anti-theft system. For which the driver's seat is fitted with 360 sensors that record pressure in accordance with a scale of zero to 256. Then, a topographic map of the driver's ass is created to be used as a personal identifier [9].

2.1.2. Biometrics from Dental

Dental recognition: It is possible to use information about dental structures, in an automatic way, to identify or verify human remains [10]. This is the dental biometric that is mainly applied to identify victims of massive disasters from their bitemarks [11]. The process of dental identification consists of three main steps: measuring dental features, labelling individual teeth with tooth indices and matching of dental features. The majority of dental features is obtained from dental radiographs. Commonly used dental features are related to tooth morphology (shape) and appearance (grey level). Dental information includes the number of teeth, tooth orientation, shape of dental restorations, etc. This information is recorded in symbolic strings (dental codes) describing types and positions of dental restorations, number of cusps in teeth, presence or absence of each tooth, etc.

2.1.3. Biometrics from ear

Ear Geometry: Ear shape recognition is a biometric field in full development. It is related to the particular geometry of each individual's ears and the form of the ear lope and the projecting portion of the outer ear. There are at least three methods for ear shape recognition: taking a photo of the ear, taking "earmarks" by pressing ear against a materiel and taking thermogram pictures of the ear [12]. Ear biometric seems to be very interesting especially in crime investigation. In fact, earprints could be left by criminals listening at doors and windows, collected by police and law enforcement agents and analysed by specialists to recognise criminals.

Ear canal feedback: Otoacoustic Emissions (OAE) [13] are a sound wave generated from within the inner ear (cochlea of the ear). OAE are known to reveal considerable differences making it unique and a potential biometric from ear. Indeed, each one of us has its personal emission frequencies and significance differences in the occurrence of spontaneous otoacoustic emissions were found between genders [14] and between ethnics [15]. OAE can be classified into three main types [16]: (a) **Spontaneous Otoacoustic Emissions** (SOAE). A spontaneous otoacoustic emission is a pure tone at a stable frequency that is continually emitted from the ear without external stimulation and are measurable with sensitive microphones in the external ear canal. (b) **Transient Evoked Otoacoustic Emissions** (TEOAE) [17]. TEOAE are characteristically stimulated with a white noise pulse of approximately 80dB SPL (peak) with a brief duration of 2ms (toneburst). (c) **Distortion Product Otoacoustic Emissions** (DPOAE). These are evoked by applying a pair of continuous sine waves at similar frequencies. Of the three types aforementioned the least suitable is the SOAE. DPOAE and TEOAE are more appropriate for biometric uses [13] [17] [18] as they are stronger responses compared to SOAE.

2.1.4. Biometrics from Eye

Iris recognition: Iris recognition technology is based on the obviously coloured ring encircling the pupil of the eye. Its nature, as an elastic connective tissue, makes it suitable for biometric applications. It has about 266 distinctive and stable characteristics, 173 of it are exploited by iris recognition technologies. These contain the trabecular meshwork, striations, furrows, rings, a corona, and freckle. Iris recognition systems involve a small camera, with high-quality resolution, to capture a black and white image of the iris [19]. The system applies mathematical pattern-recognition techniques to those images. Iris recognition is useful in both verification and identification systems.

Retina recognition: Retina recognition technology maps and analyses the unique patterns of blood vessels on the thin nerve of the posterior portion of the eye [20] [21]. Every eye has its own totally unique pattern of blood vessels; even the eyes of identical twins do not share a similar pattern. Although each pattern normally remains unchanged over a person's lifetime, they can be altered in cases of disease such as glaucoma, high blood pressure, diabetes and autoimmune deficiency syndrome. Retinal scan is more difficult because of the retina complex structure. This involves projecting an unnoticed low-energy infrared light beam into the eye of a person looking through the scanner's eyepiece. This beam of light traces a normalized path on the retina. The amount of light reflection varies during the scan, because retinal blood vessels are more absorbent of this light than the rest of the eye. The pattern of variations is encoded and stored in a database. Enrolment can simply take more than a minute.

Other biometrics from eye exist like periocular recognition [22], [23], [24] [21] and sclera recognition [25].

2.2. A classification of physiological traits

In the table below (table 1), we show how to classify physiological biometrics depending to our body parts. The key elements of the table are:

Table 1. Classification and properties of physiological biometrics

Classification of the Various Types of physiological Biometrics		Characteristics							Properties of physiological biometrics			
		Universality	**Uniqueness**	**Performance**	**Collectability**	**Acceptability**	**Circumvention**	**Cost**	**Enrolment time**	**Verification time**	**Identification**	**Required hardware**
Butt		H	L	M	M	M	M	M	min	min	Y	Chair sensor
Dental		M	M	M	M	M	M	L	min	min	Y	Dental radiograph
Ear	Ear geometry	H	M	M	L	L	H	L	min	s	Y	Camera
	Ear canal feedback	H	H	M	M	L	L	L	min	s	Y	Microphone
Eye	Iris recognition	H	H	H	L	M	L	M	min	s	Y	Scanner
	Periocular recognition	H	M	M	H	H	M	L	min	s	Y	Camera
	Retina recognition	H	H	H	L	L	H	M	min	s	Y	Scanner
	Sclera recognition	H	M	M	L	L	M	M	min	s	Y	Scanner
Face	Face recognition	H	M	M	H	M	M	L	min	s	Y	Camera
Finger & knuckles	Finger-knuckle print	M	H	H	M	H	M	M	min	s	Y	Scanner
	fingerprint	M	H	H	M	H	M	M	min	s	Y	Scanner
	3D finger recognition	M	H	H	M	H	L	M	min	s	Y	3Dlive scanner
Foots		M	H	M	H	M	H	L	min	s	Y	pressure sensor mat, CCD camera
Hand		M	L	L	H	H	M	L	min	min	N	optical camera and diodes with mirrors
Hair recognition		M	L	L	M	H	H	M	min	min	Y	camera
Knee recognition		H	M	M	L	M	M	H	min	min	Y	MRI device
Lips	print	H	H	M	M	M	M	L	min	s	Y	piece of paper or cellophane, finger printer
	shape	H	L	L	M	M	H	L	min	s	N	camera

Nail	Nailbed	M	H	M	H	H	L	L	min	s	N	Digital camera
	Nail RFID	M	H	H	H	L	L	L	min	s	Y	RFID ship
Nose	Geometry	H	M	M	H	H	H	L	min	s	N	camera
	Pores	H	M	H	M	M	M	L	min	s	Y	camera
Odour		H	H	M	M	M	M	H	min	min	Y	ENose
Palm		M	H	M	M	H	M	M	min	s	Y	Palmprint Scanner
Pores		H	M	L	L	M	M	H	min	s	N	Microscope, Scanner
Skin	Skin spectroscopy	H	H	H	L	L	L	L	min	s	N	LEDs and photodiodes
	Skin impedance	H	M	M	L	L	M	L	min	s	N	Metallic electrodes
Tongue		H	H	H	M	M	L	M	min	s	Y	Camera
Vein		H	M	L	M	M	L	M	min	s	N	Scanner
Voice		M	M	M	H	H	H	L	s	s	Y	Microphone

Biometric characteristics: H (**H**igh), **M** (**M**edium) and **L** (**L**ow),
Biometric properties: min (**min**ute), **s** (**s**econd), **Y** (**Y**ear) and **N** (**N**on applicable).

The table above describes physiological traits. This category of biometrics is evaluated based on the characteristics below:

- **Universality**: Each individual should have the biometric trait.
- **Uniqueness**: (called also Unicity or Distinctiveness) Any two individuals should be different regarding the trait.
- **Performance**: Depends on the efficiency and accuracy of the extraction and matching of the biometric.
- **Permanence**: The biometric should be sufficiently constant over a certain period of time.
- **Collectability**: The biometric should be quantitatively measurable.
- **Circumvention**: Is the ease at which a trait might be limited using an artefact or substitute
- **Acceptability**: The capturing of a biometric should be possible in a way acceptable to a large percentage of the population.

The comparative table includes four distinctive properties. In addition to a required hardware which is the sensor component, each biometric is differentiated by its enrolment and verification times. These two times are measured by seconds and minutes, as long as they are small, the underlying biometrics are assumed to be better. A fourth property is related to identification ability. The identification column informs us if the underlying trait could be used for identification or not. We can identify in the comparative table that some physiological traits are not applicable to an identification process, like pores, skin and vein biometrics.

It is clear that none of the human biometric traits meets all the above characteristics and properties. Although each biometric trait has its pros and cons; as consequence there is no optimal biometric.

3. Functioning of Biometrics and Security Issues

Biometric technologies could be used for personal identification as it could be used for verification (or authentication) purposes, depending on the application. It measures and analyses physiological and behavioural characteristics of humans. Identifying a physiological characteristic of a person is based on taking direct measurement of a part of his body, such as fingertips and facial geometry, the corresponding biometric technologies are fingerprint recognition and facial recognition. Identifying behavioural characteristics of a person is based on data extracted from his behaviours, such as voice and signature, the corresponding biometrics being voice recognition and signature recognition [26], [27]. Effectiveness of biometrics as personal identifiers is related to the fact that the measured characteristics are thought to be distinct from an individual to another. Because they are closely related to an individual, they cannot be forgotten, are more reliable, and are less readily guessed, stolen, or lost.

Biometric systems manipulate sensitive data to grant authorization access to services. Those data are generally stored in a biometric database. Given the importance of this data, it is always sought after by hackers. Any breach or data leakage can lead to dangerous consequences, as it can jeopardize the security established by the said biometric system.

In this section, we discuss a few basics of biometric system's functioning and security issues, then we introduce several, well-known, related attacks to those systems.

3.1. Notions of Security: Identification, Authentication and Authorization

When we are authorizing access to a system, two initial phases are required: identification and authentication. These terms are often confused or used synonymously by many security domain specialists, but they are in fact all distinct concepts, and should be thought of as such. Identification is what happens when you claim to have a given identity in the system, while authentication is what happens when the system establishes that you are who you claim to be. In theory, authentication process is taking place after identification process but in practice both processes are usually used in tandem. In fact, the authentication step comes, after that the system user claims a certain identity (for example providing his username to the system), to verify the claimed identity (the user should provide a shared password between him and the system). However, in the majority of cases, the **authorization** process must necessarily take place, at least, after the identification process.

Identification: Identification is nothing more than responding, in some way, to the question "**who are you?**". After providing your response to this question we say that you are claiming you are somebody. You identify yourself when you meet someone you don't know, and he asks you "who are you?". When you say, "I'm Mister Smith.", you've just identified yourself. In relation with information security, this is analogous to typing a username during the login process to a system. Sometimes, identification process is not necessary to some systems for which one can gain access to your account just with the correct code without identifying himself (such as ATM cards).

Authentication: Authentication is the process by which a system cloud validates a provided identity. It is also how one proves that he is who he claimed to be. When you type your username into the username field, it's most likely that you are going to enter also a password to prove that you are really that user. The use of a password in this step is based on "something you know", i.e. a secret between you and the system. Authentication factors could be categorised into three principal sets:

(i) Something only the user knows (Knowledge), e.g. static password, code, personal identification number;

(ii) Something only the user possesses (Ownership), e.g. driver's license, token, smart card, mobile phone;

(iii) Something the user is (Inherence), e.g. biometric characteristic, such as a fingerprint, a retina scan.

After being successfully authenticated, we have now done two things: we have claimed to be a certain identity then we have proven that we are effectively that identity. The only remaining thing is for the system to determine what we are permitted to do. This is what will be the objective of our next step.

Authorization: Generally, authorization is a process that taking place after a person has been both identified and authenticated; it's the step that determines what a person can do on the system. It allows to protect computer resources by only permitting those resources to be consumed or used by resource consumers or users that have been granted authorization to consume or to use them. If everybody logs on using the same account we can grant access to resources for everybody, or block access to resources for everybody. If everybody uses the same account, we can't make distinction between users. However, when users have been authenticated with different user accounts, they can be granted access to different resources based on their identities.

3.2. How Biometric Technologies Work

Between biometric technologies we can identify various differences in relation with its capabilities, complexity and performances, but all share several elements. Biometric identification systems are basically pattern recognition systems. They involve acquisition and scanning devices (sensors) such as cameras and scanners to capture images, prints, recordings, or measurements of a person's characteristics, and use computer software and hardware to extract (Extractor), sample, encode, transmit, store (in a Database), and compare these characteristics (Matcher). Biometric decision making (Decisor) is becoming faster thanks to automation, generally it is taking only some few seconds in real time. Despite the fact that biometric technologies gauge various characteristics in ultimately different manners, all biometric systems use analogous processes that can be articulated into two different phases: enrolment and identification or verification.

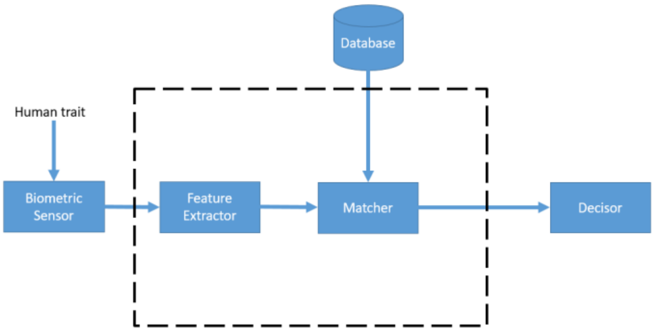

Figure 1. Typical biometric system architecture

3.2.1. *Enrolment process*

In this phase you are using the biometric system the first time. During the enrolment, biometric data from an individual is collected and stored, somewhere, as a reference template for future confrontations. The generation of a template is also influenced by slight changes in environment, pressure, positioning, distance and other factors. The quality of the template is crucial in the overall success of the biometric application. Sometimes, biometric features can change over time and people may experience problems with a biometric system, for that reason they may have to update their reference template by a re-enrolment. Enrolment takes place in 1:1 systems (verification systems) and in 1:N systems (identification systems).

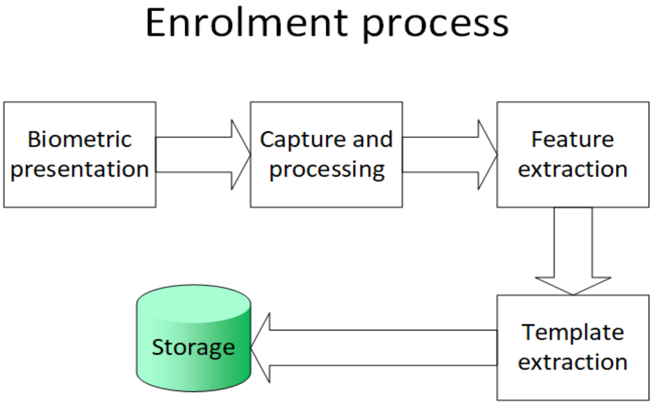

Figure 2. The biometric Enrolment process

3.2.2. *Verification process*

Concerning verification systems, the phase after enrolment is verification of a claimed identity. After the person provides the biometric identifier he or she was enrolled with, it is presented to the biometric system which captures it and generates a trial template that depends to the vendor's algorithm. The system then confronts the trial biometric template with the initially registered template of the same person, which was stored in the system during enrolment, to conclude whether the template subject to trial and the stored one match. Verification process is qualified as a one-to-one database's relation. As a consequence of the verification phase, the system will end up by a decision of match/no-match. In actual systems, this decision is obtained in less than a second. In real life, a system used by a company to authenticate their employees after providing their identities to grant access to a professional computer is a verification application of biometrics.

3.2.3. Identification process

Concerning identification systems, the phase after enrolment is to identify who the person is. Contrary to verification systems, no identifier is required. To find a match, instead of locating and comparing the person's reference template against his or her presented biometric, the trial biometric template is confronted to the initially stored templates of all persons enrolled in the system. Identification process is quailed as one-to-many database's relation. According to the decision made by the identification systems (match or no-match), we can classify these systems into two categories: positive and negative. In positive identification systems, the expected decision is "match". In fact, these systems are designed to ensure that a person's biometric information is already registered in the database. Controlling access to a secure building by checking anyone who seeks access against a database of enrolled employees could be considered as a positive identification system. In negative identification systems, the expected decision is "no-match". Indeed, these systems are designed to ensure that an individual's biometric is not enrolled in the database. A typical negative identification system allows to compare an individual's biometric against all enrolled ones in a database of all who are registered in a public benefits program to guarantee that this individual is not "double-dipping" by using fake documentations to register under manifold identities.

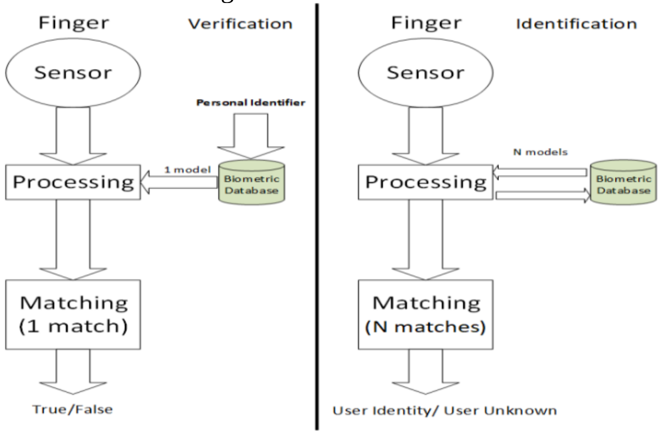

Figure 3. The biometric Verification and identification processes

3.3. Security issues for biometric databases

With the emergence of new information technologies, security concerns have becoming a challenging problem where there is sensitive data to process. Significantly, they play a critical issue for biometric data and applications. Biometric databases contain citizen's fingerprints, photos, signature templates and many other identification and verification traits used by biometric systems to automatically recognize people due to several intrinsic advantages they offer over typical procedures. Biometrics-based systems are widely used in many applications starting from criminal investigation to civilian registration, national identity document verification, border control, e-banking, e-commerce, on-line payment, physical and logical access control. Those biometric data can easily be copied without information loss, manipulated at will or forged without noticeable traces, and used to spoof original identities and bypass access control's systems. For those reasons, it is unacceptable for biometric databases to be lost, copied, stolen or forged. Otherwise, recognition systems founded on personal traits, either biological or behavioural will be questioned.

Several challenges related to personal data protection are raised by biometric-based recognition. Generally, those challenges are not posed by traditional recognition methods if compromised. For example, in contrary to PIN or password credentials which could be changed or reissued if needed, biometrics are fixe and unchangeable if they are stolen or captured. As a consequence, additional privacy concerns are behind the use, processing and storage of person's behavioural or physiological traits. In other words, more attention should have given to protect biometric databases in any information system in order to avoid consequent risks to individual's biometric data leakage.

3.4. Security attacks related to biometric systems

Biometric systems could be a subject of several attacks from the sensor stage to decision step. Consequently, the security established by biometric systems could itself be questioned. Researchers have studied these security concerns and analysed the probability of such breaches and vulnerabilities to counter the normal functioning of a biometric system [28], [29]. Security specialists have determined the potential points, of a biometric system, in which an intruder can drive an adversarial attack. Some of these security attacks are common to any information system, while the attacks using template modification and fake biometric are unique to biometric systems.

In this section we present a global review of security attacks to biometric systems in each step of the provided architecture in figure 1. We promptly talk over the characteristics of such attacks, which need to be successfully balked in biometric systems.

3.4.1. Sensor attacks

Biometric sensors could be a target of multiple attacks. From one hand, artificial fake biometric traits are presented to the sensor in order to bypass the recognition phase. This attack could have a second form, when a legitimate biometric is presented to sensor in an unauthorized manner. We call it coercitive attack: forcing a legitimate user to grant access to the system by an imposter. From the other hand, flooding the sensor with bogus access requests can cause a denial of service. Generally, the sensor is not able to differentiate between real and fake traits as it is unqualified to distinguish legitimate requests from denial of service flood. We can find in the literature: coercitive attacks, spoofing attacks, mimicry attacks, device substitution attacks and DoS attacks [28], [29].

3.4.2. Feature extractor attacks

The feature extraction is an automated process that enables the generation of a template from a biometric sample after locating and encoding its distinctive characteristics. This process may include divers degrees of image or sample processing with the aim of locating enough amount of precise data.

Falsification of biometric feature extractors include inserting of fraudulent data and replacing components to fabricate permitted features [29]. A second category of extractor attacks consists of introducing a Trojan program which generates the wanted feature set [28].

3.4.3. *Matcher attacks*

Matchers are the interface between the database and the feature extractor module. Its role is to compare the input sample with the stored template in the database. The high matching score is retained and transmitted to Decisor module to take an authorization decision to grant access to system.

Attacks on matchers turn around producing a matching score that will be accepted by the Decisor. Attacker has several ways to attain this objective. Firstly, he can capture and change the score value before arriving to Decisor module [30]. A second type of attacks includes substituting a horse Trojan program or hardware component to control the matcher behaviour [31], the Trojan is employed by the attacker to harvest users' traits extracted features and transmit it to him.

3.4.4. *Decisor attacks*

The decision step is the last one in a biometric authentication process. This operation is assured by a decision module called Decisor. The user is granted access to system or rejected on the basis of the security threshold already predefined. The degree of similarity is indicated by a score which is generated by a matching algorithm. Decisors compare the score with the threshold, the result is match (grant access), non-match (limit access) or inconclusive (prompt the user and ask for another tentative).

This biometric module can be a subject of various attacks; among them we find Trojan attack which is also present in this step. It constitutes a non-biometric module in the overall system used by attackers to introduce some security flaws. Manipulation of the score and the decision is a second class of Decisor attacks. The objective of manipulation is to capture and modify score and decision values [31].

3.4.5. *Communication channels attacks*

Between each two components of the biometric system we find a communication channel. Totally, we have four communication channels in our architecture: sensor-extractor channel, extractor-matcher channel, matcher-decisor channel and matcher-database channel. Channels are targeted by security attacks and adversaries [29].

At each one of the aforementioned channels, we can identify various threats and vulnerabilities. The attacker's goal is to intercept transferred data and grant access to the secured system. Eavesdropping is the most significant attack at any communication channel, it is a passive attack. In this scenario, the eavesdropper listens the channel and collects sensitive data for fraudulent use. A similar attack is called man-in-the-middle attack, in this scenario the enemy has the ability to intercept, modify and retransmit the compromised template between two parties without their knowledge.

3.4.6. *Database attacks*

Biometric databases are the highly sensible components of any biometric authentication based system. A database stores biometric templates and it is requested at any authentication or identification process. At this system node, the adversary tries to read existing templates, attempts to add new ones and makes an effort to modify or remove one or more existing templates [31]. If data are stored in clear, the reading of templates becomes a very simple task for the adversary. If an adversary is capable to read templates from database, he can steal the database or at least create matching artefacts (this type of attack is called masquerade). Adding, modifying or removing templates are three kinds of a, so called, tampering attack. Tempering attacks affect the authenticity of the system. Masquerade and tampering attacks pose a significant threat to remote authentication.

We can summary the aforementioned attacks in the table 2.

Table 2. ordinary attacks to a biometric system

System component	***Possible attacks***
Sensor	Coercitive attack, spoofing, device substitution, DoS
Extractor	Trojan, insertion of fraudulent data
Matcher	Trojan, insertion of fraudulent data, guessing attack, manipulation of score
Decisor	Trojan, manipulation of score and decision attack, manipulation of threshold
Channels	Eavesdropping, man in the middle, reply attack, brute force, manipulation of score and decision attack
Database	Masquerade, tampering, reading template

4. Proposed Framework for Biometric Database's Privacy

4.1. Fully Homomorphic Encryption (FHE)

Homomorphic ciphers constitute a basic cryptographic brick in many protocols and applications requiring the anonymity of the user or the confidentiality of his data. They are very useful in a context of cloud computing and outsourcing of calculations on sensitive data.

Indeed, by transporting an operation from the domain of ciphers to the domain of clear messages, these ciphers allow a third party to perform blind operations on encrypted data for the benefit of the user who is the sole owner of the private key. The operations are performed directly on the cryptograms giving the same result as if they are performed on the clear data, the only difference is that in the case of homomorphic encryption the result is obtained in encrypted form and it is the end user possessing the private key which is the only one capable of decrypting and discovering the content.

A fully homomorphic encryption scheme allows performing any type of computations over encrypted data. It was, early, conjectured by Rivest et al [32] in 1978. After about three decades, exactly in 2009, Craig Gentry [33] presented the first conception of a semantically secure fully homomorphic encryption scheme. His holy grail work is based on ideal lattices. Gentry's conception can be summarized into three main stages:

- **SomeWhat Homomorphic Encryption Scheme** (SWHE): Gentry starts with a so-called SWHE that supports a limited number of homomorphic multiplication.
- **Squashing the decryption circuit**: Gentry reduces the complexity of the decryption circuit by publishing a set of vectors whose sum of a part of them is equal to the

secret key. This so-called "squash" scheme can evaluate, in addition to its SWHE capacities, a NAND gate.

- **Bootstrapping**: the bootstrapping procedure consists of evaluating the decryption circuit plus the NAND gate to obtain a "leveled" FHE scheme which allows any circuit to be evaluated with a depth of the circuit defined at the start

This first scheme is noise-based, i.e. a noise part is added to cleartexts in order to obtain the homomorphic properties. Most of the work that followed later has inspired from Gentry's framework to design FHE cryptosystems [34], [35], [36], [37], [38], [39],… other ideas and frameworks appeared later [40], [41], [42], [1], [2]… Among the most prominent attempts to simplify homomorphic encryption schemes is the cryptosystem MORE [41]. This latter was the subject of the patent WO2014016795A2. It is a symmetric cryptosystem based on modular arithmetic whose homomorphy results from usual matrix operations, its multiplication and addition are matrix multiplication and addition.

A fully homomorphic cryptosystem is defined, in general, as a quadruple of algorithms (Gen, Enc, Dec, Eval), running in polynomial time, such as:

- $Gen(\lambda)$: is a key generation algorithm, takes as input a security parameter λ and outputs a pair of keys (sk, pk).
- $Enc(m, pk)$: is an encryption algorithm, takes as input a clear message m and a so-called public key pk and outputs a cryptogram c.
- $Dec(c, sk)$: is a decryption algorithm, takes as input a cryptogram c and a so-called secret key sk and outputs the clear message.
- $Eval(C, c_1, .., c_n)$: is an evaluation algorithm, which takes as input a circuit C and cryptograms $c_1, .., c_n$ and verifies $Dec(Eval(C, c_1, .., c_n), sk) = C(m_1, \dots, m_n)$.

The main reason for the interest in a homomorphic cryptosystem is its wide scope of applications. Indeed, for a long time there have been many applications which required an encryption scheme which could do the calculation on the encrypted data. But with the growing interest and the emergence of the cloud, new areas of application have emerged. In [43], the authors classified the applications of homomorphic encryption into three broad main categories based on whether one expects the confidentiality of the data, of the circuit (function of the computation) or both. These three categories are:

- **Private data, public functions**: as for applications in the medical field or biometrics.
- **Private data, private functions**: as for applications in the financial sector.
- **Applications in the field of prices and advertising** where just the results are public.

We notice that all of these apps assume that we had a single data owner who encrypts the content and stores it in an unsecured database. Among the advantages of homomorphic encryption is its ability to perform computations over encrypted data. This property becomes very important when we have confidential data encrypted and hosted by a third party somewhere in the world (cloud computing). The cloud allows its customers to benefit from its computing power without losing the confidentiality of their data[44].

4.2. Our Improved Noise-Free FHE

As it is already defined in [1], we presented a noise-free fully homomorphic encryption scheme quaternion and IND-CPA secure. In this part we provide an improved version of our scheme. The new scheme will support encryption of bits, instead of encryption of numbers of the provided scheme, which is hilly recommended for in a context of encrypting biometric data. The current scheme was already patented by OMPIC (Office marocain de la propriété industrielle et commerciale) under the number MA 39511 B1. The new scheme could be summarized as follows:

Homomorphic transform:

The provided cryptosystem is based on a homomorphic transform, ***BitToQuatern***, between $(\mathbb{Z}/2\mathbb{Z}, \boldsymbol{XOR}, \boldsymbol{AND})$ and $(\mathbb{H}(\mathbb{Z}), +, \times)$**.** Its inverse transform, ***QuaternToBit***, allows to find a bit from a quaternion. As it is defined in [1], we can schematize it in the diagram below:

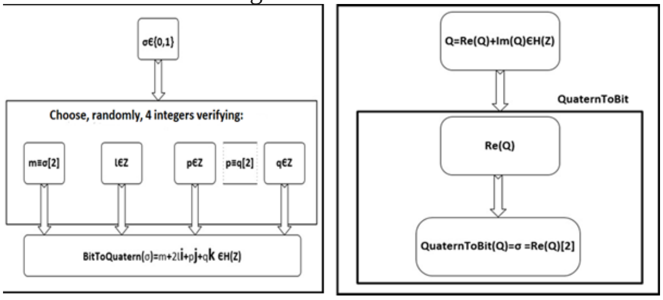
σ∈{0,1}
Choose, randomly, 4 integers verifying:
m≡σ[2]
l∈Z
p∈Z
p≡q[2]
q∈Z
BitToQuatern(σ)=m+2li+pj+qk ∈H(Z)
Q=Re(Q)+Im(Q)∈H(Z)
QuaternToBit
Re(Q)
QuaternToBit(Q)=σ =Re(Q)[2]

Figure 4. Homomorphic transform, BitToQuatern, and its inverse transform, QuaternToBit, diagrams.

Key Generation:

- Generate randomly two big prime numbers p and q.
- Then, calculate N = 2.p.q.
- Generate randomly an invertible matrix $K = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$.
- Calculate the inverse of K, Which will be denoted K^{-1}.
- The secret key is (K, K^{-1}).

Encryption:

Lets $\sigma \in \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ be a clear text. To encrypt σ we proceed as follows:

- Using the transform BitToQuatern, we transform σ into a quaternion: $m = bitToQuatern(\sigma) \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$**.**
- Generate a matrix $M = \begin{pmatrix} m & r_3 & r_4 \\ 0 & r_1 & r_5 \\ 0 & 0 & r_2 \end{pmatrix} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$ such that $r_i \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})\ \forall \boldsymbol{i} \in [\![\boldsymbol{1}, \boldsymbol{5}]\!]$ are randomly generated and $|r_1| \equiv 0[2]$.
- The cipher text of σ is $C = Enc(\sigma) = KMK^{-1} \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$.

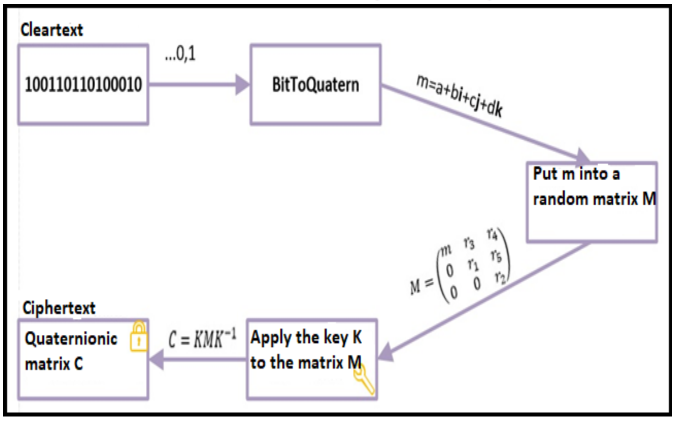

Figure 5. Encryption process for our fully homomorphic cryptosystem

Decryption:

Lets $C \in \mathbb{M}_3(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$. be a ciphertext. To decrypt C, we proceed as follows:

- Compute $M = K^{-1}CK$ using the secret key.
- Then, take the first input of the resulting matrix $m = (M)_{1,1}$.
- Finally, recover the clear message by calculating $\sigma = quaternToBit(m)$.

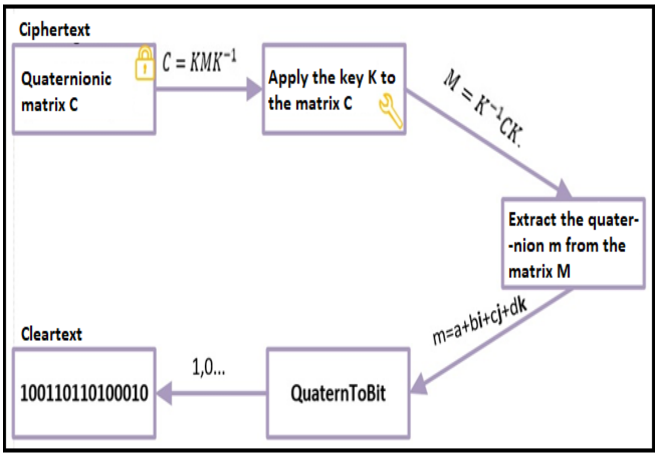

Figure 6. Decryption process for our fully homomorphic cryptosystem

Addition and multiplication:

We can, simply, verify the homomorphy of our cryptosystem as follows:

- Addition: $C_{add} = C_1 + C_2 = Enc(\sigma_1) + Enc(\sigma_2) = Enc(\sigma_1 \oplus \sigma_2)$.
- Multiplication: $C_{mult} = C_1 . C_2 = Enc(\sigma_1) . Enc(\sigma_2) = Enc(\sigma_1 \otimes \sigma_2)$.

Implementation results

We provide an implementation of our encryption system with fully homomorphic capabilities, i.e. we implement key generation, encryption, decryption, addition and multiplication operations.

Table 3. implementation results of our improved noise-free FHE

Security parameter (bit)	runtime (ms)					Overhead (Kbit)	
	Key generation	Encryption	Decryption	Addition	Multipli-cation	Secret key	Ciphertexts
256	29	4	<<1	<<1	<<1	18	9
512	74	12	<<1	<<1	<<1	36	18
1024	312	54	1	1	1	72	36
2048	2356	405	4	4	7	144	72
4096	28500	4960	10	10	18	288	144

The tests are performed using a Virtual Machine with the following characteristics: 2vCPU running at 2.40 GHz, with 256 KB L2 cache and 7 GB of RAM memory. This implementation is based on the JAVA programming language using the Eclipse IDE platform. The table 3 shows the obtained results:

The fundamental results of our tests are summarized in the table above. These results correspond to the different sizes of the security parameter n used to generate the secret key. In this table, we have summarized the fundamental operations of our fully homomorphic cryptosystem.

On the one hand, we observed that although the encryption and decryption algorithms have almost the same mathematical formulations, the execution time of the encryption is significantly higher than that of the decryption. This excessive difference between the two operations is due to the bitToQuatern transformation used during encryption, we confirm that the majority of the encryption time is spent transforming a σ∈ {0,1} bit into a Lipschitz quaternion. Regarding the evaluation operations, we observed that the addition is always done in less than a millisecond while the multiplication is done in an optimal time. This is very reasonable considering the fact that matrix operations are simple. Therefore, these time complexities come in handy in a cloud computing context with unlimited computational capabilities.

On the other hand, we have noticed that the size of the secret key is of the order of a few kilobytes for a given security parameter n while the size of the cipher text constitutes approximately half the size of the secret key. This is because the secret key consists of two arrays, but the ciphertext consists of only one array. All ciphertext sizes are fixed due to the fact that we use a fully homomorphic, noise-free encryption scheme.

4.3. Digital comparator in the encrypted domain

A digital comparator is a logic circuit which performs the comparison between 2 numbers as input in binary form denoted A and B. It has 3 outputs denoted A = B, A> B and A <B which indicate the result of the comparison as follows:

- If the number A is equal to the number B (A = B), the output A = B goes to state 1 while the outputs A> B and A <B go to state 0.
- If the number A is strictly greater than the number B, only the output A> B goes to state 1.
- If the number A is strictly lower than the number B, only the output A <B goes to state 1.

In the encrypted domain, we can evaluate homomorphicaly the comparator circuit to compare two encrypted numbers A and B. The Boolean circuit, of the comparator, could be transformed to a multivariate polynomial. This polynomial will be applied to A and B. The obtained result is an encrypted bit, when decrypted it will meet one of the above three conditions.

Digital comparator is a basic operation in a biometric matching process. It allows to compare the matching score with the defined threshold.

4.4. Biometrics in the encrypted domain

We now arrived to the description of our proposed framework. As shown in the architecture below, two principal modules are added to the original system: a homomorphic encryption module and a homomorphic decryption module. The encrypted domain consists of the following components:

- ***A homomorphic encryption module***: is a software component, directly situated at the bottom of the feature extractor. It receives templates from feature extractor, transform it into bits and encrypt it homomorphicaly using our noise-free FHE. The result, encrypted templates, is stored in the database.
- ***A homomorphic decryption module***: is a software, directly connected to the homomorphic matcher. It receives an encrypted result, a quaternionic matrix, decrypts it and send the obtained result to the decisor.
- ***A homomorphic matcher***: is a software component implementing the evaluation algorithm of our proposed noise-free homomorphic encryption scheme. Among its intrinsic algorithms we find the sus-described comparator in the encrypted domain. Other algorithms are implemented in this component such as distance comparison and match finding. Its result is obtained in an encrypted form and it is communicated to the decryption module.
- ***An encrypted database***: database containing templates homomorphicaly encrypted. It is requested by the matcher component during an authentication process.

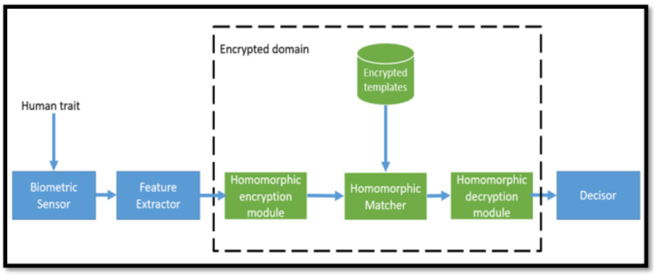

Figure 7. Schematic description of our framework for biometrics in the encrypted domain

5. Conclusion and future work

Recently, many researches have been conducted to improve biometric system's security. Biometric Databases are the most sensitive component in a biometric system given the private templates they store. However, biometric databases have still to face hard challenges related to templates privacy. In this paper, we have proposed a new framework for biometric databases security. Our framework leverages the applicability offered by homomorphic encryption and the performances, such as runtime execution and space complexity, provided by noise-free homomorphic schemes. We have presented a classification and evaluation of physiological biometrics. Moreover, we have provided a detailed study about security issues and attacks related to biometric systems. Afterwards, we have detailed our framework and provided a secure homomorphic model for biometric database privacy. An implementation of the homomorphic encryption and decryption modules is provided in this section.

In a future work, we propose to test our implementation on real biometric databases. Given the fact that homomorphic encryption schemes are, generally, designated to provide security in a cloud computing context, we propose to create biometric database in cloud computing provider. It will allow us to benefit from cloud capacities as storage and unlimited processing powers.

References

[1] A. EL-YAHYAOUI and M. ECH-CHRIF EL KETTANI, "An Efficient Fully Homomorphic Encryption Scheme," *International Journal of Network Security*, vol. 21, no. 1, pp. 91-99, 2019.

[2] A. EL-YAHYAOUI and M. ECH-CHERIF EL KETTANI, "A Verifiable Fully Homomorphic Encryption Scheme for Cloud Computing Security," *Technologies*, vol. 7, no. 1, p. 21, 2019.

[3] A. EL-YAHYOUI and M. ECH-CHERIF EL KETTANI, "Fully homomorphic encryption: Searching over encrypted cloud data," in *2nd international Conference on Big Data, Cloud and Applications*, Tetouan, Morocco, 2017.

[4] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang and S. Zimmer, "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication," in *The 12th Australasian Conference on Information Security and Privacy (ACISP '07)*, Townsville, Queensland, Australia, 2007.

[5] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," in *Fourteenth Annual ACM Symposium on Theory of Computing*, San Francisco, California, USA, 5-7 May 1982.

[6] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, "Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics," in *International Conference on Availability, Reliability, and Security*, Regensburg, Germany, 2013.

[7] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf and C. Busch, "On the Application of Homomorphic Encryption to Face Identification," in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2019.

[8] F. Catak, S. Yayilgan and M. Abomhara, "A Privacy-Preserving Fully Homomorphic Encryption and Parallel Computation Based Biometric Data Matching," *Preprints*, p. 16, 2020.

[9] N. Owano, "Engineers unleash car-seat identifier that reads your rear end," 25 12 2011. [Online]. Available: https://phys.org/news/2011-12-unleash-car-seat-rear.html. [Accessed 16 04 2019].

[10] S. Jadhav and R. Shriram, "DENTAL BIOMETRICS USED IN FORENSIC SCIENCE," *Journal of Engineering Research and Studies*, vol. 3, no. 1, 2012.

[11] Hofer and A. Marana, "Dental Biometrics: Human Identification Based On Dental Work Information," in *XX Brazilian Symposium on Computer Graphics and Image Processing*, Minas Gerais, Brazil, 2007.

[12] H.-K. Lammi, "Ear biometrics," Lappeenranta University of Technology, Lappeenranta, Finland, 2004.

[13] N. Grabham, M. Swabey, P. Chambers, M. Lutman, N. White and J. Chad, "An Evaluation of Otoacoustic Emissions as a Biometric," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 174 - 183, 2013.

[14] R. Bilger, M. Matthies, D. Hammel and M. Demorest, "Genetic implications of gender differences in the prevalence of spontaneous otoacoustic emissions," *J Speech Hear Res*, vol. 33, no. 3, pp. 418-432, 1990.

[15] M. Whitehead, N. Kamal, B. Lonsbury-Martin and G. Martin, "Spontaneous otoacoustic emissions in different racial

groups," *Scand Audiol,* vol. 22, no. 1, pp. 3-10, 1993.

[16] M. Swabey, S. Beeby, A. Brown and J. Chad, "Using Otoacoustic Emissions as a Biometric," in *International Conference on Biometric Authentication,* Hong Kong, China, 2004.

[17] M. Swabey, P. Chambers, M. Lutman, N. White, J. Chad, A. Brown and S. Beeby, "The biometric potential of transient otoacoustic emissions," *International Journal of Biometrics,* vol. 1, no. 3, pp. 349-364 , 2009.

[18] J. Gao, F. Agrafioti, S. Wang and D. Hatzinakos, "Transient Otoacoustic Emissions for biometric recognition," in *2012 IEEE International Conference on Acoustics, Speech and Signal Processing,* Kyoto, Japan, 2012.

[19] J. Daugman, "How Iris Recognition Works," *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY,* vol. 14, no. 1, pp. 21-30, 2004.

[20] C. Simon and I. Goldstein, "A New Scientific Method of Identification," *New York State Journal of Medicine,* vol. 35, no. 18, pp. 901-906, 1935.

[21] I. Nigam, M. Vatsa and R. Singh, "Ocular biometrics: A survey of modalities and fusion approaches," *Information Fusion,* vol. 26, pp. 1-35, 2015.

[22] M. Uzair, A. Mahmood, A. Mian and C. McDonald, "Periocular biometric recognition using image sets," in *2013 IEEE Workshop on Applications of Computer Vision (WACV),* Tampa, FL, USA, 2013.

[23] F. Alonso-Fernandeza and J. Bigun, "A Survey on Periocular Biometrics Research," *Pattern Recognition Letters,* vol. 85, no. 2, pp. 92-105, 2016.

[24] G. Santosa and E. Hoyle, "A fusion approach to unconstrained iris recognition," *Pattern Recognition Letters,* vol. 33, no. 18, pp. 984-990, 2012.

[25] Z. Zhou, E. Du, N. Thomas and E. Delp, "A New Human Identification Method: Sclera Recognition," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans,* vol. 42, no. 3, pp. 571 - 583, 2012.

[26] B. Gajic and K. Paliwal, "Robust speech recognition using features based on zero crossings with peak amplitudes," in *IEEE International Conference on Acoustics, Speech, and Signal Processing,,* 2003.

[27] N. Houmani, A. Mayoue, S. Garcia-Salicetti, B. Dorizzi, M. Khalil, M. Moustafa, H. Abbas, D. Muramatsu, B. Yanikoglu, A. Kholmatov, M. Martinez-Diaz, J. Fierrez, J. Ortega-Garcia, J. Roure Alcobé, J. Fabregas, M. Faundez-Zanuy, J. Pascual-Gaspar, V. Cardenoso-Payo and C. Vivaracho-Pascual, "BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures," *Pattern Recognition,* vol. 45, pp. 993-1003, 2012.

[28] N. Dahiya and C. Kant, "Biometrics Security Concerns," in *Second International Conference on Advanced Computing & Communication Technologies,* 2012.

[29] P. Campisi, "Security and Privacy in Biometrics: Towards a Holistic Approach," in *Security and Privacy in Biometrics,* London, Springer-Verlag , 2013, pp. 1-23.

[30] R. Jain and C. Kant, "Attacks on Biometric Systems: An Overview," *International Journal of Advances in Scientific Research,* vol. 1, no. 7, pp. 283-288, 2015.

[31] J. Mwema, M. Kimwele and S. Kimwele, "A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates," *International Journal of Computer Trends and Technology (IJCTT),* vol. 20, no. 1, pp. 12-18, 2015.

[32] R. Rivest, L. Adleman and M. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation,* vol. 4, no. 11, pp. 169-180, 1978.

[33] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *41st Annual ACM Symposium on Theory of Computing, (STOC 2009),* Bethesda, MD, USA, 2009.

[34] N. Smart and F. Vercautern, "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," Cryptology ePrint Archive, Report 2009/571, IACR, 2009.

[35] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," Cryptology ePrint Archive, Report 2009/616, 2009.

[36] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE," IACR, 2011.

[37] Z. Brakerski, "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP," IACR, 2012.

[38] C. Gentry, A. Sahai and B. Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based," IACR, 2013.

[39] I. Chillotti , N. Gama , M. Georgieva and M. Izabachène, "Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds," IACR, 2016.

[40] L. Xiao, O. Bastani and L. Yen, "An efficient homomorphic encryption protocol for multi-user systems," Cryptology ePrint Archive, Report 2012/193, 2012.

[41] A. Kipnis and E. Hibshoosh, "Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification," Cryptology ePrint Archive, Report 2012/637, 2012.

[42] J. Li and L. Wang, "Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings," Cryptology eprint report 2015/641, 2015.

[43] K. Lauter, M. Naehrig and V. Vaikuntanathan, "Can homomorphic encryption be practical?," Cryptology eprint report 405/2011, 2011.

[44] MR. Baharon, Q. Shi, MF. Abdollah, SM. Warusia, S.M.M Yassine and A. Idriss "An Improved Fully Homomorphic Encryption Scheme for Cloud Computing" International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10 N. 3, December 2018