A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks

Christina-Angeliki Toli, Bart Preneel
Department of Electrical Engineering ESAT/COSIC -KU Leuven & iMinds
Kasteelpark Arenberg 10, bus 2452, Leuven-Heverlee B-3001, Belgium

Abstract

The exponential growth of immigration crisis and the recent terrorism cases revealed the increase of fraud occurrences, cloning and identity theft with numerous social, economic and political consequences. The trustworthiness of biometrics during verification processes has been compromised by spoofing attackers sprang up to exploit the security gaps. Additionally, the cryptography's role in the area is highly important as it may promote fair assessment procedures and foster public trust by serving the demands for proportionality, reducing the concerns about national surveillance. Literature efforts are devoted to studying model threats and problems raised by targeted malicious actions for biometric techniques. However, attacks against multi-modal crypto-biometric systems have not received much attention. This paper presents cryptosystems, intrusions and countermeasures for single, multiple modalities and complicated schemes. Finally, a novel bimodal privacy friendly cryptosystem is suggested, able to reject such kind of attacks, presenting an anti-spoofing behavior under the cooperation between user and the function. The aim of this multidisciplinary work is to organize the current performances on how to develop security, contribute to research by designs able to address real-world use cases and pinpoint the potentiality for improvements.

1. Introduction

Until relatively recently, biometric enabled systems have replaced the traditional forms of individuals' recognition of his/her presence, access to facilities or log in to an account as their traits can be very discriminative yet less easily lost or stolen. Automated identity management, using face, hand or fingerprints, has become an experience in everyday life, mainly due to their diffusion in technologies such as electronic passports or IDs. From border control, to log on computers, mailing and eBanking services, biometrics constitute a unique and integral part of the user, to whom are associated with, and this is a serious tangible reason for being vulnerable to activities that threat to compromise not only reliability of the application, but also security and privacy rights of the person [11].

A closer look at the explanation for any extensive attack to fields related to biometrics will lead to the nature of the data, the personal non-biometric information that may be stored and correlated or other private facts such as the medical condition of the user that may be enclosed and revealed on occasions where someone's identity is not appropriately protected. In terms of spoofing, a non-colluding honest entity tries to fake somebody else's identity by presenting samples of that person's traits, or tries to gain benefit from the "leakage" of stored biometric information in a database or an electronic chip. Considering the special assumption when a biometric trait is compromised, then it cannot be canceled and renewed, hence moreover, it seems critical that may be used to create gelatin genetic clones of fingerprints, contact lens with a copy of iris or retinal scans, artificial replicas of faces, facial samples in the form of photographs, a video or a 3D mask. Voice or even gait can be recorded, inducing a system to falsely infer a presence under another's identity. A behavioral biometric such as signature, handwriting are not stolen, under the classical term, but can be easily mimicked and used to a certain degree for illegal means. These concerns have given space to public debates on the pressing matter of

confidence in authorized, biometry compulsive systems and therefore, societal, ethical themes.

As an address to the challenges of strengthened privacy for human characteristics, a range of standards and security methodologies have been suggested. Standard conventional cryptographic algorithms have been characterized, simply, as not enough, as a result of not allowing and supporting comparison between template and fresh sample caught on sensor, thus making the system possibly to be cheated. In this philosophy, biometric template protection schemes have been deployed. The paramount idea is the secured form of the stored template, making it unusable without authorization, but still capable for recognition its true energetic owner. The approaches try to follow the requirements of accuracy, irreversibility, diversity, unlinkability, revocability. At the direction of enhancing security, privacy information and overcome drawbacks in both areas, the combinations of biometrics with cryptography techniques were born [9]. Crypto-biometric systems or biometric cryptosystems, as they are denoted in this paper, respect the previously referred compulsions and additionally can obtain cryptographic/crypto-bio keys strongly linked to the user's identity.

Although crypto-biometrics propose alternative solutions, biometric recognition systems are still suffering and sometimes defeated by intruders. Vulnerabilities primarily include direct and indirect attacks performed at the sensor level, or correspondingly, inside the parts of the system, such as communication channels, storage domain, feature and matcher extractions. Direct operations happen when an attacker tries to masquerade as a valid and authorized user by changing his/her biometric characteristics, claiming a different identity posing himself/herself or presenting false traits. Surprisingly, multi-biometric systems, based on their sources, separated to multi -sensors, -recorded samples, -algorithmics, -units and -modals, are constitute a more difficult, but not impossible target. Ideally, several mechanisms have been tried for the defense of security for the involved items in a system, with controversial results. From a realistic point of research, academic and industrial trials on detection, encryption and anti-spoofing measures have been proposed to deal, in some extent, with these threats.

In addition to these, admittedly, there has never been a proposed model on how best biometrics applications can be secured, especially those ones that are related to governmental and organizational purposes [11]. The proposals for centralized database systems including information for national ID cards or passports bring about a feeling of discomfort, reinforcing the assertions wherein biometrics have seen intrinsically as privacy's foe. Conversely, keeping pace with technological changes, biometric schemes as a modern and sometimes mandatory key to validate transactions must also be given the capacity and the resources to deal with millions of expected requests, always respecting their primary objectives of data minimization, accuracy, transparency, confidentiality etc. Template protection models should prevent the re/generation of the original template from the initial, and the laws should strictly be followed to ensure their acceptance from citizens.

This study is motivated by recent advances in the scientific field of biometric system security, and protected templates to ensure the secrecy of person's identity. Its target is to present and add new information to the studies against fraud processes to biometric based verification technologies, something that since 2012 is indicated as well, from the increasing number of projects aim to suggest ideas for preventing risks, directly applicable to special issues, such as border control. Our essential objective here is to clarify the role of cryptology in biometrics, and examine how honest is the statement for a safe and reliable biometric application environment, when this is constantly exposed to human mind's contrivances. The remainder of the article is organized as follows: In the next two sections, a thorough summarized review on research articles is analyzed, particularly on the development of standard metrics, protocols and datasets for the appraisal of the progress, introducing readers to enlightenment. The fourth part is devoted to single and/or multi-biometric cryptosystems, spoofing attacks, and resistance processes. Fifth section aims to present the design of an innovative multi-modal model. It is a suggestion capable of being used in electronic passport applications based on liveness detection and RFID access control as combined mechanisms for reinforcement the cryptographic bearing against spoofing. The privacy standards and principals are also discussed, while a standard evaluation methodology which is needed to assess the influence of countermeasures on biometric system performance is indicated. As a conclusion, comprehensive remarks together with some directions for future approaches are listed, providing food for thought.

2. Preliminaries on crypto-biometrics

2.1. Biometric cryptosystems and protocols

Approaches towards security of biometric technologies are briefly presented in this section. The variety of the concepts are divided to schemes that aspire to transform the aforementioned data, reducing the possibilities for generation of the initial trait used during the enrollment phase, and to cryptosystems that combine known cryptographic functions to derive

cryptographic keys from biometric data. A uniform classification of the various techniques according to their functionality is described diagrammatically in Figure 1. In the first division, encryption, hashing, transformation and other cryptographic techniques produce one-bit verification for biometric systems. Next in order, data are used to obtain keys that further will be used as an extra secured method. Ordinary biometric systems requires prior a database which contains stored biometric or non-biometric references to the data for further comparison causes. The lack of revocability for each of these pieces and the very existence of a place from where information could be leaked, leading to numerous concerns.

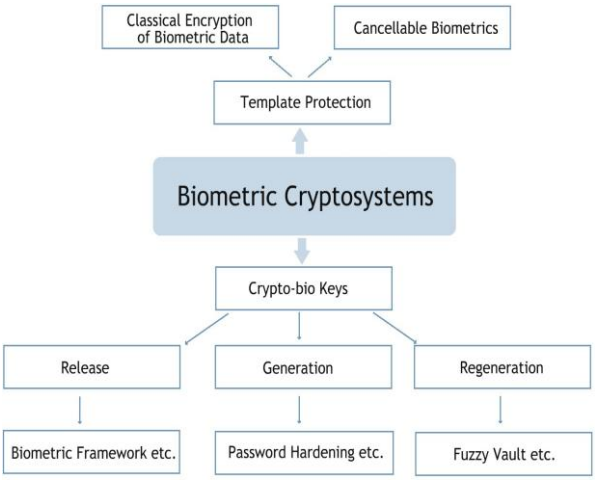

Figure 1. Categories of crypto-biometric systems

For this reason and following the lines of the diagram, classical encryption of biometric data, such as the Advanced Encryption Standard (AES) technique, the trait collaborates with one, or more secrets, similar to passwords that can be stored also in a token or smart card, preserving diversity. Cancellable biometrics category has been studied extensively and inspired various designs for other proposed methodologies. The fundamental ideology can be found in the one-way function re/irre-versible feature transformations, where there is luxury for multiple transformed templates and their uses across applications, under the same identity. At the second cryptosystems' family, the creation and reissuance of keys from biometric data constitute a remarkable and template-free concept. There is a cryptographic framework that is used to securely store just a key born after enrollment and released only over successful verification. This key can be irrelevant or stable bit-string directly extracted from biometrics and in binding approaches can be regenerated, as it is combined with the biometric data using cryptography and possible to be retrieved, later [17].

Protocols for re-generation crypto-biometrics in systems are come to address the specific ways on how to share the keys between the untrusted parties of an authorized user/client and an intended server's principle, and as a field lacks of research progress. Symmetric-key cryptography is fast but too risky, on the grounds that several cryptanalytic attacks can occur in the event of using a single key for a large scale application. Public key suggestions are vulnerable to other kinds of attacks and initially they do not include the verification of authenticity to each entity. To overcome the limitations, protocols designs help to share the crypto-bio keys or create secure authenticated sessions based on biometrics [9].

Taking advantage of this collective knowledge on the core technologies of both biometrics and cryptography, pseudo-identities based mostly on fingerprint characteristics have been carefully chosen during the initial design phase to accomplish a workable trustworthy and friendly scheme that serves principals of user's privacy [18]. The typical architecture of a related ecosystem is based on the independent generation of references coming directly from live biometric samples or already stored biometric templates which after their use as parameters to the embed and non-invertible, one-way, yet unique, functions are finally fully deleted/destroyed. The encoder verifies the identity and builds additional auxiliary data. These information may serve the purposes of interoperability. The methodology is considered to be successful when the final non-biometric data can provide multiple renewable and protected templates, independent pseudo identities for the same individual within an application able to be used across other systems to prevent database cross-matching and linking, preventing impersonation and providing data separation for people with similar features and ability to handle a duplicate enrollment check scenario.

Back to the process, at the second phase, some supplementary data like knowledge-based secrets to be entered by the enrollee (e.g. passwords, signature, secrets) are used as an input to the pseudo-identity encoder and their string is not stored. During verification process, re-creation of a pseudo-identity or directly verification a previously stored pseudo-identity based on a provided recognition sample is performed. The transformation of information and the provided auxiliary data are also used and of course the same supplementary data from the user. The comparator compares both elements or identities to check if originally coming from the first subject. Validity checks and expiration can be controlled especially for characteristics that can change with the passing of the years. Revocation is also available, in case of deleting the pseudo identity from a database, and/or removing the authorization, then the re-enrollment may result in a new protected template. Figure 2 presents the creation

and verification of protected templates by pseudo-identities.

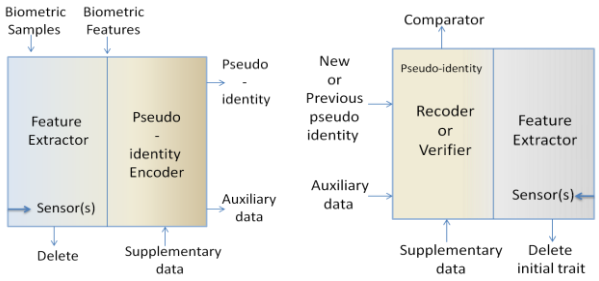

Figure 2. Biometric protection on pseudo-identities

Indubitably, in every scenario, the verification performance and the evaluation of the overall function of the crypto-biometric systems largely depend and based on the baseline of its system. The error correcting codes algorithms are used to improve the degrades and analyze any perspectives able to change, in a better level, each approach. The important factors are the adoption of multi-biometrics as an emerging development, understanding that obtaining high entropy keys is still a challenging, but encouraging issue. The use of passwords, tokens, electronic documents or smart cards can secure user's privacy, the appropriate secured sharing of the keys based on totally untrusted involved sides on a system and the ability to combine basic elements from each category suffice to design new complete hybrid systems.

2.2. Hotspots at biometric systems

The security breaches directly or indirectly, as described above, may aim towards different parts in system modules. Eight categories are used for notice the points for possible threats, such as the generic scheme in Figure 3 portrays. The frame symbolizes the inner aura and attacks that can take place in that are further divided into three groups [2]. Threats at the communication channels between different parts of the system, attacks to the feature and matcher extractors, those ones that could take place under the assumption of the database of information is compromised. The direct, also known as spoofing attacks are substantially described at the next subsection and here indicated as the first spot at the level of sensor.

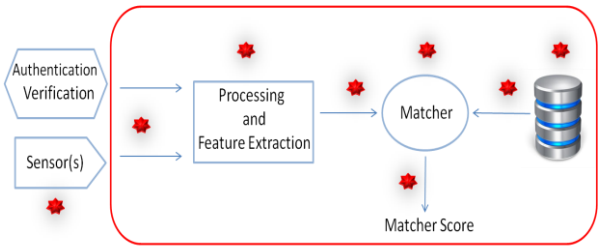

Figure 3. Eight areas in emergency

An analytical outlook to indirect attacks involves a deviant and the communication tunnel between user and the valid end system's controller. The attacker must mainly know specific information about the process of the whole application, the template format, the scores, communications protocol, the data transmission elements and can perform an access to all its stages. In this way, the intruder can gain the extraction, changing, deleting, adding of important data on identities. Specifically, the communication channels across consecutive parts of the system can be intercepted by an eavesdropper who changes surreptitiously the messages in the link, manipulates the scores, decisions and results or makes brute force attacks by exhaustively trying to find the input that can unlock the region of interest. During the pre-processing and feature extraction progresses, insertion of impostor data and component replacement can happen, while the same could take place as well at the matcher level with the hill-climbing algorithms, consisting on iteratively changing some synthetically generated templates until the right one is found. Lastly, the database's region is characterized as imperatively dangerous and involves malicious tampering at the templates from reading to modifications of the links between biometric data, increasing privacy concerns.

3. Comprehensive literature review

3.1. Spoofing attacks

In the case of spoofing attacks that may take place directly towards the initial level of sensor, a zero-effort or active impostor tries to positively claim a different identity deceiving the acquisition system. The means of this kind attack are highly depended on the type and quality of design and application. For the first mentioned, an unauthorized person uses his/her own trait that by mistake can be matched to a template. This cascade effect happens due to dysfunctional false acceptance rates of a system that make it vulnerable. Obfuscation intents are carried out without the requirement of advanced technical skills, by presenting a counterfeited stolen, copied, replicated biometric and the range includes gummy fingerprints, photos, three dimensional-3D shaped models or falsification of facial characteristics using make-up, plastic surgery, imitations or short video clips for gait, signature or handwriting, recorded speech modality and voice conversion, high resolution pictures of iris or even ears. To sum up, sophisticated cheaters have constantly managed to artistically fool the most smart computer devices simply by taking the advantage of the increasing popularity of social network websites where photographs are available, such as facebook, instagram, youtube etc.

Research has proved that none scheme is completely spoof-proof, since almost all commercial devices by private security firms are defeated after this kind of attack. However, the issue is not about the hacked systems but people and this is a particular challenge, not only in criminal, but also in civil matters. The implications are gradually increased across different devices and public services. Depending on the position of the attack, recently published works have managed to categorize and evaluate them with regards to the scores of rates that a system can demonstrate when it is threaten. Insufficient, sub-optimal, optimal and super-optimal attacks constitute the terminology for spoofing acts [4].

From an ethical perspective, a deceiver can claim an identity and gain access to private data or parallel information that may lead him/her to someone's car, mobile, computer, house, electronic passport, totally ruining a personality in society. A decade ago, all these would be heard like a myth or seen as a movie scenario, nevertheless, nowadays persons may well consider such information intimate and part of a broadly acceptable status quo, and hence demand a vigilance attitude from companies and authorities, with skeptical position against any alarming behavior could threaten their interests. Undoubtedly, it remains really hard for non specialists to assess the security-low-level parts of a system and perfectly compose their plan, but still there is the belief about those who if they are motivated will find an idea on how to get around any barriers used to protect the targeted system [10]. To overcome these arguments, applications should be designed following the security level needed according to its potential purpose, the scale of the data and concurrently follow privacy by design rules, covering the ISO Standards, respecting legal provisions.

3.2. Anti-spoofing countermeasures

Up to this point, in research community different methods have been suggested for facing this long-neglected problem against many biometric modes, referred as anti-spoofing, spoof detection or presentation attack detection. By definition, their role is to confer a highly positive characterization about system's trustworthiness [7]. In this way, the major objective is to ensure the protected environment of an application which can recognize only genuine users and not detect and prevent spoofing attacks, as is mistakenly believed. Having this in mind, the questions about the huge chasm between research results and real-world applications can be answered [15]. Minding the gap, the technology of a biometric verification system should contain by design the incorporation of mechanisms that reject spoofing attacks and are under alliance with the parts of the final system considerations and characterize its overall susceptibility.

One the most familiar and user-comfort technique that is used for increasing the awkwardness to spoof a system are passwords or smart cards, offering the opportunity for supervising the verification process. Although the way has been successfully, at some percentage, practiced on transactions, other recognition applications that require communication between services and enrolled person, such as travelers' checks, need other anti-spoofing methods, involving the combination of multi-modal biometrics for one identity and liveness detection. Human physiologic information do not indicate that the person who is present at the time of capture is actually alive. Liveness detection tests some data inherent to the biometric or additional processing of information captured by reader to extract contextual, discriminating features or extra hardware. On the same wavelength, pulse oximetry, electrocardiogram, palm vein, keystroke, typing rhythm, gait, ear acoustic properties, finger/hand temperature sensing, facial thermograms as continuous authentication mechanisms and challenge/response actions describe the cooperation of the user who provides unintentionally or must do something, a blink, pupil, lip or head movement, allowing the system to understand his/her real presence.

Algorithms, freshly proposed countermeasures, standards, protocols and recorded databases for further analysis have received upsurge attention, with varying degrees of spoofing vulnerability, covering a range of attack scenarios and acquisition conditions [13]. Methods are classified in three categories, firstly, a real living body possess color, texture, elasticity and supplementary intrinsic properties, which can be used to check the validity, human expressions, reflex and involuntary signals are secondly grouped. Finally, coming from traditional forensic environments, the collected trait is examined for spotting clues of forgery of friction ridge skin clarity. Academic and industrial projects choose the baseline, plot the licit/normal scenarios and the error rates criteria for the experiments, conducting on freely datasets, available for offline work, containing samples for different modalities. Among the most "overused" evaluated biometrics are fingerprints, iris and face, due to their widely accepted distinctiveness [10].

Respectively, face presentation potential can be handled by subject-specific 3D facial masks which analyze local binary patterns based measures. A powerful way to eliminate similar threats are the background motion correlation and texture of the surrounding facial region quality measurements, something that could be useful especially to more realistic scenarios [19]. For fingerprints, algorithms that can perform an analysis about the capture of

multiple samples of a biometric instance in a short time frame are combined with those that allow live detection and segmentation of the finger, including defenses against gelatin, gummy and silicon samples and others that offer processing of the photo with graphical operations, enabling a convenient thought about how to capture multiple views of modality from different fingers from one subject. The results prove well-promising rates, even though the existence of a purely incapable of being deceived climate system is simply a utopia, under the current circumstances. A novel multi-spectral approach to manage these challenges is to use the proposed cascade structures as a part of a larger anti-spoofing solution that involves multiple modalities from the user, his/her movements to justify the presence, algorithms that overcome the noises, simulate light reflections, determine the scene motion, fixations, speed, acceleration, or even anticipate video replay attacks. The developments may be evaluated through test protocols, applied to more comprehensive databases, and meanwhile the techniques should to be based on specific frameworks, supporting larger scales and each generalization need to be carefully controlled.

4. Mutli-biometric cryptosystems

4.1. Attacks

The technologies of multi or single biometric cryptosystems have been encountered to infiltrate systems, preventing from some malicious performances, while remain exposed to classic spoofing ones. Briefly, it is pointed out that a skillful adversary has to know additional transform parameters or secret keys to defeat the area with previously enrolled samples, since both categories used to cooperate with helper data or are bound to cryptographic techniques and tokens. In such a condition, reconstruction of the original template, and consequently its raw usage or the synthesization of fake physical biometrics, is greatly complicated. The multi-modalities for one identity offer the advantage of extremely low false acceptance attacks in a tampering hypothesis. On the contrary, if a single trait is compromised then the whole template can be recovered, when a blended replacement attack take place, where subject and attacker's template and distinct parts of larger sets are merged into one [20].

Cancellable approaches transform non/-invertibly can unlock the genuine user's biometric or some elements of it, respectively [12]. Fuzzy commitment schemes and vaults, which are related to entropy rates and wittily hiding the biometric (e.g. minutiae and chaff points for fingerprints), are vulnerable if the algorithms are poor. Helper data and key-re-generation schemes extracting short keys or suffering from improper accuracy present high tolerance, making achievable the composition of an approximation of the initial biometric from its hashes. Coercitive, device substitution intrusions and any possible combination of serial venomous acts could be applied sufficiently, compounding a worst possible scenario, but rather unrealistic in everyday contexts.

Since it remains still necessary to test the robustness of multi-modal biometric systems, especially for combinations such as face-fingerprint or/and face-iris, under various realistic hypotheses, recent studies [14] conducted some experiments. This analysis may allow figuring out to what extent each balanced countermeasure is representative of the performance. The relevant endeavor was based on established state-of-the-art authentication technologies for each modality and different combinations of attacking story lines using datasets of spoofed templates or traits. The final comments led us to the denouement that multi-modal schemes suffer from lack of unsuitable strong protection for their template, as the design of optimized fusion rules is currently under research. At the very least, attacking assumptions are too pessimistic and result in a significant overestimation of the false acceptance rates, a case that turned out to be positively reassuring, but certainly non-effective for more advanced and elaborate intrusions.

4.2. Resistance

Response-focused methodology on the basis of possibility to integrate liveness detection or the mentioned anti-spoofing methods include experimental investigations to verify whether and to what extent multi-modal verification systems could be assessed as securely protected. Until now, studies on spoofing underline that using multi-biometrics, the recognition performance is higher but unfortunately unimodal approaches handle better external attacks [3], [5]. To reduce the risk of exposure of the combined template, if a single trait revealed, the selection of other biometrics, akin to hand-fingerprint, face-iris, instead of multiple fingerprint samples, for example, is recommended, based on empirical evidences. For increasing robustness, the design of stronger fusion rules (score or feature level are recommended) between samples is mandatory. Additionally, cryptosystems and especially crypto-bio keys ideas for multi-modalities are not only more efficient than mono-modal ones, but simultaneously privacy friendly. These suggestions pretend to bring some insight into the difficult problem of evaluation through the effective countermeasures that can minimize the effects of threats by taking into consideration the techniques of fusion, the serial or parallel modes, the type of cryptographic algorithms,

complexion of the application according to the hardware and its interconnects [20]. Finally, we emphasize that any protection mechanism should respect design principles and keep the overall balance of the system, without underestimating that extra efforts can bring about the cost of sharply reduction of verification performance.

5. Bimodal person verification system

People from dozens of nations have already acquired their new electronic passport equipped with contactless chip that stores personal data. The expansion of illegal occurrences in this area increases the lack of public trust with numerous privacy, physical safety, and psychological comfort consequences [7], [10]. As a counterweight for the theoretical analysis of the previous sections, Figure 4 introduces a bimodal biometric model for person identification made up of face and fingerprint, or face and iris matchers. The framework is a bold initiative in the deployment of three technologies: crypto-biometrics, anti-spoofing countermeasures and Radio Frequency Identification (RFID). This ePassport idea is inspired by previous works on spoofing for biometrics [4] and designs to defeat attacks through implementations of RFID authentication protocols and data encryption, increasing the complexity and therefore robustness [16], while cryptographically advocating the secrecy requirements for biometric data, which is mandatory for identity documents schemes [6], [11].

5.1. Function and the design process

During enrollment a pair of datasets is collected. To preserve the principals of protection of user's privacy, the created template consists of transformed minimal elements of the initial biometrics binded together under a cryptographic algorithm which uses them to create keys. The extended version of this deployment can be understood as this part was explained previously in Section 2, Subsection 2.1, paragraph for biometric template protection based on pseudo-identities. The scheme involves auxiliary data delivered from the involved hardware, authority etc. The supplementary data in our design coming from the liveness detection process. The final non-biometric information stored on ePassport's chip are the crypto-bio key, which can be unlocked only when both biometrics are matched, traveler's personal details and document's type, digital number, etc.

The description of the anti-spoofing verification system involves liveness detection method combined with the current RFID access control process. When a user approaches to an E-Gate for automatic passport checking, video sequences are captured by its cameras. Then the system requires the cooperation of person who has to turn left or right the head and provide his/her fingerprint to a sensor (or move eye to an iris movement tracker). The three dimensional facial object as a result helps system to separate an alive human from a photo. The matching parameters are scored under a fusion rule which its optimal threshold depends on both of them, as a mechanism against multi-biometric template threats [20]. After judgment, the recognition procedure demands the use of final fusion score to extract from the database (chip) the cryptographic key and thus the informative content.

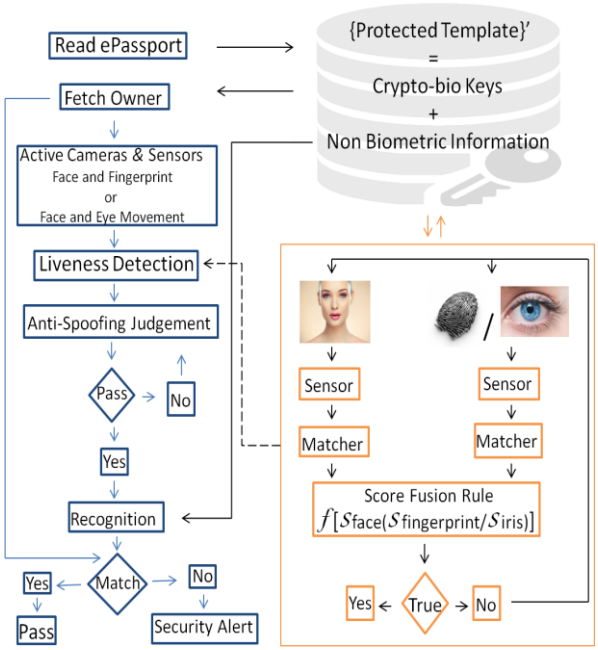

Figure 4. Flow chart of framework

5.2. Usability and advantages

Exploring the privacy and security usability of this method, authors respected the needs of such an impending worldwide next-generation authentication technology, as those were determined in admissible experiments [6]. The framework preserves data confidentiality as the initial biometric used for enrollment and verification or authentication is minimal and can be only available for the creation of the pseudo-identity. The final chip does not store biometric information and is additionally transformed using one-way bit functions. The re-generation or revocation of the pseudo-references may be an answer to lost identity documents or compromised identities. This approach as a biometric template mechanism could be also useful for many other applications. For example using only identity cards or ePassports, if someone travells from one country to another, for

gaining access at his/her bank account [11]. The supporting architecture of RFID protection mechanisms provides extra security for sensitive information, such as birth date or nationality that are carried on passports.

Liveness detection as an anti-spoofing countermeasure is nowadays among the most "acceptable" ways against spoofing of identity documents, during border control checks. The process can ensure the presence of the passport's owner. Furthermore, analyzing the result of sensor on a three subject-specific 3D facial trait with local binary patterns and those data delivered after the cooperation of person, iris movement tracking or presenting his/her fingerprints, the system can be smart enough to understand a genuine user or not.

The design requires the matching of many parameters that are scored under fusion rules, as a more tested method for better results in modalities like those used in our scheme. The optimal threshold depends on both of the strings "unlocked" under the presence of its biometric characteristic, something that can overcome the threat of exposure the whole template in multi-biometric template combinations [20]. The overall strings are cryptographically secured to proof that the judgment during the recognition procedure will minimize the false acceptance rates.

Summarizing, this deployment definitely deserves a better analysis as it is just the first step of spoofing against next-generation identification systems. The encouraging part is the fact that this thought underlies on previously researches that emphasize how important is to combine all the current knowledge in cryptography to protect the biometric systems and the human rights to privacy. The anti-spoofing methods based on the cooperation of machine-user add a new layer to secure authentication, and relevant deployments after test and evaluation can benefit the needs of citizens, government and industry.

5.3. Vulnerabilities and limitations

The vulnerabilities of this framework found on false acceptance percentages for an imposter's recognition and ingenious spoofing actions, under police presence and could be considered as worst-case assumptions. ICAO standards and ISO protocols through documents that unequivocally identify their bearers were assumed to guarantee the protection from the document forgery. RFID access control processes and other impacts on security issues in ePassports, even though they are a charming field, are beyond the scope of this paper.

As limitations of the design could be characterized the poor quality of the cryptographic methodologies used in producing the pseudo-identities or/and score fusion rules results. The function is time consuming, regarding that it performs different steps to provide a final result. This is a significant drawback considering that it should be used as a method for border control with millions visitors daily. The facial recognition as the first and immutable part of this system is weak during liveness detection performances as the result may vary if the user moves the head fast, increasing the error rates. The fingerprints present shortcomings, as well, due to the fact that are affected by age. Finally, pseudo-identities have been implemented in applications only for fingerprints and it remains untested their performance in other biometric traits.

Research about the function of the suggested model is currently aimed on tests on the pseudo-identities for other samples. Secondly, the selection of fusion rules will be carefully selected according to the need of the scheme, as those were underlined above. The final experiments will be conducted on datasets of "real" and spoofed biometric elements. The overall accuracy and privacy evaluation will be determinant for the acceptance of the methods.

6. Conclusion

The paper represents an attempt to acknowledge and account for the schemes using combination of cryptography with biometric characteristics and how this could play an increasing role in electronic documents and transactions for identifying a person, limiting security risks. Current methods and their design suffer from vulnerabilities, and here is where measures become crucial in order to protect schemes and the overall efficiency of government and commercial applications. Spoofing attacks at the sensor level of a system used for automatic recognition of people from their biometric characteristics have been tackled by independent and/or collaborated to initial design and application, anti-spoofing attempts [8]. To appraise data protection problems, multi-modalities, current research developments on suggestions against invasive actions and a prototype face-fingerprint/iris cryptosystem have been presented. Create an all-inclusive view, we believe that this project will help to better evaluate the impact of spoofing attacks from a security and privacy engineering aspect, contributing to ongoing and expected attempts in pattern recognition area.

In outcome's atmosphere, the application of biometrics in different services requires high accuracy rates, secure personal information storage and reliable generation of data while the whole process of transfer is proof. Identity thief might exploit in occasion of low protection levels. Even so, some modalities are more robust than others, however, this should not be interpreted as meaning they are more reliable [1].

Spoofing and countermeasure assessments are a complex part for each study as it is mandatory to think all the involved possibilities and design generic frameworks with a manageable impact of usability. Challenge-response approaches seem to be supplementary to the traditional ones and more effective for risky applications. The standard evaluation methodology during the phases of the architecture can lead to better independent networks and fused countermeasures as a valuable strategy.

For some conditions, even if anti-spoofing measures could adequately assessed, the rapid progress of adversaries' actions at the initial steps of verification purposes throw up wider concerns on public narratives of privacy and frequent monitoring of individuals. The advancement of theory on secured access control and practical design implementations of the provided valuable experience on technologies will improve their robustness.

7. Future research

Directions for further research and open issues may be focused on anti-spoofing techniques for biometric multi-modalities and their combinations, seeking to reduce the different degrees of deception/lying, while enhancing the proper function of the system. An anti-spoofing method is not constructed to operate as a stand-alone procedure but together with the biometric recognition system. The design must be in a way that does not suffer from error recognition rates itself. Cryptography can offer significant, but inadequate solutions in this emerging technology, and thus next steps on encryption schemes may promote the security strength against intrusive attacks. Multi-biometric systems can be easily cracked by spoofing only one trait and future works should flatly investigate how to bring robust results on score level fusion rules and provide protocols for provable secure authentication based on template protection schemes.

From another angle, state-of-the-art suggests the use of databases for spoofing and anti-spoofing analysis but still lacks to cover all the possible scenarios and certainly the implementation in real-world applications. The problem of generalization should be addressed as well, due to the fact that current findings may cover individual occasions for some biometric traits, leaving gaps to varying areas of a system that verifies or identifies biometrically users. Concurrently, the missing pieces of the puzzle for better approaches may lie at the combination of different anti-spoofing algorithms. Liveness detection efforts, and challenge approaches with the cooperation of user, could be tested to offer advantages versus tricks that can fool existing systems.

Apart from design ideas and open research questions on the protected operation of the system, the major themes of human privacy and rights to anonymization, facing the obstacles of societal suspicions over surveillance, and other specified and legitimate services should be covered. Decisively, the starting setup is vital for the entire field. Human biometrics may be collected and processed under detailed protocols, only compatible and accordingly related to the scope of the authority involved in the transaction, always respecting proportionality and serving the forensic experts thoughts on the prevention of spoofing, where we may profit more from a careful appraisal of the processes, supporting the structure of the biometric system.

8. Acknowledgements

Authors would like to thank colleagues from KU Leuven, University of Sassari, Michigan State University and University of Halmstad, for their ideas. The attention, support, comments, and contribution of anonymous reviewers regarding improvements of this PhD work, is gratefully acknowledged.

9. References

[1] A. Hadid, N. Evans, S. Marcel, and J. Fierrez. Biometrics systems under spoofing attack: An evaluation methodology and lessons learned. *IEEE Signal Process. Mag.,* 32(5):20–30, 2015.

[2] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security,* 2011(1):1-25, 2011.

[3] M. Gomez-Barrero, J. Galbally, and J. Fiérrez. Effcient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters,* 36:243-253, 2014.

[4] I. Chingovska, A. R. dos Anjos, and S. Marcel. Biometrics evaluation under spoofing attacks. *IEEE Transactions on Information Forensics and Security,* 9(12):2264-2276, 2014.

[5] G. L. Marcialis, P. Coli, and F. Roli. Fingerprint liveness detection based on fake finger characteristics. *IJDCF,* 4(3):1–19, 2012

[6] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in E-Passports. *IACR Cryptology ePrint Archive,* 2005:95, 2005.

[7] A. P. Rebera, M. E. Bonfanti, and S. Venier. Societal and ethical implications of anti-spoofing technologies in biometrics. *Science and Engineering Ethics,* 20(1):155-169, 2014.

[8] E. Marasco and A. Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Comput. Surv.,* 47(2):28:1-28:36, 2014.

[9] S. G. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi. Enhancing Information Security and Privacy by Combining Biometrics with Cryptography. *Synthesis Lectures on Information Security, Privacy, and Trust.* Morgan Claypool Publishers, 2012.

[10] S. Marcel, M. S. Nixon, and S. Z. Li, editors. Handbook of Biometric Anti-Spoofing - Trusted Biometrics under Spoofing Attacks. *Advances in Computer Vision and Pattern Recognition.* Springer, 2014.

[11] C. A. Shoniregun, S. Crosier. Securing biometrics applications. *Springer-Verlag US, Book,* London;New York : Springer, 2008.

[12] C. Li and J. Hu. Attacks via record multiplicity on cancelable biometrics templates. *Concurrency and Computation: Practice and Experience,* 26(8):1593-1605, 2014.

[13] R. Raghavendra, C. Busch. Presentation attack detection algorithm for face and iris biometrics. *Signal Processing Conference (EUSIPCO), Proceedings of the 22nd European,* pages 1387-1391, 1-5 Sept. 2014

[14] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli. Robustness of multi-modal biometric verification systems under realistic spoofing attacks. *In 2011 IEEE International Joint Conference on Biometrics, IJCB 2011,* Washington, DC, USA, October 11-13, 2011, pages 1–6, 2011.

[15] De Freitas Pereira, T., Anjos, A., De Martino, J.M., Marcel, S., Can face anti-spoofing countermeasures work in a real world scenario?, *Biometrics (ICB) International Conference,* pages 1-8, 4-7 June 2013.

[16] B. Jing, P. P. K. Chan, W. W. Y. Ng, and D. S. Yeung. Anti-spoofing system for RFID access control combining with face recognition. *In International Conference on Machine Learning and Cybernetics, ICMLC 2010,* Qingdao, China, July 11-14, Proceedings, pages 698-703, 2010.

[17] D. Bissessar, C. Adams, and D. Liu. Using biometric key commitments to prevent unauthorized lending of cryptographic credentials. *In 2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, Canada,* July 23-24, pages 75–83, 2014.

[18] J. Breebaart, C. Busch, J. Grave, and E. Kindt. A reference architecture for biometric template protection based on pseudo identities. *In BIOSIG 2008 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 11.-12. Darmstadt, Germany,* pages 25–38, 2008.

[19] A. Hadid. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. *In IEEE Conference on Computer Vision and Pattern Recognition, CVPR Workshops 2014,* Columbus, OH, USA, June 23-28, pages 113-118, 2014.

[20] Z. Akhtar, B. Biggio, G. Fumera, and G. L. Marcialis. Robustness of multi-modal biometric systems under realistic spoof attacks against all traits. *In IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, BIOMS 2011,* Milan, Italy, September 28, pages 1-6, 2011.

