Enhancing Security by Combining Biometrics and Cryptography

Diana Popa
Automatic Control and Computer Science
University Politehnica of Bucharest
diana_maria.popa@stud.acs.upb.ro

Emil Simion
Mathematics and Applied Informatics in Engineering
University Politehnica of Bucharest
emil.simion@upb.ro

***Abstract*— The impressive amount of recent technological advancements in the area of information systems have brought along, besides the multitude of positive aspects, some negative aspects too. The most obvious one is represented by the fact that the technological innovations are prone to various categories of threats. Making sure that information stays safe, unaltered and secret is an integral part of providing technology that behaves in the manner it is supposed to.**
Along with researching techniques of effectively securing the communication, other aspects that also deserve to receive attention are authentication, authorization and accounting. One security aspect that has been the most intensely researched in the past from the three, is authentication. From the various methods used in verifying the identity of users, one more recent one is biometrics that can significantly heighten the safety and security of a system. However, authenticating the user into an information system may not be entirely safe all the time.
The aim of this paper is to present an overview of the different plausible methods of combining cryptography related concepts and biometrics techniques. This additional attachment of cryptography has proven to make the process of gaining access to an information system much more secure.
The problem tackled in this paper will be presented from a two way perspective: on one hand, it will be discussed how biometrics can make use of cryptography-specific solutions in order to enhance its powers and, on the other hand, it will be presented how cryptography aspects can use the specific biometric data of a user to generate encryption keys that are much harder to decipher or to obtain. After this methods are presented, the theoretical basis for measuring performance of a biometric system will be presented and a survey on current performance results on fuzzy vault techniques will be enumerated and described.

***Index Terms*— biometrics, cryptography, security, fuzzy vault, cancelable biometrics**

I. INTRODUCTION

The early sole target of **cryptography** was to find ways of altering some message in order to make it unreadable until it reaches the correct intended receiver which in turn should be able to decipher its meaning. However, nowadays the intends of cryptography have extended from just confidentiality related purposes to more complex concepts like mutual authentication between different entities, digital signatures issuance, integrity checks capabilities, digital stamps for storing time of creation of some arbitrary message.

On the other hand, **biometrics** refer to some intrinsic characteristics that a certain person possesses and they can be categorized into psychological traits (iris, face, fingerprint, voice, even ear shape) to behavioral ones (gait, signatures, keystrokes dynamics). Thus, biometrics represent a way of authenticating a user into a system by making use of its distinctive personal traits. Given the fact that they are not based on knowledge or possession (in contrast to the traditional method of using PINs, passwords or gesture patterns), they are not prone to being lost, stolen or forgotten.

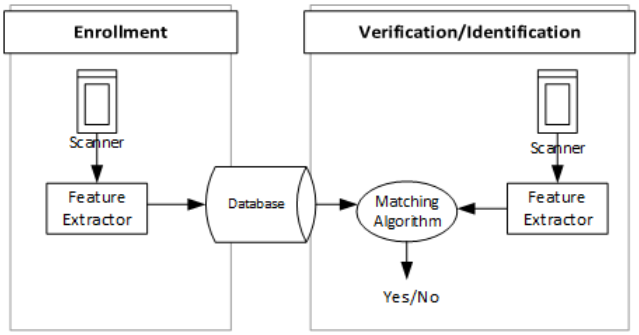

Fig. 1. Functioning Modes of a Biometric System

A biometrics-based system behaves as a system for recognizing patterns and they can work into one of the two modes: *identification* and *verification*.
Figure 1 exposes the two phases of such a recognition system. The first phase, which is called the enrollment, the biometric data of some person are collected and are stored in a database for future use. It can also be observed from the image that the second phase of the biometric system use can either be represented by *verification* or *identification* procedures, depending on what we need the biometric system to offer us.

The purpose of the *verification* phase is to check if the identity that is claimed by the user matches against one specific template from the database. This is a ”one-to-one” process as the system compares only the template provided by the current user, that is trying to gain some rights, and the only template from the database that is associated to the identity that has those rights.
On the other hand, the *identification* phase is a ”one-to-many” process as it uses the one template being introduced at some arbitrary moment in time to search among all the templates stored in the database as part of the enrollment

step to find the one that outreaches some threshold of similarity.

When it comes to identifying vulnerabilities in each of the main concepts described above (i.e. cryptography and biometrics), the major security issue, as far as **encryption schemes**, is how to make sure that the secret key (or the private key in the context of asymmetric cryptography) remains secret. The importance of key management in symmetric and asymmetric encryption schemes was first studied and outlined by its pioneer, Shannon, in 1948[20].
On the other hand, one major security concern in the case of **biometric system**, is template protection. Thus, implementing methods to ensure that the template data stored at the time of enrollment can not be damaged, misused, interfered with when they are transmitted over some network is integral for any secure biometric system. It was shown in the past by authors of [13] that if an attacker can gain access to a database that stores fingerprints it could use them to create artificial fingers to impersonate another person.

This paper is organized as follows. In the second section some previous techniques on each of the two perspectives of this paper will be analyzed. In section III, we will focus on two of the selected paradigms of each of these two perspectives, will present the algorithm that lies at their core and a performance evaluation will be executed on each of them. In the last section the realizations of this paper in the form of conclusions will be established.

II. Related Work

In order to better grasp the differences between each of the two perspectives presented in this paper regarding different methods of applying biometrics to cryptography, and the other way around, we firstly analyze each one of them by presenting previous research separately on each of them.

A. Template Protection using Cryptography

This important security issue refers mainly to protecting against confidentiality- related attacks. This means that during storage or transmission over some external network, an attacker is not able to read the biometric data and thus be able to reuse or recreate it.

The obvious solution of simply encrypting the data with some symmetric encryption scheme is not a feasible solution. Suppose there is some biometric data B that needs to be encrypted and some secret key K used to encrypt it to some final message $C_K(B)$ which is the one stored in the database for future reference. At the time of verification, let's say the biometric acquisition mechanism will collect the biometric data B' (the chances of B being identical to B' are very low). And thus, the final message obtained is $C_K(B')$ which needs to be compared with $C_K(B)$ by the matching algorithm (as per Figure 1). However, by taking into account another important property of symmetric encryption algorithms, even when B is very similar to B', the resultant outputs [i.e. $C_K(B)$ and $C_K(B')$] are very different.

However, a more complex model which succeeds in solving the problem of noisy biometrics are **shielding functions** which were firstly researched by Linnartz et al. in [12]. In their proposed model, the authors make use of *δ-contracting functions*, a new concept introduced in the same paper. These functions receive as parameter two vectors: one is a constant vector (W) chosen such that, when the other second vector's value (X) remains in some arbitrarily chosen radius δ, the output of the function's value is constant. Indeed, the second vector X represents the biometric information collected from the acquisition device. In the case where the function's value is constant, the value of it is used as a secret key K. One more distinctive feature of this technique is that in the database are stored two things: the encrypted value of the secret key K and the constant input vector of the δ-contracting function. At verification, the δ-contracting function is applied to the constant vector W from the database and some new vector Y. If the difference between this Y and the one used at enrollment X is less than some δ, the contracting function should return the same value, which is the secret from enrollment K. The encrypted value of this K is computed and it is compared with the one stored in the database. If they are equal the system would return an accept.

However, the most popular concept that proposes a system for protecting the template data against theft, is **cancelable biometrics**. As per the pioneering research provided in 2001 by authors of [17], this cancelable technique was invented as a solution to solve the major risk posed by the possibility of some biometrics being stolen. In contrast to some PIN, password etc, that upon being stolen can somehow be replaced, in the case of biometrics, that is impossible. So, the authors propose a technique for intentionally altering the biometric using a mathematical transform and applying all the matching verification inside the transform's domain. In contrast to a symmetric encryption scheme, the transforms used to 'cancel' biometrics are non-invertible, which means that after it is applied, there would be practically impossible for an attacker to obtain the initial data from the distorted one. Moreover, if the biometric data happens to be lost, or if the transform is somehow disclosed, new biometric measures are to be collected and a new transform will be applied to obtain the biometric template that is to be stored in the centralized database.

In 2007, Ratha et al. [16] proposed three of the transformations that were to become the most frequently used transformations for distorting some biometric traits. The *cartesian transformation* implies the division of the space where the minutiae of the fingerprints lies into multiple rectangles that have the same size. It may look like a matrix where at some position can exist multiple

values. Then some transform is applied on the cells to bring them in a different position. The second type is the *polar transformation* where the space is, this time, divided into sectors and the minutiae are placed given their polar coordinates. A transformation matrix is also applied on each of the sectors of the main configuration. It may be the case that after this minutiae that were initially in different sectors, may now lie in the same sector from the imaginary circle. The *functional transformation* comes as a solution to a shortcoming that both the *Cartesian* and the *Polar* transform have. A small change in the initial localization of the minutiae points leads to a significant impact on the transformed configuration. In order to obtain the where and how much some minutiae point may be moved, they propose to use the phase and the scaled value of 2d Gaussians.

A very recent study [19] that focus on **performance evaluation** of different security measures for encrypting systems, aims at presenting a comparative risk analysis of various techniques used to secure biometrics in general: cancelable biometrics, encryption and 'liveness detection' which refers to mechanisms that can detect the authenticity of some biometric measurement in order to avoid spoofing attacks such as artificial fingers, recorded videos, contact lenses in case of a face recognition system. The results show that cancelable biometrics are less riskier than encryption but are less safe than the 'liveness detection' techniques.

B. Enhanced Key Management using Biometrics

The cryptographic systems where biometrics are used, in a manner or other, to possibly enhance the security level of that system is called a **biometric cryptosystem**. In general, at the core of any cryptosystem lie three types of algorithms that are mandatory:

- the key generation algorithm
- the encryption algorithm
- the key decryption algorithm

However, based on the necessities of the context in which a cryptosystem is to be implemented, other algorithms can be attached to the three mentioned above. It can be seen in [22] where the authors implement a public key cryptosystem where they need to develop two more algorithms (i.e. the digital signature and the identity verification algorithm) in order to sign the message to be sent and to be able to verify that the signature of that message is authentic or not, respectively.

A bio-cryptosystem actually impacts the first main algorithm of any cryptosystem (i.e. the key generation algorithm). Basically, biometrics are introduced in order to make the process of generating and managing secret keys more secure. In contrast to the template protection issue discussed above, where cryptographic solutions were employed in order to make biometric information stay safe, in this second case, biometric data represents a new helper method of generating (and thus securing) cryptographic keys.
In specialty papers, the process of securing secret keys with biometrics is further divided into two categories: **biometric key-binding** and **biometric key-generation** and this is how related previous work will also be presented in this paper.

1) Biometric Key-Binding: In this particular case, at the time of enrollment an unique secret key will be generated based on the biometrics provided. This key will be stored in secured centralized databases together with the template data. It is important to note that their combination is not simply stored in plain mode, some kind of undecipherable blending of the two is created (we will see more when describing specific current techniques).

One very popular key-binding scheme is called **Biometric Encryption** (it is so popular that it can also be found under the shortcut *BE* in specialty papers). The first ever study of 'BE', published in 1996 [24], is called *Mytec1*. Unfortunately the implementation did not give satisfactory results as far as accuracy and security level requirements. Not until 1998, did the first practical scheme of 'BE' from the same authors [21] appear.
However, a more recent version of 'BE' which is used for face recognition is presented in [25]. It is interesting that this study inherits concepts presented in the first pioneering works of 'BE' concept (i.e. [24], [21]). First of all, the cryptographic key used in generated using RNG (Random Number Generator), as suggested in [21] but contrary to the suggestion of the latest to use 3DES algorithm for encryption, the authors from the [25], actually use AES. They use the PCA algorithm in order to create a vector of discriminating features extracted from the facial images. In [21], the authors suggest the use of SHA-1 as the hashing algorithm for encrypting the key, however, advances in technology, determined the authors of the more recent work [25] to use SHA-512 for that. They also used the Quantization Index Modulation (QIM), as described in [3], in order to effectively bind the feature vector extracted and the hashed encrypted version of the cryptographic key. The QIM module for decryption will be used at the verification step, in order to unbind the two components mentioned.

Even though the first work on the *Fuzzy Vault* method has appeared much later [8], this method has gained probably the most popularity of the methods proposed for managing encryption keys inside biometric cryptosystems. The first scheme proposed by Juels and Sudan [8] did not offer an implementation also and was based on the previous work done by Juels and Wattenberg in [9]. In the latest paper mentioned the authors make use of error correcting codes in order to solve the problem of noisiness between different acquired biometrics. Their method basically chooses a codeword c from the set of some error correcting code and this can be perceived as the cryptographic key (the secret). At enrollment, the hash of this codeword $h(c)$ and

the difference between the biometric collected (x) and the codeword is stored ($x - c$). At verification, some decoding function is used in order to obtain the new codeword c'. The hash of the obtained codeword c' is computed: $h(c')$ and the condition for acceptance is that $h(c) = h(c')$ (we cannot directly compare c and c' as c is not stored).

The method proposed in [8] is more powerful as it allows the biometric information collected to vary not only in linear noisiness, but also in the ordering of the consisting symbols which can be very frequently happen for collected biometrics. The secret of their novel scheme is to make use of polynomials in which to embed the secret (i.e. encryption key). The degree of the polynomial (t) is equal to the number of symbols in the biometric collected (A). The vault will actually be composed of tuples consisting of the point where the polynomial was evaluated and the associated values obtained. It is important to note that some other random points are added to the vault with the express intend to add noise to the vault (for attack-mitigation purposes). In order to unlock this vault, some cryptosystem will initially have as input this vault consisting of tuples and the new biometrics (with t symbols in it also). The algorithm will search for the points in the vault whose first component of the tuple is equal to the points in the collected biometric information. Basically, by using the biometrics the random points will be extracted out, and only the values where the polynomial was evaluated will remain in the end. After obtaining this set of points, the Reed-Solomon algorithm will be applied. This decoding algorithm can output the polynomial from a field F given the points where this was evaluated and some maximum rank (in this case, we know that the rank is equal to t as specified before).

2) Biometric Key-Generation: In the case of key-generation schemes in biometric cryptosystems, the secret key is generated based on the biometric information. Given the uniqueness of biometric data, a unique secret key will also be derived. In other words, the biometric information also behaves as the encryption key.
An example of such a scheme, where the biometric template is directly used as input to generate some key is described in [5] where they propose a public key infrastructure. At the time of enrollment, the user needs to input ten measurements which will then passed through the "Feature Coding" stage. This basically includes a feature extraction steps and a feature coding step where every discriminant selected is to be encoded to a decimal number. All these decimal codes are joined and the string resulted is used as input to generate a pair of keys (public and private). At enrollment, only the public one is kept. Intuitively enough, at verification time, the private key obtained by following the same steps, but with the current collected biometrics, will be checked against the public key from enrollment to see if they are indeed a pair. Upon success, acceptance is given to the user.

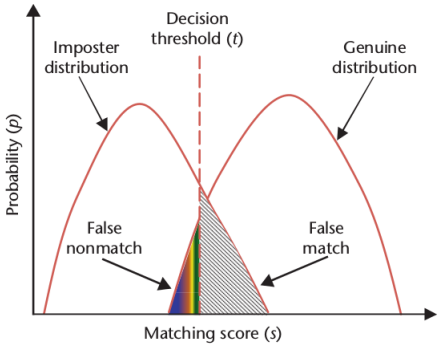

Fig. 2. Biometric Error Rates (taken from [1])

III. Performance Evaluation

A. Theoretical Basis

In the past sections we discussed feasible methods that can be used in conjunction but a very important aspect when changing the usual course of action of a cryptosystem is also making sure that the usability of the encryption system is not affected above a certain limit. Also we would like to see if the system also maintains (in the best case scenario, it actually exceeds) the security level of the original biometric-based authenticating system.

- *False Acceptance Rate* or *False Match Rate* is a metric for evaluating the level of security and it basically expresses how likely is a biometric system to make mistakes by authenticating a user who is an intruder. The formula used to calculate `FAR` is:

$$FAR = Pr(\frac{NFA}{NIA}), \tag{1}$$

where NFA= Number of False Acceptances,
and NIA= Number of Impostor Attempts.

- *False Reject Rate* or *False Non-Match Rate* represents the probability that a biometric system may fail to authenticate legitimate user. It is a percentage of how many of the genuine attempts were wrongly rejected. Formula for `FRR` is:

$$FRR = Pr(\frac{NFR}{NLA}), \tag{2}$$

where NFR = Number of False Rejections,
and NLA = Number of Legitimate Attempts.

The decision of every biometric system to reject or accept authentication attempts is taken by computing a matching score s of how similar the two biometrics templates are. This matching score s has to be greater or equal than some threshold `T`. In conclusion, both `FAR` and `FRR` are dependent upon this decision threshold.

The pairs of templates that pertain to the same user form the **genuine distribution** while the pairs of matches that

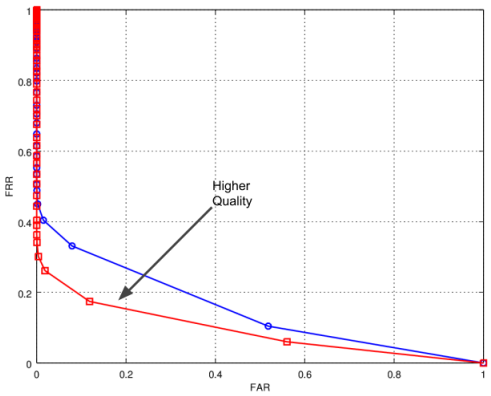

Fig. 3. Receiver Operating Characteristic (ROC created in Matlab)

belong to different persons form the **impostor distribution**, as can be seen in Figure 2. These distributions are influenced by the value of the `s` and `T` (as defined above). We can also observe the areas of false non-match (`FRR`) and the false match (`FAR`) distributions.

As per [2], the **convenience** of a biometrics system can be measured in terms of the `FRR`. With the term convenience, the authors refer to the availability and usability of the system. The higher the `FRR`, the more the biometric system will become more of a inconvenience to some user's legitimate authentication attempts, as per:

$$Convenience = 1 - FRR \tag{3}$$

On the other hand, Bolle et al [2] state that the `FAR` is a measure of the **security** level of some biometrics system and the higher the `FAR`, the less secure a system is, as per:

$$Security = 1 - FAR \tag{4}$$

It can be deduced from the above formulas, that actually the stability of a biometrics system lies at the core of a trade-off between security and convenience. In the scenario where every user is denied access (i.e. `FRR=1`, `FAR=0$`, we are dealing with an extremely secure, but unusable system. If, on the other hand, the biometric system would allow everyone access (i.e. `FAR=1`, `FRR=0$`, we would be facing a very flexible and convenient system, but otherwise an extremely risky one as far as security aspects.

As we can see from the graphic displayed in Figure 2, the `FAR` and `FRR` are dependent on the threshold (`T`). So, let us consider that the functions `FAR(T)` and `FRR(T)` express the error rates when the biometric decisional system is set to function at some threshold. Given all this, we can express the trade-off between security and convenience through a 2D curve:

$$ROC(T) = (FAR(T), FRR(T)) \rightarrow \begin{cases} (1,0) \text{ as } T \rightarrow -\infty \\ (0,1) \text{ as } T \rightarrow \infty \end{cases} \tag{5}$$

This 2D curve is called *Receiver Operating Characteristic (ROC)* in specialty books and an example of such a curve can be seen in Figure 3 where the `ROCs` for corresponding to two different biometric systems have been drawn. The `ROC` underlines the trade-off between `FAR` and `FRR`. The curve that is closer to the axes is the one representing a higher-quality system, as it means the values for the `FAR` will be smaller for any arbitrary `FRR` and the value for the `FRR` will always be smaller for any fixed `FAR`.

B. FRR and FAR for Proposed Fuzzy Vault Methods

Over the course of time, a lot of fuzzy commitment schemes were proposed, each of them bringing a different aspect of novelty. For the purpose of this survey, we gathered the experimental results from papers offering performance results in terms of `FAR` and `FRR`. It can be noticed from the classification, that in 2006, Hao et al [6] proposed a method of applying biometrics to cryptographic keys in order to make the secret more secure. One original aspect of their work is that they used Hadamard and Reed-Solomon error correcting codes for natural biometric variations and for distortion generated by the capturing device, respectively. They tested their method on a database containing 700 iris samples (70 different users with 10 samples each one) and they succeeded in obtaining the best results at the time of their publication. In [18], the authors propose the use of intra-class error analysis as a pre-processing method. They rearrange the iris biometrics in order to better exploit the capacities of the error correcting codes. Their results are very close to those of Hao et al [6] but do not exceed them.

In a more recent paper from 2013, [7], the authors succeed in obtaining competitive results by enhancing the original fuzzy method proposed of Juels and Sudan [8]. They implement a new method of quantizing the minutiae points by dividing the data into bins of variable size, in contrast to the old methods of distributing the minutiae in bins of equal size. The distribution obtained by their methods is far more uniform and thus obtains better results that can be seen in Table I.

Another fingerprint bio-cryptosystem is proposed by the authors of [14] which also focus on a new way of representing the minutiae. The author uses *Binarized Phase Spectrum* quantization scheme which is uses the Fourier phase spectrum. Their system obtains better results than [7] as far as `FAR`, but their `FRR` (`FNMR`) is worse.

TABLE I
PREVIOUS EXPERIMENTAL RESULTS FOR PROPOSED FUZZY VAULT TECHNIQUES

Authors	FAR	FRR	Biometrics
Hao et al [6]	0.0	0.47	Iris
Hartlof et al [7]	0.0044	0.2025	Finger Print
Rathgeb et al [18]	0.0	0.64	Iris
Nandakumar [14]	0.0	12.6	Finger Print
Kudlacik et al [10]	0.61/1.52	22.16/12.16	Off-line Signature
Faruki et al [4]	8.0	10.67	On-line Signature
Kumar et al [11]	0.51	8.3	Finger Print
	0.46	7.33	Palm Print
	0.31	12.46	Iris
	0.64	8.5	Hand Vein
Nandakumar et al [15]	8.0	9.0	Finger Print + Finger Vein + Iris

In more recent studies, such as the one from [10], the fuzzy vault method was applied to recognize off-line signatures. The gathering of discriminators points from the signature is done by establishing the middle of the signature and then dividing the signature by lines drawn at different angles. The features are represented by the points lying at the intersection with these lines. As far as online signatures (the signatures that are taken on a pen based tablet) there are other discriminators that can be applied such as: pen pressure, number of times the pen was not touching the tablet. The results for off-line signature and on-line signature using fuzzy vault are displayed in Table I. The more recent results for online signature, ([4]) show poorer performance than those for off-line signatures but they are also acceptable results.

In table I some other interesting results are those from the study of Kumar et al [11] which implemented a fuzzy based algorithm and tested it across databases that contained biometrics from different categories. More exactly, they tested them against finger print, palm print, iris, hand vein. It is an interesting approach as in general in every paper only one category of biometrics is exploited and looked at. As per the results gathered, we can see that the two candidates for the best results are the ones obtained for palm print and iris. The palm print offers a more usable system than the case where this method is used for iris but less secure. On the other hand, from all the results, the most secure system is guaranteed by the case where the iris is used as a method to authenticate because it gives the lowest FAR and the highest FRR (Table I).

An multi-biometric system approach is given in [15] where the authors make use of the fuzzy vault algorithm as it was firstly presented in the original paper to prove that if the methods is applied on a combination of biometrics (fingerprint, iris, finger vein) the FAR and FRR show better values than in the case where these mentioned biometric information were used individually. We can see the results in Table I.

As far as Table I, we can conclude that in general the fuzzy vault techniques developed focus more on ensuring high levels of security given that, as a whole, there are better results in terms of FAR. The winner of the results seems to remain Hao et al with their Hadamard and Reed-Solomon error correcting techniques which succeed in obtaining a FAR rate equal to 0 and a FRR smaller than 0.5.

C. Test Results

In our paper we propose a testing framework for the publicly available implementation of the fuzzy vault technique aimed at protecting fingerprint templates proposed by Tams in [23]. They also inspire their work from the pioneers of the fuzzy scheme, Juels and Sudan. We will make a performance evaluation of their work by using the FVC 2002 DB1_B database of fingerprint templates. FVC represents the the Second International Competition for Fingerprint Verification Algorithms. The database used contains ten fingers each having 8 samples (a total of 80 fingerprint samples).

We tested it on a laptop environment running at a 2.3Ghz frequency, having an Intel I5 core processor inside and 8GB of RAM available. The code is written in C language and the testing framework was written using shell scripting (bash). Another MATLAB script is used in order to convert the images from 'tiff' format (which is the publicly available format of the FVC DB1_B database.

The testing framework gives us the possibility to also vary the degree of the secret polynomial which is correlated to the minutiae extracted from the fingerprint. In order to calculate the FAR we created a vault with all 8 fingers using a single image per finger (enrollment phase). In order to verify, we give as input all the other 7 left images, so in total we make 10 (fingers) * 7 (samples per fingers for verification) = 70 iterations (legitimate access intents). As far as calculating the FRR, we permuted to the right the images. We tested it with permutation to one, two and three distances away from the initial position for every fingerprint image and tested every position with the whole remaining bunch of images per finger (7). The implementation available offers support for varying the degree of the polynomial used and we varied it to 7, 10 and 12. The results can be seen in Table II.

TABLE II
EXPERIMENTAL RESULTS FOR FUZZY VAULT TECHNIQUE ON FVC DB1_B

Degree of polynomial	FAR	FRR
7	0.37%	0.47%
10	0.02%	0.08%
12	0.0%	0.12%

We can observe that in this case also we obtained that security is preferred over convenience as we obtained better results for the FAR column. We can also deduce from this that the greater the degree gets the more accurate the system becomes which is normal for fuzzy vault method as the

greater the polynomial, the chaff points inserted are less influential.

IV. Conclusion

In this paper we presented various techniques of enhancing the security of information systems by looking at ways of using biometric and cryptography techniques combined. We looked at this problem from a two way perspective by presenting the main threats for these two concepts and the proposed solutions over the course of time. We also presented the theoretical basis of measuring the performance of a biometric system. We decided to dive deeper into the fuzzy vault popular method of encrypting a secret using biometrics and used it as a base to show performance results obtained over the time in terms of FAR and FRR.

V. Acknowledgment

This work has been funded by University Politehnica of Bucharest, through the Excellence Research Grants Program, UPB GEX. Identifier: UPBEXCELENTA2016 Research project title, Contract number 22/26.09.2017 (acronym: 406).

References

[1] Is Alice. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 2003.

[2] Ruud M Bolle, Jonathan Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. *Guide to biometrics*. Springer Science & Business Media, 2013.

[3] Brian Chen and Gregory W Wornell. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4):1423–1443, 2001.

[4] Md Jahid Faruki, Ng Zhi Lun, and Syed Khaleel Ahmed. Handwritten signature verification: Online verification using a fuzzy inference system. In *2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, pages 232–237. IEEE, 2015.

[5] Hao Feng and Chan Choong Wah. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(4):159–164, 2002.

[6] Feng Hao, Ross Anderson, and John Daugman. Combining crypto with biometrics effectively. *IEEE transactions on computers*, 55(9):1081–1088, 2006.

[7] Jesse Hartloff, Maxwell Bileschi, Sergey Tulyakov, Jimmy Dobler, Atri Rudra, and Venu Govindaraju. Security analysis for fingerprint fuzzy vaults. In *Spie Defense, Security, and Sensing*, pages 871204–871204. International Society for Optics and Photonics, 2013.

[8] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[9] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36. ACM, 1999.

[10] Przemysław Kudłacik and Piotr Porwik. A new approach to signature recognition using the fuzzy method. *Pattern Analysis and Applications*, 17(3):451–463, 2014.

[11] Amioy Kumar, M Hanmandlu, and Hari M Gupta. A new scheme for the polynomial based biometric cryptosystems. *ISRN Machine Vision*, 2014, 2014.

[12] Jean-Paul Linnartz and Pim Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 393–402. Springer, 2003.

[13] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging 2002*, pages 275–289. International Society for Optics and Photonics, 2002.

[14] Karthik Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *2010 IEEE International Workshop on Information Forensics and Security*, pages 1–6. IEEE, 2010.

[15] Karthik Nandakumar and Anil K Jain. Multibiometric template security using fuzzy vault. In *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*, pages 1–6. IEEE, 2008.

[16] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007.

[17] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3):614–634, 2001.

[18] Christian Rathgeb and Andreas Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *Visual Information Processing (EUVIP), 2010 2nd European Workshop on*, pages 41–44. IEEE, 2010.

[19] SHIN Sanggyu and Shogo SHIMIZU. A study of cancelable biometrics in the security improvement of biometric authentication system using fault tree analysis. *International Journal of Affective Engineering*, 15(4):351–359, 2016.

[20] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[21] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and Bhagavatula Vijaya Kumar. Biometric encryption using image processing. In *Photonics West'98 Electronic Imaging*, pages 178–188. International Society for Optics and Photonics, 1998.

[22] Shenghui Su and Shuwang Lü. A public key cryptosystem based on three new provable problems. *Theoretical Computer Science*, 426:91–117, 2012.

[23] Benjamin Tams. Attacks and countermeasures in fingerprint based biometric cryptosystems. *arXiv preprint arXiv:1304.7386*, 2013.

[24] George J Tomko, Colin Soutar, and Gregory J Schmidt. Fingerprint controlled public key cryptographic system, July 30 1996. US Patent 5,541,994.

[25] R Valarmathi, S Sridevi Sathiya Priya, P Karthigai Kumar, and NM SivaMangai. A biometric encryption using face recognition system for watch list. In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, pages 1–5. IEEE, 2014.