Balancing is the Key
Performing Finger Vein Template Protection using Fuzzy Commitment

Mélanie Favre[1], Sylvaine Picard[2*], Julien Bringer[1] and Hervé Chabanne[1,3]
[1]*Morpho, Issy-les-Moulineaux, France*
[2]*Safran, Magny-les-Hameaux, France*
[3]*Télécom ParisTech, Paris, France*

Keywords: Fuzzy Commitment, Finger Vein, Product Codes, Template Protection Scheme.

Abstract: We propose a novel vein extraction technique adapted to template protection and use it to apply a fuzzy commitment scheme. We construct dedicated error correcting codes that enable us to maintain a good accuracy after template protection. In a second application, we offer to overcome the alignment issues when comparing two vein templates by performing this step outside of the protection scheme. Different implementations are proposed to explore trade-offs between False Rejection Rate, False Acceptance Rate, comparison time and security. All approaches are tested on the recent database of University of Twente from ICB 2013. Our biometric performances are close to state of the art approaches whilst bringing security with the template protection scheme.

1 INTRODUCTION

Biometrics provide a reliable and convenient way of individual authentication. The use of physical traits has the advantage that they cannot be lost or forgotten. However, the storage of biometric templates may lead to security and privacy issues. In order to thwart these problems, different solutions for privacy protection have been proposed (ISO, 2011). A first set of techniques is to protect the template with a template-level transformation, often denoted by biometric template protection. This can offer a first layer of security without impacting too much the system. More robust security protection will rely on more complex architectures that work at the system level (not restricted to the template-level). The underlying idea of the template-level approach is to derive a protected version of the enrolled biometric template and to store it instead of the first one. The transformation mechanism is considered as public and it must be difficult to reconstruct the template from the protected one without the genuine user's biometric data. The level of difficulty that one can achieve is very often dependent on the difficulty to reverse the transformation and the difficulty to find a matching template. That motivates us to find a good trade-off between false positive rate and reversibility.

Among the well known biometric template protection schemes there are the fuzzy commitment scheme (Juels and Wattenberg, 1999) and the fuzzy vault scheme (Juels and Sudan, 2006). Both approaches commit to a secret value under a noise-tolerant key. The first scheme deals with fixed-length binary keys while the latter is able to deal with unordered sets. First introduced in (Juels and Wattenberg, 1999), the fuzzy commitment scheme binds a binary biometric template to a random codeword. The idea is to overcome the biometric variance by means of error correction. The error correction capacity has to coincide with the chosen threshold deliminating intra and inter-class variance. The fuzzy commitment scheme has been applied to many different biometric modalities and representations: a survey can be found, for instance, in (Rathgeb and Uhl, 2011). We propose in this paper to use it with finger vein biometrics. An attempt on backhand vein has been carried out in (Hartung and Busch, 2009) and fuzzy commitments has also been applied on finger vein in (Yang et al., 2013), but after a first bio-hashing step (that relies on a secret parameter). Our approach deals with non-hashed finger vein templates. Note that the security evaluation of the fuzzy commitment scheme is still an open problem despite recent proposals (see for instance (Simoens et al., 2012)). However, this work

*Work done during employment at Morpho

Favre M., Picard S., Bringer J. and Chabanne H..
Balancing is the Key - Performing Finger Vein Template Protection using Fuzzy Commitment.
DOI: 10.5220/0005241403040311
In *Proceedings of the 1st International Conference on Information Systems Security and Privacy* (ICISSP-2015), pages 304-311
ISBN: 978-989-758-081-9

has not the ambition of bringing new elements on its security, but rather to focus on showing how to apply efficiently the fuzzy commitment scheme to finger vein biometrics.

To do so, it is necessary to take a closer look at the manner vein information is represented and compared. Since Miura *et al.* publications (Miura et al., 2004) (Miura et al., 2007), vein feature extraction and vein recognition problems have generated an increasing interest among the biometrics research community. However, finger vein recognition is still a recent research field. Therefore research about a fundamental stage for recognition systems like feature extraction is still vivid. Different strategies have been proposed, for example, local representation with SIFT (Ladoux et al., 2009) and minutiae (Yu et al., 2009). To be well suited for fuzzy commitment scheme, an interesting characteristic for vein recognition is to allow comparison with the Hamming distance. Several papers are interesting from this point of view. For example, Lee *et al.* use in (Lee et al., 2010) a 50 x 20 LBP coded vector to characterize a finger. Comparison is done thanks to a weighted Hamming distance. In (Zhou and Kumar, 2010), Zhou and Kumar use different representations for palm vein recognition: Multi-scale local vesselness based on Hessian eigenvalues, Localized Radon Transform and Ordinal representation. In this case again, the comparison of these representations is based on the Hamming distance. Finally, Hartung *et al.* in (Hartung et al., 2011; Hartung et al., 2012) adapt Spectral Minutiae (Xu et al., 2009) to backhand vein recognition with encouraging performances. In this work, we propose a novel vein extraction technique and novel error correcting code constructions to reach a very good ratio between accuracy and security.

This article is structured as follows. In section 2 we give a brief overview of vein extraction techniques, we introduce an efficient technique to derive binary templates that can be compared via Hamming classifier, and we describe the database we used for our experiments. Section 3 details the modalities of the fuzzy commitment as we applied it, and the way we chose the underlying error correcting codes while section 4 presents the experiments we carried out. Finally, section 5 concludes our study.

2 VEIN BIOMETRICS

2.1 Vein Extraction for Template Protection

In the context of template protection, it is necessary to adapt data representation to get an effective protection scheme and minimize information leaks. To do so, some methods have already been proposed ((Hartung et al., 2011), (Fuksis et al., 2011), (Hirata and Takahashi, 2009)). With the fuzzy commitment scheme, one very important point is to provide templates that can be compared with the Hamming distance. However, guaranteeing *Hamming-wise* comparison is not enough to provide a good data representation. Security analysis shows that it is also necessary to be careful in order to make attacks by false acceptance or brute force difficult.

In general, vein acquisition systems reveal only main vessels. Therefore, the main part of finger vein images is made of *background*, that means none vessel information. If vein extraction precisely respects vessels net, then extracted templates will present a majority of black pixels. In a biometrics recognition context it is not a problem. In the context of template protection this bias facilitates attacks. Indeed, fake templates with a majority of black pixels would take advantage of this bias reducing the distance between a protected template and themselves.

To eliminate this problem, we propose a quite counter-intuitive scheme: do not respect the real vessel information! We propose to make sure that vein templates contain as much as possible an equal number of white and black pixels. This way, we go a step closer to random data. Our solution can be applied to different vein extraction methods. Moreover it does not need to use several templates as input for balancing the white and black pixels: the algorithm is made to work with one image to be compatible with single-image enrollment schemes.

Let I be the vein image, $E_v(I)$ the extraction function. The only requirement on E_v is to be a continuous and smooth function on $[0,255]$. Then, template T is constructed as follows:

$$T(x,y) = \begin{cases} 1 & if \quad E_v(x,y) \geq thresh \\ 0 & if \quad E_v(x,y) < thresh \end{cases} \qquad (1)$$

Where *thresh* is chosen for each image I in order to get the number of 1 and the number of 0 as close as possible in T. That is to say *thresh* is the median of $E_v(x,y)$. It is clear that some pixels set to one do not represent finger vein. This is a consequence of

balancing the template. As stated earlier, this rule can be applied to any continuous E_v function, for example for some 2D adaptation of (Frangi et al., 1998) or any continuous operator mentioned above. In this article we use a proprietary function E_v based on a rough modelisation of finger veins.

2.2 Vein Database Description

The lack of public database has been a problem up to now. Fortunately, some databases are now available ((Kumar and Zhou, 2012), (Ton and Veldhuis, 2013)), and hopefully some more should be available in the future. For this experiment, we work with UTFVP database from University of Twente (Ton and Veldhuis, 2013). These data represent 60 person's 6 fingers (index finger, middle finger, and annular finger of both hands). Data were acquired during two different sessions allowing four acquisitions by finger. In general, image quality is good.

Image resolution is 126 pixels per centimeter (ppcm). In order to work with a compact representation of finger veins, we downsample the images by a factor of 5 in each dimension. Finger's outlines are easily computed using gradients of the image. Some finger orientation correction is done by computing finger principal axis and performing a rotation in order to get it horizontal. Then, to code reference finger images we use a 100 $\times$ 30 finger area centered on the middle of the image which corresponds roughly to the middle phalanx. This zone is usually described as the most stable and the most discriminant area for finger vein recognition. Figure 1 shows a finger from Twente database and its corresponding balanced encoded version.

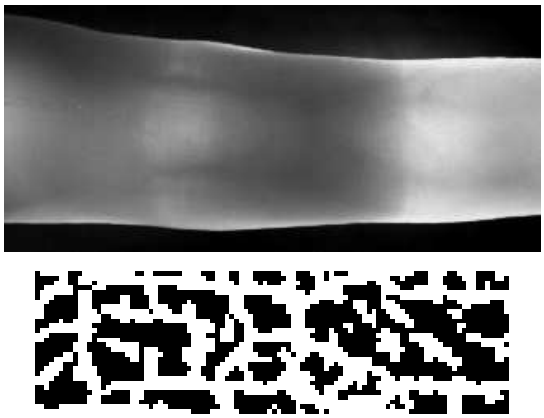

Figure 1: Finger vein from Twente database and its corresponding balanced coding.

For query images we use a 128 $\times$ 44 area centered on the middle of the image. We use this a priori positioning because finger position is quite stable between two acquisitions. In the case of a bitwise comparison, different sizes of coding areas for query images and reference images allow to absorb small translations. For example, during the comparison stage, it is possible to move the reference template over the search template to find the highest matching score position. When relative finger positions can vary a lot, Yang has proposed in (Yang and Li, 2010) to detect phalanges position in order to determine the region of interest for coding. In our tests, only small translations between query and reference images can be handled.

To estimate accuracy of our finger vein coding, we perform authentication tests without template protection. That is, we evaluate the amount of different pixels in the common area of 100 $\times$ 30 between reference and verification templates. We test different positions and keep the one corresponding to the smallest distance. For each finger we use the first image as a reference, and two images, acquired during second acquisition session, for the query images. The results are summarized in table 1, while figure 2 gives an overview of the distances we have to deal with.

Table 1: Performances without template protection.

Nb Gen. Tests	Nb Imp. Tests	EER (%)	FRR (%) @FAR10^{-4}	FRR (%) @FAR10^{-5}
720	258480	0.56	2.22	3.89

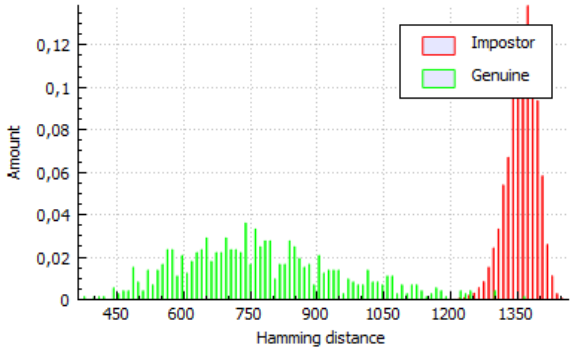

Figure 2: Hamming distances.

Despite constraints on the coding strategy due to our motivation to apply fuzzy commitment, our EER is close to the best EER described in (Ton and Veldhuis, 2013), that is 0.4%.

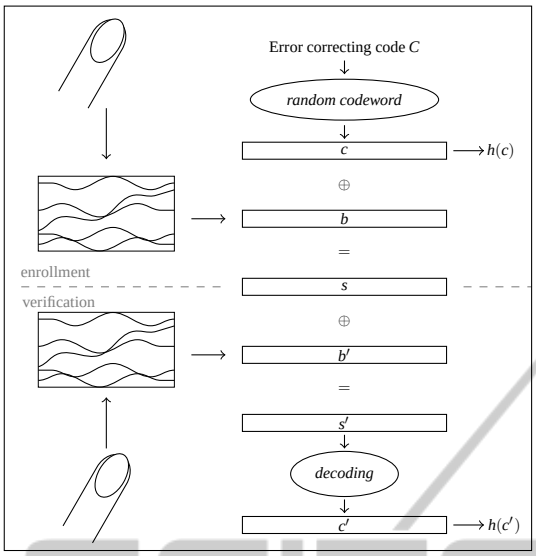

Figure 3: Fuzzy Commitment scheme.

3 FUZZY COMMITMENT

3.1 Background

Before detailing how the fuzzy commitment works, we give a brief recall on error-correcting codes. The goal of these primitives is to transmit a message m over a noisy channel. To do so, the message is mapped before transmission to a bigger data string c - called *codeword* - containing redundant information. This way, if some limited parts of c are corrupted during transmission, c can be reconstructed through a decoding algorithm, and therefore also m. More formally, a linear binary error-correcting code C is denoted by $[n,k,d]$ where k is the original size of the message called *dimension*, n the size of the redundant string called *length* and d denotes the smallest Hamming distance between two codewords of C. The correction capacity of C is bounded by $(d-1)/2$.

The fuzzy commitment scheme applied to biometrics demands a binary fixed-length biometric template b that is masked by a random codeword c to form a *protected* template $s = b \oplus c$. Meanwhile, the hash value $h(c)$ is stored together with s. During authentication, a fresh biometric template b' is presented and XORed with s to get $s' = b' \oplus s = b' \oplus b \oplus c$. Decoding algorithm is applied on s' to get a codeword c'. If b and b' are within a certain thresholding in terms of Hamming distance, then $c' = c$ which can be checked by $h(c') = h(c)$. Figure 3 depicts the whole process.

An upper bound for the security of the fuzzy commitment is given by the dimension k of the error-correcting code used, as it gives the amount of information of the key bound to the biometric template b. Many more sophisticated security analysis of the scheme have been carried out, see for instance (Stoianov et al., 2009; Ignatenko and Willems, 2010; Smith, 2004; Tuyls and Goseling, 2004). Most weaknesses come from the non uniform distribution of errors in the biometric templates. The use of balanced black and white vein templates limits this point. The scheme is also subject to false acceptance attacks (see for instance (Korte and Plaga, 2007)). As soon as an impostor manages to authenticate, the codeword bound to the template is retrieved (and consequently the original template b as well). False acceptance rate should thus remain low in order to limit this threat. The use of a soft-decoding algorithm instead of a classical decoding algorithm may also lead to increased false acceptances as it enables to decode more errors. Finally, cross-matching and decodability attacks have been studied (Simoens et al., 2009; Kelkboom et al., 2011). Here we focus on the two main issues that are the dimension of the code and the false acceptance rate (FAR). In particular, we aim a quite low FAR, that is set to be approximately between 10^{-4} and 10^{-5}.

3.2 Our Construction Choices

The choice of the error-correcting code has to be done regarding the amount of errors one has to deal within the biometric setting. Thus, we measured the distance corresponding to roughly 0.001% of false acceptance on Twente database. It turned out that we have around 36% of different pixels in this case.

In order to overcome this error rate, we have chosen to use product codes in our scheme. Product codes are a class of error-correcting codes constructed from two or more subcodes. $C = C_1[n_1,k_1,d_1] \times C_2[n_2,k_2,d_2]$ is a $[n_1n_2,k_1k_2,d_1d_2]$ code whose codewords can be seen as $n_2 \times n_1$ matrices whose columns are codewords from C_2 and rows codewords from C_1. When k_1 and k_2 are small enough, the *min-sum* algorithm (Tanner, 1981) can be used to decode product codes in a very efficient way. It is an iterative process that associates two scores between 0 and 1 at each element of the matrix. These values represent the costs to put the element to 0 (resp. to 1). Scores are initialized regarding the word to be decoded and are improved iteratively. At each iteration, the algorithm looks for the codeword that costs the least. The error correction capacity of the min-sum algorithm is assured to be $d_1d_2/2$ if two iterations are performed but it can go much further in practice. For our experiments, we have limited the amount of iterations to five, as it is a good compromise between error correction and execution time. Finally, product codes can be composed

of more than two subcodes in a straightforward manner. The decoding process is then a less direct adaptation, details can be found in (Wu et al., 2007), but we use the most intuitive approach.

Min-sum decoding along with product codes have been successfully applied in fuzzy commitment schemes with iris and fingerprint in (Bringer et al., 2008; Bringer et al., 2007). We follow these examples by choosing product codes with similar properties, that is permitting to reach the lowest possible false rejection rate in the Shannon sense (Shannon, 2001). But we go a step further and use for the first time in this kind of setting product codes of dimension 3 and 4 in order to achieve a good trade-off between execution time, code dimension and error correction capacity. In fact, subcodes with good qualities (weight distribution, correction capacity) are often codes with n a power of two. The product codes we tested are composed of repetition codes and of order 1 Reed-Muller codes (Muller, 1954; Reed, 1954) which are known to have good weight distributions. As we have 3000 pixels in each template, we have chosen to use an area of 2048 pixels to perform the fuzzy commitment scheme. The choice of these pixels has been done regarding the areas in pictures less impacted by errors. As stated in section 2.2, the middle of the phalanx is more stable, we thus naturally evinced pixels on the horizontal borders. Our area of interest is roughly the 68×30 central zone of each picture.

4 EXPERIMENTS

4.1 Fuzzy Commitment with One Reference Template

Traditionally, vein comparison consists in testing many translations of one template on the other in order to find the best one corresponding to the smallest amount of different pixels. In our setting, we test up to 225 translations. To apply a fuzzy commitment in this case, we need to perform as many decodings as tested translations (but we can stop if one decoding is correct).

4.1.1 Using an Interleaving

The error repartition inside a finger vein picture is not random, there is a correlation between neighboring pixels. We have thus introduced a random permutation, as a way to interleave the pixels, that we apply on the 2048 bits extracted from the template. This way, the efficiency of the min-sum decoding algorithm is increased and we were able to decode further than without the permutation. Note that the permutation is not a secret, it is just introduced to enhance the decoding capacity of the min-sum algorithm in our setting. Moreover, the use of a permutation allows to be resistant against cross-matching and decodability attacks.

4.1.2 Tests and Performances

For our tests, we used the first image of each finger as reference template and used third and fourth images for verification. This leads to 259,200 comparisons, among them 720 are genuine. Table 2 sums up the performances we were able to reach. Execution timings include the 225 decodings. Our experiments were run on a computer with a 3.3GHz Intel Core i5 processor and 8GB of RAM. Compared to the biometric performances presented in section 2.2, our results are degraded. This comes mainly from the fact that we use only two thirds of the pictures. We can also remark that the dimension of the error correcting codes can reach 50 bits.

Table 2: Performances of the fuzzy commitment scheme with one reference template (2048 bits).

Error correcting code	Dim. (bits)	FAR (%)	FRR (%)	Exec. (ms)
RM(4,1)×RM(5,1)×[4,1,4]	30	0.01	4.31	560
[8,2,4]×RM(4,1)×RM(4,1)	50	0.03	3.05	350

4.2 Using a Second Reference Template

In order to improve the biometric performances, and especially reduce false acceptance rates, we propose to enroll a second reference template and impose to match against both templates to authenticate. To overcome the alignment problem that would soar the amount of decodings with two templates, we additionally introduce a way to perform alignment before the commitment scheme itself.

Just as Uludag *et al.* used a helper data to perform alignment of fingerprints before a fuzzy vault scheme in (Uludag and Jain, 2006), we use a part of the biometric templates to best overlap them. To do so, we separate each reference template into distinct areas. We extract a small central zone of 276 pixels that is stored in clear and used later to evaluate the optimal translation – but only for that purpose as a second and **distinct** part of 2048 pixels is used to perform the fuzzy commitment itself. We concatenate the two 2048-pixel areas of both templates to form a 4096-bit word that we bind to a codeword just as before. The stored template contains now 2×276 pixels in clear and a 4096-bit protected string. Again, we

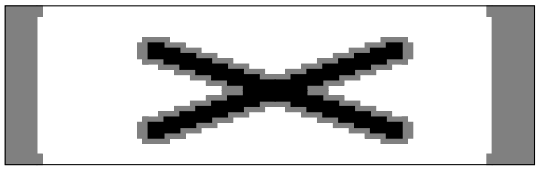

Figure 4: Choice of the areas: in black the alignment area, in white the code zone (used for the fuzzy commitment) and in gray unused pixels.

use a random permutation in order to break the correlation between neighboring pixels.

Figure 4 depicts the image dividing as we performed it. We chose a cross form for the alignment part in order to be able to absorb the different translations we have to test.

During authentication, we first use the two alignment areas from the reference templates to find the best translations inside the freshly acquired image. We then extract the two corresponding areas of 2048 pixels to form a 4096-bit template that is XORed with the secure template stored in the database. Finally, the result of this is decoded. Again, we limit the min-sum algorithm to five iterations.

4.2.1 Performances

We used the two first images of each finger for enrollment and the same two last images as before for verification. The amount and nature of tests stay thus unchanged.

Table 3 depicts our secure sketch results in term of biometric accuracy, code dimension and execution time. We propose two error-correcting codes that permit to achieve low false acceptance rates whilst remaining quite accurate. The execution time is also drastically reduced, as we have only one decoding to perform. The key size is also improved but is limited to 64 bits due the amount of errors to correct that is rather high.

Table 3: Performances of the fuzzy commitment scheme with two reference templates (4096 bits).

Error correcting code	Dim. (bits)	FAR (%)	FRR (%)	Exec. (ms)
RM(6,1)×RM(6,1)	49	0.0035	2.92	11
[8,2,4]×[8,2,4]×RM(3,1)×RM(3,1)	64	0.0023	3.33	2.1

Compared to the biometric performances presented in section 2.2, we are able to get the same performances with two reference templates instead of one in section 2.2.

4.2.2 Security of the Scheme

Intuitively, the use of the central alignment area in clear leads to information leakages. Veins have some predictable patterns, mostly horizontal lines, that could be exploited in order to guess some pixels of the code zone knowing the alignment area. We have estimated the leakage coming from the alignment zone by measuring the correlation between neighboring pixels in the whole database. Table 4 shows the result of our measures. As we can see, there is a higher horizontal correlation than the vertical one. The correlation is quite high for the pixels at distance one in any direction and it stays high for the the pixels at distance two horizontally (thick, blue values in the table). We have therefore chosen to surround the alignment area by a security zone (kind of DMZ) of one pixel vertically and two pixels horizontally (see the gray zone around the cross in Figure 4). This reduces the possibility to exploit the information coming from the alignment area. We remove the most predictable pixels of the code zone, knowing the helper data, in order to limit the information leakage. However it is clear that this approach is a trade-off between execution time and security.

Table 4: Pixel correlation for different distances in Twente database.

dy \ dx	-3	-2	-1	0	1	2	3
-3	-0.11	-0.10	-0.10	-0.09	-0.11	-0.11	-0.11
-2	-0.02	0.03	0.09	0.11	0.07	0.01	-0.03
-1	0.13	0.27	**0.42**	**0.51**	**0.41**	0.25	0.12
0	0.21	**0.41**	**0.67**	1.00	**0.67**	**0.41**	0.21
1	0.12	0.25	**0.41**	**0.51**	**0.42**	0.27	0.13
2	-0.03	0.01	0.07	0.11	0.09	0.02	-0.02
3	-0.11	-0.11	-0.11	-0.09	-0.10	-0.10	-0.11

Our scheme, like any fuzzy commitment scheme, is vulnerable to false acceptance attacks. We manage to keep the false acceptance rate low in order to limit the threat. Considering the code [8,2,4]×[8,2,4]×RM(3,1)×RM(3,1), if an attacker has access to a protected template, we would need a database of around 45000 vein templates in order to statistically decode it by false acceptance.

As stated in sections 4.1 ans 4.2, we limited our experiments to five min-sum iterations for the decoding. But an attacker could try more iterations in order to decode further. We have evaluated the potential of this threat by studying the execution of the fuzzy commitment with the code [8,2,4]×[8,2,4]×RM(3,1)×RM(3,1). We increased the number of iterations to 10 and measured the difference: execution time grows to 3.5ms while FAR

stays almost stable with 0.0035%. In fact, more than 20% of impostor comparisons already lead to a successful decoding with five min-sum iterations, but the codeword found was not the right one (it is the hash comparison $h(c) = h(c')$ that lead to a reject). Increasing the amount of iterations seems to have a poor impact on the true decoding capacity. We thus expect the possible gain for an attacker to test more min-sum iterations to be small.

5 CONCLUSION

In this paper, we apply a fuzzy commitment scheme with finger vein biometrics. An adaptation of vein encoding is proposed making vein template privacy protection techniques efficient and more secured. The idea is to get a binary template with an equal number of black and white pixels. This reduces efficiently the risk of successful attacks. Moreover, it is very general and can be applied to any continuous vein extraction function. We also manage to pass over the alignment problem by performing this step outside of the protection scheme. Doing so, we limit information leaks by analyzing their potential and adapting the coding area. We show how to increase accuracy and code dimension using two reference templates. Although the fuzzy commitment scheme is inherently sensitive to false acceptance attacks as any template-level protection technique, our biometric performances are pretty competitive with FAR close to 10^{-5} and thus ensuring a first layer of security through a template protection scheme. Finally, but not least, the comparison times we obtain are compatible with realistic use cases.

ACKNOWLEDGEMENTS

This work has been partially funded by the European FP7 BEAT project (SEC-284989).

Authors would like to thank Raymond Veldhuis for making the UTFVP database available for their research work.

REFERENCES

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., and Zémor, G. (2007). Optimal iris fuzzy sketches. In *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, pages 1–6. IEEE.

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., and Zémor, G. (2008). Theoretical and practical boundaries of binary secure sketches. *Information Forensics and Security, IEEE Transactions on*, 3(4):673–683.

Frangi, A. F., Niessen, W. J., Vincken, K. L., and Viergever, M. A. (1998). Multiscale vessel enhancement filtering. In *Medical Image Computing and Computer-Assisted Interventation-MICCAI'98*, pages 130–137. Springer.

Fuksis, R., Kadikis, A., and Greitans, M. (2011). Biohashing and fusion of palmprint and palm vein biometric data. In *Hand-Based Biometrics (ICHB), 2011 International Conference on*, pages 1–6. IEEE.

Hartung, D., Aastrup Olsen, M., Xu, H., Thanh Nguyen, H., and Busch, C. (2012). Comprehensive analysis of spectral minutiae for vein pattern recognition. *Biometrics, IET*, 1(1):25–36.

Hartung, D. and Busch, C. (2009). Why vein recognition needs privacy protection. In *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, pages 1090–1095. IEEE.

Hartung, D., Olsen, M. A., Xu, H., and Busch, C. (2011). Spectral minutiae for vein pattern recognition. In *Biometrics (IJCB), 2011 International Joint Conference on*, pages 1–7. IEEE.

Hirata, S. and Takahashi, K. (2009). Cancelable biometrics with perfect secrecy for correlation-based matching. In *Advances in Biometrics*, pages 868–878. Springer.

Ignatenko, T. and Willems, F. M. (2010). Information leakage in fuzzy commitment schemes. *Information Forensics and Security, IEEE Transactions on*, 5(2):337–348.

ISO (2011). Standard iso/iec 24745:2011. information technology – security techniques – biometric information protection.

Juels, A. and Sudan, M. (2006). A fuzzy vault scheme. *Des. Codes Cryptography*, 38(2):237–257.

Juels, A. and Wattenberg, M. (1999). A fuzzy commitment scheme. In Motiwalla, J. and Tsudik, G., editors, *ACM Conference on Computer and Communications Security*, pages 28–36. ACM.

Kelkboom, E. J., Breebaart, J., Kevenaar, T. A., Buhan, I., and Veldhuis, R. N. (2011). Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *Information Forensics and Security, IEEE Transactions on*, 6(1):107–121.

Korte, U. and Plaga, R. (2007). Cryptographic protection of biometric templates: Chance, challenges and applications. In Brömme, A., Busch, C., and Hühnlein, D., editors, *BIOSIG*, volume 108 of *LNI*, pages 33–46. GI.

Kumar, A. and Zhou, Y. (2012). Human identification using finger images. *Image Processing, IEEE Transactions on*, 21(4):2228–2244.

Ladoux, P.-O., Rosenberger, C., and Dorizzi, B. (2009). Palm vein verification system based on sift matching. In *Advances in Biometrics*, pages 1290–1298. Springer.

Lee, H. C., Kang, B. J., Lee, E. C., and Park, K. R. (2010). Finger vein recognition using weighted local binary pattern code based on a support vector machine. *Jour-*

nal of Zhejiang University SCIENCE C, 11(7):514–524.

Miura, N., Nagasaka, A., and Miyatake, T. (2004). Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Machine Vision and Applications*, 15(4):194–203.

Miura, N., Nagasaka, A., and Miyatake, T. (2007). Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE TRANSACTIONS on Information and Systems*, 90(8):1185–1194.

Muller, D. E. (1954). Application of boolean algebra to switching circuit design and to error detection. *Electronic Computers, Transactions of the IRE Professional Group on*, (3):6–12.

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

Reed, I. (1954). A class of multiple-error-correcting codes and the decoding scheme. *Information Theory, Transactions of the IRE Professional Group on*, 4(4):38–49.

Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55.

Simoens, K., Tuyls, P., and Preneel, B. (2009). Privacy weaknesses in biometric sketches. In *IEEE Symposium on Security and Privacy*, pages 188–203. IEEE Computer Society.

Simoens, K., Yang, B., Zhou, X., Beato, F., Busch, C., Newton, E. M., and Preneel, B. (2012). Criteria towards metrics for benchmarking template protection algorithms. In Jain, A. K., Ross, A., Prabhakar, S., and Kim, J., editors, *ICB*, pages 498–505. IEEE.

Smith, A. D. (2004). *Maintaining secrecy when information leakage is unavoidable*. PhD thesis, Citeseer.

Stoianov, A., Kevenaar, T., and Van der Veen, M. (2009). Security issues of biometric encryption. In *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference*, pages 34–39. IEEE.

Tanner, R. M. (1981). A recursive approach to low complexity codes. *Information Theory, IEEE Transactions on*, 27(5):533–547.

Ton, B. and Veldhuis, R. (2013). A high quality finger vascular pattern dataset collected using a custom designed capturing device. In *Biometrics (ICB), 2013 International Conference on*, pages 1–5. IEEE.

Tuyls, P. and Goseling, J. (2004). Capacity and examples of template-protecting biometric authentication systems. In *Biometric Authentication*, pages 158–170. Springer.

Uludag, U. and Jain, A. (2006). Securing fingerprint template: Fuzzy vault with helper data. In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on*, pages 163–163. IEEE.

Wu, X., He, Y., and Zhu, G. (2007). Performance of improved three-dimensional turbo product code decoder. In *Integration Technology, 2007. ICIT'07. IEEE International Conference on*, pages 563–567. IEEE.

Xu, H., Veldhuis, R., Bazen, A. M., Kevenaar, T. A., Akkermans, T. A., and Gokberk, B. (2009). Fingerprint verification using spectral minutiae representations. *Information Forensics and Security, IEEE Transactions on*, 4(3):397–409.

Yang, J. and Li, X. (2010). Efficient finger vein localization and recognition. In *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 1148–1151. IEEE.

Yang, W., Hu, J., and Wang, S. (2013). A finger-vein based cancellable bio-cryptosystem. In *Network and System Security*, pages 784–790. Springer.

Yu, C.-B., Qin, H.-F., Cui, Y.-Z., and Hu, X.-Q. (2009). Finger-vein image recognition combining modified hausdorff distance with minutiae feature matching. *Interdisciplinary Sciences: Computational Life Sciences*, 1(4):280–289.

Zhou, Y. and Kumar, A. (2010). Contactless palm vein identification using multiple representations. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, pages 1–6. IEEE.