TOWARDS GENERATING PROTECTED FINGERPRINT TEMPLATES BASED ON BLOOM FILTERS

Guoqiang Li[*], *Bian Yang*[*], *Christian Rathgeb*[†] *and Christoph Busch*[*†]

[*] Norwegian Information Security Laboratory at Gjøvik University College, Norway
[†] da/sec - Biometrics and Internet Security Research Group Hochschule Darmstadt, Darmstadt, Germany

ABSTRACT

In order to satisfy the requirements for security and privacy of biometric enrolment data records, it is essential to protect this reference data by applying appropriate template protection schemes. Bloom filters have been applied successfully on iris biometrics and face biometrics and achieved good result in terms of irreversibility and biometric performance. In this paper we study, whether it is feasible to employ Bloom filters on fingerprint templates. In order to be resilient with fingerprint sample variations, a pre-alignment process is applied prior to binary template generation. After generating the binary template matrix, we propose to subdivide the matrix and achieve a variable size of the binary template. Experiments were conducted on public databases to confirm the proposed ideas. According to experimental results, applying Bloom filters on fingerprint template doesn't degrade the accuracy of the fingerprint recognition system. Therefore, we can conclude that it is feasible to apply Bloom filters on fingerprint biometrics.

Index Terms— fingerprint recognition, template protection, Bloom Filters

1. INTRODUCTION

Fingerprint recognition has been widely adopted to authentication systems in order to verify the idenity claim of an individual. From the security and privacy perspective, securing the fingerprint reference data is essential because of the permanence properties of the biometric fingerprint characteristic. Unlike conventional passwords, which can be re-enrolled using a new password after leakage [1] this more challenging for biometric reference data. In addition, it has been proven that the original fingerprint information and potentially sensitive medical information can be reconstructed from a fingerprint template [2; 3]. Therefore, studying biometric template protection schemes has received increasing attention in the biometric community. In accordance with the international standard ISO/IEC 24745 [4], a biometric template protection method need to meet two major requirements:

This work is funded under grant agreement 284862 for the EU-FP7 large-scale integrated project FIDELITY.

- Irreversibility: it should be infeasible to reconstruct the original biometric template from the protected template;
- Unlinkability: different versions of protected templates can be generated from one and the same sample should not match.

A variety of biometric template protection schemes have been proposed in literature. These approaches can be roughly classified into two categories: biometric cryptosystem and cancelable biometrics (also refers to feature transformation) [5]. The idea of biometric cryptosystem is to protect or retrieve the cryptographic key by using biometric data. The comparison process is operated by verifying the hash result of extracted key against stored hash data. There are two types of fingerprint cryptosystems, which are based on fuzzy vault [6; 7] and fuzzy commitment [8] respectively. The majority of these approaches require some public information (called the helper data) to properly align fingerprint samples, which is critical and challenging to achieve.

Ratha et al .[9] promoted the concept of cancelable biometrics, which can meet the two requirements of irreversibility and unlinkability. The idea of cancelable biometrics is to generate as many protected template (or called transformed template) as needed by issuing a new transformation key, and the comparison process can be operated on transformed templates. Researchers [10; 11; 12] have employed this concept to generate cancelable fingerprint templates. However, these approaches caused a significant degradation in biometric performance. Another feature transformation approach based on minutia cylinder-code representation [13] achieved good performance, but it doesn't guarantee the unlinkability.

Bloom filters has been introduced in the field of research, deriving an iris template protection scheme by Rathgeb et al. [14; 15]. The irreversibility can be guaranteed by mapping multiple codewords to an identical position, and unlinkability based on application-specific secret are current research topics with promising results [14]. Since applying Bloom filters on iris templates and also on face templates is feasible, it inspired us to investigate the application of Bloom filters on fingerprint templates. Comparing to iris template whose size is fixed, the size of a fingerprint template is generally

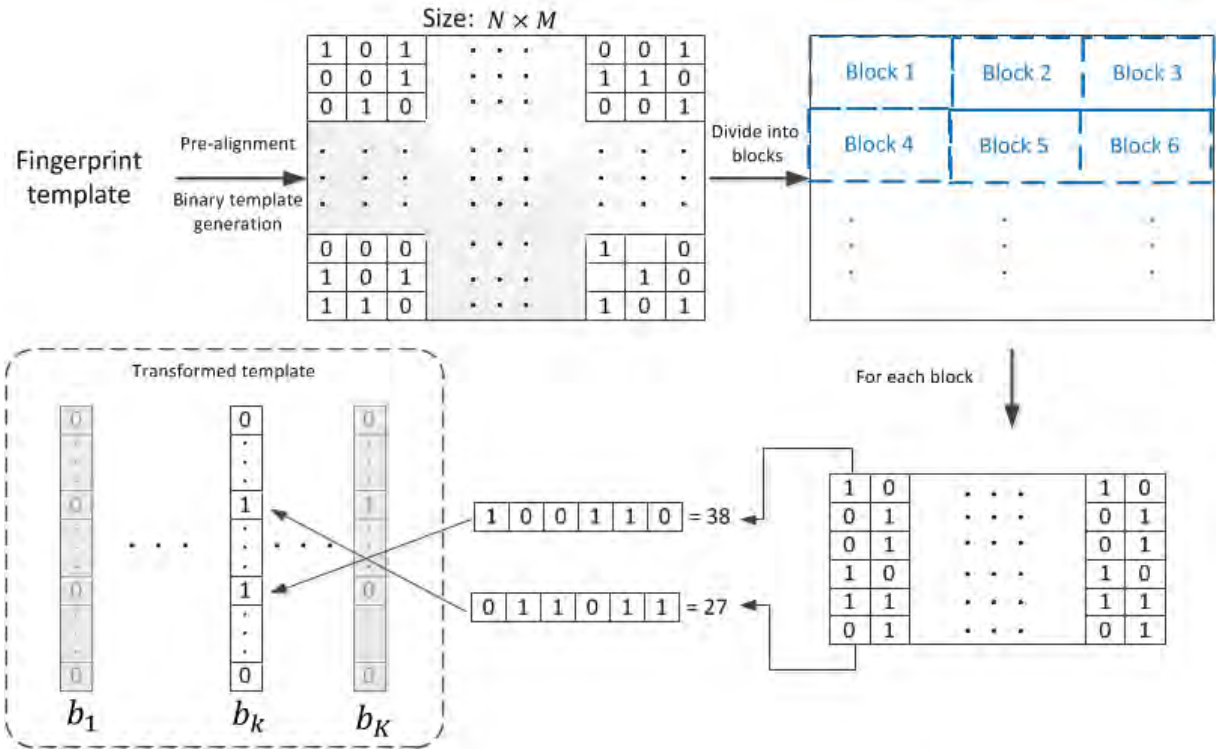

Fig. 1: The process of transformed template generation by applying Bloom filters on fingerprint template

variable and large. This presents a challenge to apply Bloom filters on fingerprint template. In this paper, we addressed this challenge and explore introducing the concept of Bloom filters on fingerprint templates. The remainder of this paper is organized as follows: Section 2 describes the details of pre-alignment, binary template generation and the mapping to Bloom filters; the experimental results of performance evaluation are reported in Section 3. Section 4 discusses future works and concludes this paper.

2. APPLYING BLOOM FILTERS TO FINGERPRINT

As we mentioned earlier, the purpose of cancelable biometrics is to transform the fingerprint template into a protected domain where the matching process can take place. Fig. 1 illustrates the process of generating this transformed template by applying Bloom filters on fingerprint template. The first step of proposed approach is a fingerprint pre-alignment module where only minutiae which are located in a circle will be used for the binary template generation as shown in Fig.2. The reason for adding this pre-alignment module is that the minutiae included in the circle are more robust and reliable than the minutiae closed to border during the fingerprint sample acquisition. The circle's radius r is adjustable according to the resolution of fingerprint sample. The centre point (C_x, C_y) of this circle is the reference point of each sample image. This reference point can be efficiently detected by using a simple rule:

- (1) if only one core point is detected by fingerprint template extractor (we chose NeuroTechnology Verifinger 6.0 extractor [16], this core point will be considered as reference point;
- (2) if multiple core points are extracted, the uppermost core point will be chosen as reference point;
- (3) if the extractor doesn't detected any core point, then the reference point will be calculated using equation (1)-(2).

$$C_x = \min(m_{(i,x)}) + \frac{\max(m_{(i,x)}) - \min(m_{(i,x)})}{2} \quad (1)$$

$$C_y = \min(m_{(i,y)}) + \frac{\max(m_{(i,y)}) - \min(m_{(i,y)})}{2} \quad (2)$$

where $m_{(i,x)}$ is the X coordinate of minutia m_i and $m_{(i,y)}$ is the Y coordinate of minutia m_i.

After fingerprint alignment, the proposed approach adapted the binary generation scheme developed by Yang [17]. Fig. 3 depicts the procedures of this scheme which will output a binary template with size $N \times M$, where N is a fixed value for all samples and M relies on the number of minutiae in each sample. The binary template is composed by the

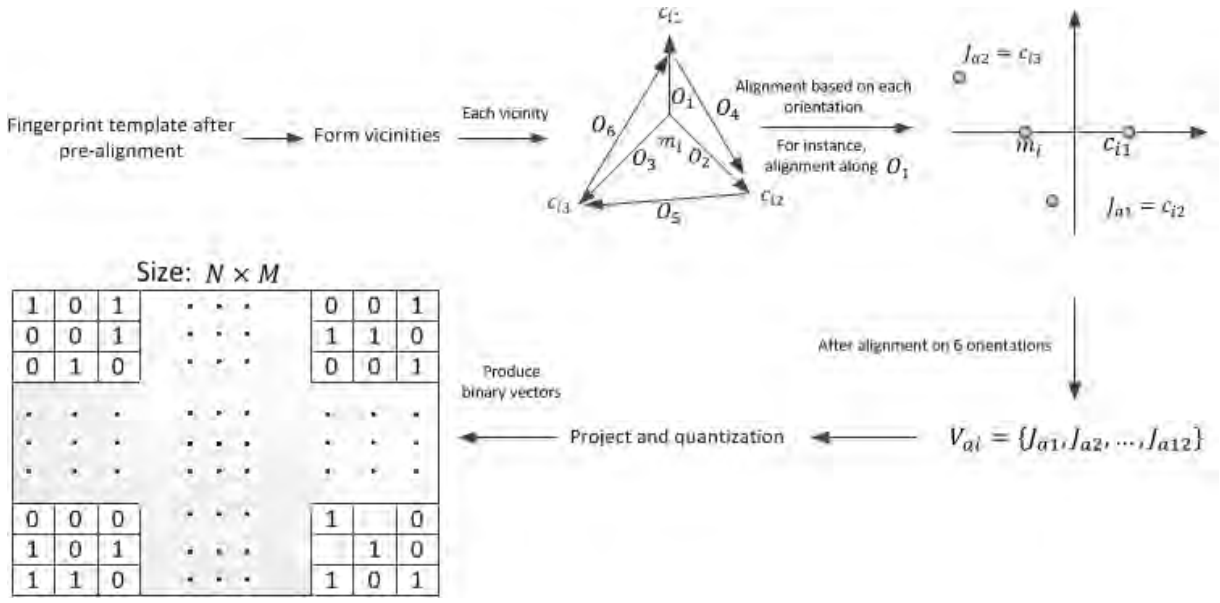

Fig. 3: Procedures of binary template generation

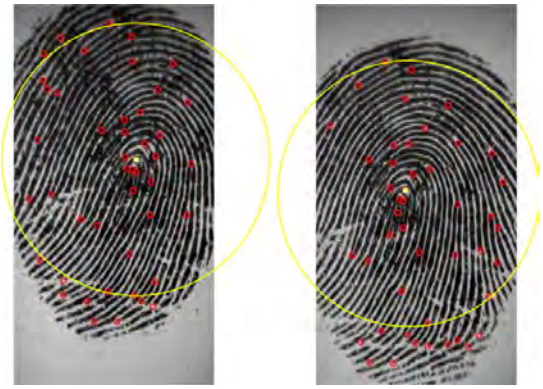

Fig. 2: Pre-alignment: only minutiae (marked by red circle) which are located in the yellow circle will be used for binary template generation

$N-$dimensional binary vectors generated from each minutiae vicinity. A minutiae vicinity is a basic unit which is formed by four minutiae including a center minutia and its three closest neighboring minutiae sorted by ascending order based on their Euclidean distance with the center minutia [18]. Each minutiae vicinity contains 6 orientations which are defined between minutiae pairs as seen in Fig. 3. If we use each orientation as X axis in a new coordinate system, the remaining minutia pair can be geometrically-aligned. For instance in Fig. 3, a new aligned minutiae pair J_{a1}, J_{a2} can be obtained if we use the orientation O_1 as a new coordinate system. Thus 6 new minutia pairs can be obtained after this geometric alignment. A 36-dimensional vector V can be composed by concatenating the coordinates x, y and angle information from these 12 new minutiae. This 36-dimensional vector will be used as input for projection and quantization which is performed by the Equation (3).

$$t = Q(R^T V) \tag{3}$$

where R^T consists of 16 random matrices used for all samples, $Q(\cdot)$ is a quantizer (positive as 1 and non-positive as 0) to output an $36 * 16$ bits binary string H. The post-processing consists of two steps: firstly, the first half of H is XORed by the latter half to downsize the binary string to $H/2$ bits; secondly, a N bit binary can be produced by discarding the last $H/2 - N$ bits, where we set $H/2 > N$ in binary template generation.

Since Bloom filters operate on a binary block with word size w, we propose the binary matrix B is divided into a set of blocks from both horizontal and vertical direction as shown in Fig.1. From horizontal direction, the columns are partitioned into 3 pieces separated at p^{th} column and q^{th} column. From vertical direction, the binary binary matrix will be divided into N/w parts. For instance, the first block is $B(1:w, 1:p)$ and the second block is $B(1:w, (p+1):q)$. The total number of blocks is $3 * N/w$. Mapping each block BM_i into a Bloom filters b_i is similar to employ Bloom filters on iris recognition in paper[14]. A Bloom filter b is a bit array with length $2^w - 1$ and initially all bits to 0. The bit at position h_x of Bloom filter b will be flipped to 1 if the decimal value of a column is equal to h_x. The bit will remain at 1 even if there are multiple columns mapped to the same position. This is also the reason why Bloom filters meets the irreversibility requirement.

During the comparison phase, the dissimilarity score is calculated by using Equation (4) for two transformed templates, where we assume R as reference and P as probe.

$$DS(R,P) = \sum_{i,j=1}^{K} \frac{HD(b\_R_i, b\_P_i)}{|b_i| + |b_j|} \quad (4)$$

where $|b\_R_i| \neq 0, |b\_P_i| \neq 0$, K is the number of Bloom filters, b_R_i is the Bloom filter in reference template R and b_P_i is the corresponding Bloom filter in probe template P. $|b|$ denotes the amount of bits with value 1 in a Bloom filter b.

3. PERFORMANCE EVALUATION

To evaluate the performance of template protection scheme, researchers generally apply the stolen-token case [19] which still guarantee the irreversibility. The following Equal Error Rate (EER) is calculated under this assumption. In addition, a corresponding unprotected EER is also calculated by directly using binary template without Bloom filters in order to analyse the impact of applying Bloom filters. A comparison score from these binary templates is calculated as the number of match cases of all columns in the reference template and all columns in the probe templates. We consider two columns are matched if the Hamming distance between these two columns is less than a threshold TH (empirically we set TH to 40). The experiments were conducted on FVC_2002_DB1A [20], FVC_2002_DB2A [20] and $MCYT\text{-}fingerprint$-100 [21]. The fingerprint extractor adopted in our experiments is NeuroTechnology Verifinger 6.0 Extractor [16] which sorts the minutia by its coordinate Y in default. The details of experimental setting and results are introduced as follows.

3.1. Experiments on FVC database

The performance was evaluated on FVC_2002_DB1A and FVC_2002_DB2A respectively. FVC_2002_DB1A consists of 800 samples which were captured from 100 fingers with 8 samples per finger. These samples have the size 388*374 pixels and are generally sorted by the sample quality in descending order. We designed two types of experiments to study the performance variation under different setting:

- Setting one: investigate the performance impact by varying the word size at 8, 10, 12 and 13. In this case, the first sample of each finger is enrolled as reference sample, and the second sample of each finger is used for probe sample.
- Setting two: investigate the performance impact by using different sample quality. In this setting, the first sample of each finger is still enrolled as reference sample, but the probe sample will be chosen from second sample, third sample and sixth sample respectively. And the word size w is fixed at 13.

w	Blocks' number	EER after Bloom filters	EER without Bloom filters	EER difference
8	96	0.19	0.02	-0.17
10	75	0.09		-0.07
12	63	0.04		-0.02
13	57	0.03		-0.01

Table 1: EERs on $FVC2002\_DB1A$ under different word size (Setting one)

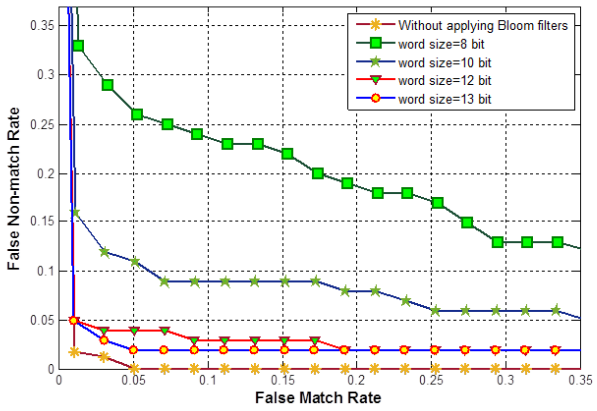

Fig. 4: DET curve on $FVC2002\_DB1A$ under different word size (Setting one)

The radius r of the circle which is used in pre-alignment processing is set to 190 in FVC_2002_DB1A, and $p = 45, q = 90$. Fig.4 illustrates Detection Error Trade-off (DET) curve under setting one for FVC_2002_DB1A. We can observe that the performance significantly improves as long as word size w increases. On the other hand, the computational complexity also rises with word size. Therefore, increasing the word size has to stop at some point where the system can afford the complexity. Table 1 lists the ERRs after applying Bloom filters and ERRs without Bloom filters under Setting one. We can see accuracy performance slight decrease at word size $w = 13$. Table 2 gives the EERs under Setting two. Observed from the results, the fingerprint quality has heave impact on the accuracy performance which would be a challenging work in the future.

These two settings were also applied on database FVC_2002_DB2A which has the sample image with size 296×560 pixels. The parameters in this database were set as $r = 210, p = 45, q = 90$. Fig.5 illustrates the DET curve under Setting one using different word sizes. Table 4 lists the

Probe samples	EER after Bloom filters	EER without Bloom filters	EER difference
Second sample	0.03	0.02	-0.01
Third sample	0.07	0.02	-0.05
Sixth sample	0.14	0.05	-0.09

Table 2: EERs on $FVC2002\_DB1A$ using different probe samples (Setting two)

EERs for this setting, and Table 4 gives the EERs for using different samples as probe. We can see that the biometric performance even slightly better than the performance without using Bloom filters, although the performance still suffers from the low sample quality.

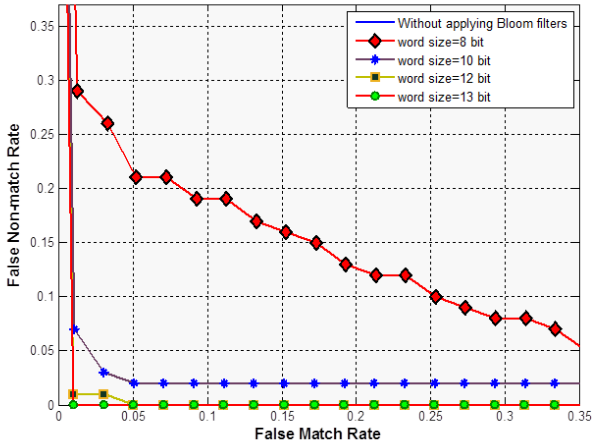

Fig. 5: DET curve on $FVC2002\_DB2A$ under different word size (Setting one)

3.2. Experiments on MCYT100

The experiments were also conducted on $MCYT\text{-}fingerprint$-100[21] which consists of 100 subjects with 10 fingers used for fingerprint sample acquisition. We chose the sample with size 256×400 captured by an optical capture device which is model UareU from Digital Persona[21]. We selected the third sample of each finger as reference, and the second sample of each finger as probe due to the observation that these two samples have better quality comparing to the remaining samples. The rest of parameters were set as $r = 115, p = 45, q = 90$. Table 5 lists the ERRs for ten fingers respectively. The results show that using proposed approach on 6^{th} finger doesn't lose any information after applying Bloom filters comparing to the performance without Bloom filters. The performance on the rest of fingers slight decreases.

w	Blocks' number	EER after Bloom filters	EER without Bloom filters	EER difference
8	96	0.16	0.01	-0.15
10	75	0.03		-0.02
12	63	0.01		0
13	57	0.005		+0.05

Table 3: EERs on $FVC2002\_DB2A$ under different word size (Setting one)

Probe samples	EER after Bloom filters	EER without Bloom filters	EER difference
Second sample	0.005	0.01	+0.005
Third sample	0.03	0.003	-0.027
Sixth sample	0.11	0.06	-0.05

Table 4: EERs on $FVC2002\_DB2A$ using different probe samples (Setting two)

4. CONCLUSION

Due to the concerns of security and privacy on biometric data, we studied applying Bloom filters to protected the fingerprint template in this paper. A pre-alignment process is deployed before generating the binary template in order to be robust with the fingerprint sample translation. In addition, we

Finger ID	EER after Bloom filters	EER without Bloom filters	EER difference
0	0.01	0.003	-0.007
1	0.04	0.02	-0.02
2	0.04	0.03	-0.01
3	0.07	0.03	-0.04
4	0.05	0.02	-0-03
5	0.03	0.01	-0.02
6	0.03	0.03	0
7	0.08	0.04	-0.04
8	0.09	0.07	-0.02
9	0.06	0.03	-0.03

Table 5: ERRs on database $MCYT\text{-}fingerprint$-100 running for ten fingers respectively

proposed to divide the binary template matrix from both horizontal direction and vertical direction since the size of fingerprint binary template is large and variable. Experiments were conducted on $FVC2002\_BD1A$, $FVC2002\_BD2A$ and $MCYT\text{-}fingerprint$-100 respectively. According to the performance evaluation, the biometric performance doesn't degrade after applying Bloom filters if the fingerprint sample has good quality. Therefore, we can conclude that it is feasible to apply Bloom filters on fingerprint biometrics. Moreover, the biometric performance is still suffering from poor quality fingerprint images based on the experimental results. Our future work will focus on improving proposed approach which can be resilient to the low quality samples.

References

[1] Sergey Tulyakov, Faisal Farooq, and Venu Govindaraju, "Symmetric hash functions for fingerprint minutiae," in *Pattern Recognition and Image Analysis*, pp. 30–38. Springer, 2005.

[2] Raffaele Cappelli, Dario Maio, Alessandra Lumini, and Davide Maltoni, "Fingerprint image reconstruction from standard templates," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 29, no. 9, pp. 1489–1503, 2007.

[3] Jianjiang Feng and Anil K Jain, "Fingerprint reconstruction: from minutiae to phase," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 33, no. 2, pp. 209–223, 2011.

[4] ISO/IEC 24745:2011, "Information Technology - Security Techniques– Biometric Information Protection," .

[5] Christian Rathgeb and Andreas Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 1–25, 2011.

[6] Karthik Nandakumar, Anil K Jain, and Sharath Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 4, pp. 744–757, 2007.

[7] Ari Juels and Madhu Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[8] Andrew Beng Jin Teoh and Jaihie Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electronics Express*, vol. 4, no. 23, pp. 724–730, 2007.

[9] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[10] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle, "Generating cancelable fingerprint templates," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 29, no. 4, pp. 561–572, 2007.

[11] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, and Sangyoun Lee, "Alignment-free cancelable fingerprint templates based on local minutiae information," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 37, no. 4, pp. 980–992, 2007.

[12] Sharat Chikkerur, Nalini K Ratha, Jonathan H Connell, and Ruud M Bolle, "Generating registration-free cancelable fingerprint templates," in *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*. IEEE, 2008, pp. 1–6.

[13] Matteo Ferrara, Davide Maltoni, and Raffaele Cappelli, "Noninvertible minutia cylinder-code representation," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 6, pp. 1727–1737, 2012.

[14] Christoph Busch Christian Rathgeb, Frank Breitinger and Harald Baier, "On the application of Bloom filters to iris biometrics," *IET Biometrics*, 2014.

[15] Marta Gomez-Barrero, Christian Rathgeb, Javier Galbally, Julian Fierrez, and Christoph Busch, "Protected facial biometric templates based on local gabor patterns and adaptive Bloom filters," .

[16] "Verifinger," http://www.neurotechnology.com/verifinger.html, Accessed: 2013-10-30.

[17] Bian Yang, Christoph Busch, Davrondzhon Gafurov, and Patrick Bours, "Renewable minutiae templates with tunable size and security," in *Pattern Recognition (ICPR), 2010 20th International Conference on*. IEEE, 2010, pp. 878–881.

[18] Bian Yang and Christoph Busch, "Parameterized geometric alignment for minutiae-based fingerprint template protection," in *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*. IEEE, 2009, pp. 1–6.

[19] A Teoh and Chong Tze Yuang, "Cancelable biometrics realization with multispace random projections," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 37, no. 5, pp. 1096–1106, 2007.

[20] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar, *Handbook of fingerprint recognition*, springer, 2009.

[21] "Mcyt100 database," http://atvs.ii.uam.es/index, Accessed: 2014-10-01.