A Two-Factor Protection Scheme for MCC Fingerprint Templates

Matteo Ferrara, Davide Maltoni, and Raffaele Cappelli

Department of Computer Science and Engineering
University of Bologna
Via Sacchi, 3 - 47521 Cesena (FC), Italy
{matteo.ferrara, davide.maltoni, raffaele.cappelli}@unibo.it

Abstract: Minutia Cylinder-Code (MCC) is an effective representation for robust and fast fingerprint matching. To avoid that MCC templates can disclose sensitive information about position and angle of minutiae, a protected MCC representation was recently introduced (called P-MCC). Inspite of a satisfactory level of accuracy and irreversibility, P-MCC templates cannot be revoked. In this paper we propose a twofactor protection scheme that makes P-MCC templates revocable.

1 Introduction

Among the three basic approaches to user authentication (knowledge factors, possession factors, biometrics), only biometric systems can guarantee the *identity of the user*: the other two factors can simply confirm that the user *knows* a given information or that the user *owns* a given device or token. On the other hand, the properties that make biometric traits so interesting for automated user authentication (uniqueness and permanence), also raise potential privacy problems: for instance, a biometric sample may be used to link activities of the same user across different applications, or some biometric features may allow medical or other sensitive data to be revealed [RU11]. Moreover, a biometric trait, if compromised cannot be revoked and renewed: this is in contrast with passwords and tokens that can be easily reissued. For these reasons it is very important to protect biometric templates, making them unusable without authorization, but without losing the capability to verify the user's identity [Si12]. It is desirable that a *Biometric Template Protection (BTP)* method satisfies the following requirements [Br09]: *accuracy*, *irreversibility*, *diversity* and *unlinkability*.

Since fingerprints are the most largely used biometric trait, developing effective fingerprint BTP methods is a crucial challenge and the research is very active on this topic [RU11].

This paper introduces a novel fingerprint template protection scheme, evaluates its accuracy and security according to well-defined criteria [Si12], and tests its robustness against various types of attack. The proposed scheme is based on a combination of a user secret key and a non-invertible minutiae representation (P-MCC [FMC12]): these two factors allow the BTP requirements to be met. In particular, as confirmed by the extensive experimentation performed on six public databases, the new method markedly outperforms most of the state-of-the-art techniques and is robust against different attack

scenarios. Please refer to [FMC14] for an extended report containing more details about i) the state-of-the-art of fingerprint template protection schemes (in particular focusing on two-factor approaches), ii) P-MCC representation and iii) experiment evaluation.
The rest of this paper is organized as follows. Section 2 describes the novel two-factor protection scheme. Section 3 reports experiments on public databases to evaluate accuracy and security of the new approach, to compare it against the state-of-the-art, and to test its robustness against potential attacks. Finally, Section 4 draws some concluding remarks.

2 Two-factor protection scheme (2P-MCC)

As discussed in [FMC12], P-MCC representation guarantees irreversibility and accuracy but not diversity and unlinkability [Si12]. In some preliminary studies a random projection transform [TY07] was combined to the P-MCC representation to fulfill diversity and unlinkability requirements: although such solution showed good results in terms of recognition accuracy, it was not robust enough against token-stolen attacks. The two-factor method proposed in this work (called 2P-MCC) is simple but proved to allow a good trade-off between accuracy and security: the basic idea is to select a subset of the original bits and scrambling them according to a secret key, as described in detail in the following sections.

2.1 From P-MCC to 2P-MCC

Let $\hat{V}$ be a P-MCC$_k$ template (where k denotes the amount of dimensionality reduction, see [FMC12]) and let s be a user-specific secret key. Then, for a given $c \in \mathbb{N}$, $0 < c \leq k$, let $P_c(s) = (p_1, p_2, \dots, p_c)$ be a partial permutation [Wi14] of set $\{0, \dots, k-1\}$, randomly generated using s as seed for a cryptographically secure pseudorandom number generator. The function $\mathcal{F}_{P_c(s)}: \{0,1\}^k \rightarrow \{0,1\}^c$ maps a k-dimensional bit-vector $\hat{\mathbf{v}}_m$ into a c-dimensional binary space, according to the partial permutation obtained from the secret key s:

$$\mathcal{F}_{P_c(s)}(\hat{\mathbf{v}}_m) = \left[\hat{\mathbf{v}}_m[p_1], \hat{\mathbf{v}}_m[p_2], \dots, \hat{\mathbf{v}}_m[p_c]\right], \qquad p_1, p_2, \dots, p_c \in P_c(s) \tag{1}$$

The 2P-MCC template $\ddot{V}$ is a set of bit-vectors defined as:

$$\ddot{V} = \left\{\ddot{\mathbf{v}}_m | \ddot{\mathbf{v}}_m = \mathcal{F}_{P_c(s)}(\hat{\mathbf{v}}_m), \hat{\mathbf{v}}_m \in \hat{V}\right\} \tag{2}$$

2.2 Similarity computation

The transformation proposed to convert P-MCC templates into 2P-MCC templates does not alter the similarity metric between bit vectors. As described in [FMC12] for P-MCC, let $\ddot{\mathbf{v}}_a$ and $\ddot{\mathbf{v}}_b$ be the 2P-MCC bit-vectors; their similarity can be computed as:

$$\gamma(\ddot{\mathbf{v}}_a, \ddot{\mathbf{v}}_b) = 1 - \frac{\|\ddot{\mathbf{v}}_a \text{ XOR } \ddot{\mathbf{v}}_b\|_1}{c} \tag{3}$$

where XOR denotes the *bitwise-exclusive-or* between two bit-vectors, $\|\cdot\|_1$ represents the 1-norm, and c the length of the bit-vectors. Note that the 1-norm of a bit-vector can be simply computed as the population count (number of bits with value one). The

similarity $\gamma(\ddot{\mathbf{v}}_a, \ddot{\mathbf{v}}_b)$ is always in the range [0,1], where zero means no similarity and one maximum similarity.
In order to compare two protected templates S_A and S_B, a single value denoting their overall similarity has to be obtained from the two sets of bit-vectors. To this purpose, the *Local Greedy Similarity* (LGS) approach, originally proposed in [Ca10], can be used to calculate the global match score as described in [FMC12]. Note that, this approach does not assume any a priori ordering of the bit-vectors: this allows to randomly shuffle them inside each 2P-MCC template, to increase the robustness against various types of attacks (e.g., correlation attacks [KY08]).

3 Experimentation

This section describes several experiments carried out to evaluate the proposed method and to compare it with the state-of-the-art.

3.1 Minutiae extraction and creation of 2P-MCC descriptors

A state-of-the-art minutiae extraction algorithm (already used in [FMC12]) has been employed to extract minutiae templates from all fingerprints in all data sets.
2P-MCC descriptors have been derived from the minutiae templates as described in Section 2. To study the trade-off between accuracy and security, four different combinations of parameters (k, c) have been used: $(64,64)$, $(64,48)$, $(32,32)$ and $(32,24)$.

3.2 Verification accuracy

For a full comparison with the state-of-the-art, the evaluation of biometric verification accuracy has been carried out on FVC2002 [Ma02], FVC2004 [Ma04], and FVC2006 [Ca07] datasets (see Table I in [FMC14]) using the *FVC protocol* [FMC14]. The following performance indicators are considered: Equal-Error-Rate (EER), lowest FNMR for FMR≤0.1% (FMR_{1000}), and lowest FNMR for FMR=0% (Z_{FMR}). To avoid unfair comparison with single-factor techniques, the accuracy in the *token-stolen scenario* [Ya10] is also reported. To simulate this scenario, all the protected templates are generated using the same secret key s.
Tables I compares the accuracy of the proposed protection scheme against other two-factor approaches. It is worth noting that:

- 2P-$MCC_{64,64}$ is more accurate than most of the existing approaches, except for [MD13];
- as expected, decreasing k and/or c reduces the accuracy.

Tables II compares the accuracy of the proposed protection scheme against other two-factor approaches, under token-stolen scenario. Only two-factor approaches for which authors provide results under the token-stolen scenario are here considered. It is worth noting that:

- 2P-$MCC_{64,64}$ overcomes all existing approaches, but one case (EER on FVC2002 DB1 in Table II);
- 2P-$MCC_{64,48}$ and 2P-$MCC_{32,32}$ are often more accurate than existing approaches;
- 2P-$MCC_{32,24}$ in some cases outperforms other approaches.

TABLE I
VERIFICATION ACCURACY (PERCENTAGE VALUES).

	FVC2002												FVC2004			FVC2006		
	DB1			DB2			DB3			DB4			DB1			DB2		
	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}
2P-$MCC_{64,64}$	2.0	3.1	4.3	1.1	1.3	1.4	4.4	8.4	11.8	3.1	5.0	6.6	3.0	6.8	9.1	0.1	0.1	0.2
2P-$MCC_{64,48}$	2.9	6.4	7.2	1.7	2.7	4.2	6.7	14.4	16.6	4.2	7.4	11.2	4.9	13.1	24.6	0.2	0.3	0.4
2P-$MCC_{32,32}$	4.5	7.4	10.8	2.7	4.7	6.8	7.8	18.4	20.0	5.1	13.6	15.2	6.1	16.5	19.7	0.3	0.6	0.9
2P-$MCC_{32,24}$	6.8	14.0	14.9	4.4	11.1	13.2	11.2	28.0	30.9	7.8	21.6	26.3	8.8	30.8	40.1	0.9	2.5	4.9
[BSW07]	2.1	-	-	1.2	-	-	-	-	-	-	-	-	8.6	-	-	-	-	-
[MD13]	0.7	-	-	0.4	-	-	3.8	-	-	1.4	-	-	1.9	-	-	-	-	-

TABLE II
VERIFICATION ACCURACY IN THE TOKEN-STOLEN SCENARIO (PERCENTAGE VALUES).

	FVC2002												FVC2004			FVC2006		
	DB1			DB2			DB3			DB4			DB1			DB2		
	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}	EER	FMR_{1000}	Z_{FMR}
2P-$MCC_{64,64}$	3.3	6.5	8.1	1.8	3.5	5.5	7.8	18.2	20.7	6.6	18.5	21.2	6.3	18.3	22.2	0.3	0.5	1.1
2P-$MCC_{64,48}$	4.6	8.6	9.1	2.5	5.6	6.1	9.9	21.9	27.4	7.8	19.3	28.3	8.4	22.1	23.6	0.6	1.2	2.2
2P-$MCC_{32,32}$	6.6	14.8	19.5	4.3	11.5	16.4	12.2	29.6	34.5	11.2	33.5	37.1	9.5	29.4	31.0	1.0	2.3	3.5
2P-$MCC_{32,24}$	8.6	23.8	29.9	6.8	16.9	19.9	15.7	37.3	50.1	12.5	39.9	45.3	11.5	38.1	48.8	1.9	4.9	9.3
[Tu07]	3.0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
[Ah08]	7.2	-	-	3.6	-	-	11.8	-	-	11.5	-	-	-	-	-	-	-	-
[KTG10]	-	-	-	5.0	-	-	-	-	-	-	-	-	-	-	-	-	-	-
[Li10]	-	23.7	31.2	-	15.7	27.7	-	-	-	-	-	-	-	-	-	-	-	-

3.3 Security analysis

In the following paragraphs, specific experiments are reported to evaluate how 2P-MCC improves P-MCC irreversibility and provides unlinkability, which are the two fundamental security requirements for any BTP method [Si12] [Br09].

Irreversibility

To meet the irreversibility requirement, the protected template should not allow the original minutiae template to be retrieved. The irreversibility of 2P-MCC descriptors is based on three elements: i) the irreversibility of the P-MCC representation, already widely discussed in [FMC12], ii) the secrecy of the user-specific key, and iii) the information loss due to the reduction of the bit-vector length when $c < k$.

If a 2P-MCC template is stolen by an attacker, and the attacker does not know the user-specific key s, reversing the protect template is practically unfeasible, since the attacker has no clue about the partial permutation $P_c(s)$ used to create it. In fact, the number of c-permutations of k objects is equal to $\frac{k!}{(k-c)!}$ [Wi14], which corresponds to $5.5 \cdot 10^{26} \cong 2^{89}$ possibilities for 2P-$MCC_{32,24}$, and to $1.3 \cdot 10^{89} \cong 2^{296}$ possibilities for 2P-$MCC_{64,64}$.

If the user-specific secret key s has been stolen as well, the partial permutation $P_c(s)$, used to create the stolen template $\ddot{V}$, can be derived. Then, using $P_c(s)$, it is possible to

recover a P-MCC template $\tilde{V}$ from $\ddot{V}$. Note that if $c = k$, then $\tilde{V} = \hat{V}$, where $\hat{V}$ is the original template from which the 2P-MCC template was generated. Otherwise, when $c < k$, the bit-vectors $\tilde{\mathbf{v}}_m \in \tilde{V}$ can be only partially recovered (i.e., $k - c$ bits in $\tilde{\mathbf{v}}_m$ are $undefined$ since their corresponding values were not stored in $\ddot{\mathbf{v}}_m$ during the protection step).

In conclusion, the following observations can be drawn:

- In the worst scenario, when both protected template and secret key have been stolen and $c = k$, the irreversibility level is the same of P-MCC: hence it is still quite hard to retrieve some information about the original minutiae. As an example, for $k = 64$, a sophisticated attack strategy is able to reconstruct 26.5% of the original minutiae, but on the other hand, it is unable to reconstruct 73.5% of the minutiae and creates 69.5% false minutiae [FMC12].
- If the attacker stole the protected template but does not know the key, the irreversibility level is much higher, since the attacker would have to find the right partial permutation before trying to reconstruct the minutiae template from the P-MCC representation as discussed above. For instance, for 2P-MCC$_{64,64}$ there are 2^{296} possible permutations, which makes a brute-force attack unfeasible.
- Finally, when $c < k$, 2P-MCC offers a further protection since a portion of the P-MCC information is not stored in the template.

Unlinkability

To meet the unlinkability requirement, protected templates generated from the same biometric trait using different secret keys should be as different as protected templates generated from different biometric traits. To check this requirement, the following score distributions are analyzed:

- *Same Sample*: match scores among templates generated from the same fingerprint sample using different keys;
- *Same Finger*: match scores among templates generated from different impressions of the same finger using different keys;
- *Different Finger*: match scores among templates generated from the first sample of different fingerprints using different keys.

Figure 1 shows the above score distributions computed on FVC2006 DB2 dataset for different values of k and c. It can be noted that the three curves are almost overlapped in all graphs: this means that the dissimilarity between protected templates generated from the same sample/finger is comparable to that of protected templates generated from different fingers.

3.4 Robustness against attacks

This section describes experiments aimed at assessing the robustness of 2P-MCC against two different attacks: the former based on revoked templates, and the latter on compromised security keys.

Revoked template attack

As discussed in the previous sections, 2P-MCC provides diversity and unlinkability, thus allowing templates to be revoked and renewed. Systematic experiments have been

performed to evaluate if it is possible to use revoked templates to attack a system based on 2P-MCC. In particular, two attack scenarios have been considered:

- Type-I attack, where a revoked template is used to attack a system containing a renewed template created from the same impression;
- Type-II attack, where a revoked template is used to attack a system containing a renewed template created from another impression of the same finger.

Both attack scenarios have been evaluated under two different security levels: medium-security (matching threshold set to 0.1% FMR), and high-security (matching-threshold set to 0% FMR) [FMC12]. The attack simulations have been performed on the FVC2006 DB2 dataset, producing 1680 and 9240 type-I and type-II attacks, respectively. Table III reports the percentage of successful attacks under both security levels.

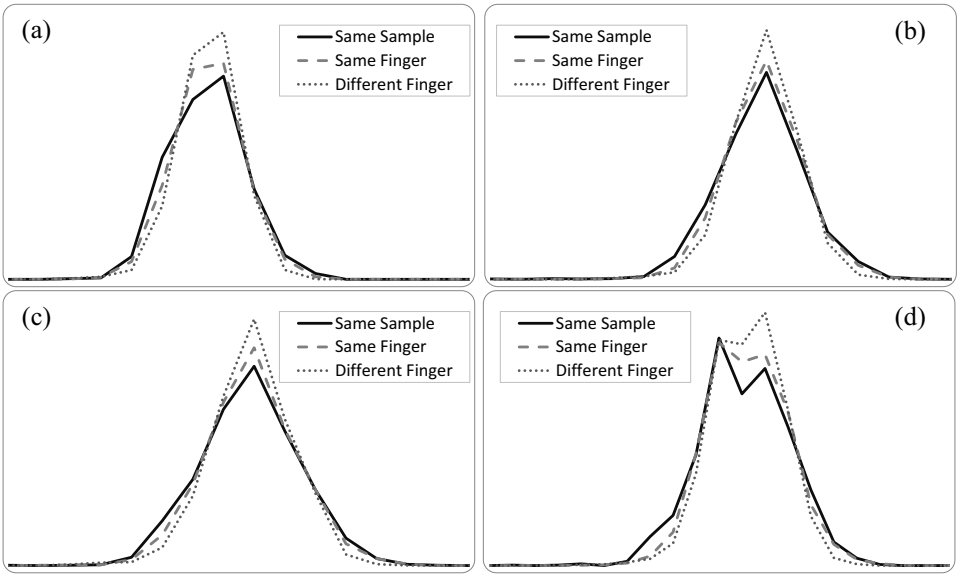

Figure 1: Score distribution graphs for the proposed protection method to evaluate unlinkability requirement on FVC2006 DB2 dataset: (a) (64,64), (b) (64,48), (c) (32,32) and (d) (32,24).

TABLE III
PERCENTAGE OF SUCCESSFUL ATTACKS (USING A REVOKED 2P-MCC TEMPLATE) ON FVC2006 DB2 AT MEDIUM- AND HIGH-SECURITY LEVEL.

Method	Medium-security		High-security	
	Type-I Attack	Type-II Attack	Type-I Attack	Type-II Attack
2P-MCC$_{64,64}$	0.71%	0.02%	0.00%	0.00%
2P-MCC$_{64,48}$	0.77%	0.17%	0.24%	0.08%
2P-MCC$_{32,32}$	0.65%	0.21%	0.24%	0.09%
2P-MCC$_{32,24}$	0.77%	0.09%	0.06%	0.02%

Token-stolen attack

The accuracy of many two-factor methods strongly depends on the secrecy of the user-specific keys. In these cases, the knowledge of a key allows to easily find collisions (i.e., produce false matches) even if the attacker does not possess the biometric sample. For

this reason, as already discussed in Section 3.2, the robustness of a two-factor system must be also reported in the token-stolen scenario.
This section reports the results of experiments aimed at evaluating the robustness of 2P-MCC against token-stolen attacks; in particular, it is assumed that the attacker knows the secret key of each user and the percentage of successful attacks is reported for the same two security levels defined in the previous section: i) medium- and ii) high-security. The attack simulation has been performed on the FVC2006 DB2 dataset, producing 9730 attack attempts. Table IV reports the percentage of successful attacks: the robustness of 2P-MCC is confirmed, especially at the high-security level.

TABLE IV
PERCENTAGE OF SUCCESSFUL ATTACKS (UNDER THE TOKEN-STOLEN SCENARIO) ON FVC2006 DB2 AT MEDIUM- AND HIGH-SECURITY LEVEL.

Method	Medium-security	High-security
2P-MCC$_{64,64}$	4.62%	0.86%
2P-MCC$_{64,48}$	1.53%	0.53%
2P-MCC$_{32,32}$	2.50%	1.23%
2P-MCC$_{32,24}$	1.14%	0.08%

4 Conclusions

In this paper we propose 2P-MCC, a new two-factor template protection approach that confers to P-MCC the desirable properties of diversity and unlinkability. We evaluated different parameterizations of 2P-MCC and systematically compared them against state-of-the-art approaches on several benchmarks and scenarios. A thorough security analysis, in line with recent guidelines and recommendations [Si12] [Br09], was also carried out. The experimental results show that in most of the cases 2P-MCC performs better than existing techniques and is quite robust against token-stolen scenario, which is known to be the main pitfall of two-factors schemes.
Turning a P-MCC template into a 2P-MCC one is straightforward and computationally light; while in this paper we proposed a simple permutation-based method, in principle other more sophisticate hamming-distance preserving transforms could be used: this is what we intend to investigate in our future research.

Acknowledgment

The work leading to these results has received funding from the European Community's Framework Programme (FP7/2007-2013) under grant agreement n° 284862.

References

[Ah08] D. Ahn, S. G. Kong, Y. S. Chung, and K. Y. Moon, "Matching with Secure Fingerprint Templates using Non-invertible Transform," in *proc. on Image and Signal Processing*, 2008.

[Br09] J. Breebaart, B. Yang, I. Buhan-Dulman, and C. Busch, "Biometric template protection - The need for open standards," *Datenschutz und Datensicherheit*, vol. 33, no. 5, 2009.

[BSW07] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," in *in proocedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* , 2007, pp. 1-8.

[Ca07] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today*, vol. 15, no. 7-8, pp. 7-9, August 2007.

[Ca10] R. Cappelli, M. Ferrara, D. Maltoni, and M. Tistarelli, "MCC: a Baseline Algorithm for Fingerprint Verification in FVC-onGoing," in *proceedings 11th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, Singapore, 2010.

[FMC12] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1727-1737, December 2012.

[FMC14] M. Ferrara, D. Maltoni, and R. Cappelli, "A Simple and Effective Two-Factor Protection Scheme for MCC Fingerprint Templates," Biometric System Laboratory - University of Bologna, Technical Report, 2014.

[KTG10] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of Symmetric Hash Functions for Secure Fingerprint Matching," in *proc. 20th International Conference on Pattern Recognition*, 2010.

[KY08] A. Kholmatov and B. Yanikoglu, "Realization of Correlation Attack Against the Fuzzy Vault Scheme," in *proceedings of SPIE Symposium on Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, San Jose (USA), 2008.

[Li10] P. Li et al., "An Alignment-Free Fingerprint Cryptosystem Based on Fuzzy Vault Scheme," *Journal of Network and Computer Applications*, vol. 33, no. 3, May 2010.

[Ma02] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "FVC2002: Second fingerprint verification competition," in *Int. Conf. on Pattern Recognition*, vol. 16, 2002.

[Ma04] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition," in *proceedings International Conference on Biometric Authentication (ICBA04)*, Hong Kong, 2004, pp. 1-7.

[MD13] L. Mirmohamadsadeghi and A. Drygajlo, "A template privacy protection scheme for fingerprint minutiae descriptors," in *proceedings of 12th International Conference of the Biometrics Special Interest Group, BIOSIG*, Darmstadt, 2013, pp. 185-192.

[RU11] C. Rathgeb and A. Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics," *EURASIP Journal on Information Security*, 2011.

[Si12] K. Simoens et al., "Criteria Towards Metrics for Benchmarking Template Protection Algorithms," in *proc. of the 5th IEEE/IAPR Int. Conference on Biometrics*, 2012.

[Tu07] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric Hash Functions for Secure Fingerprint Biometric Systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427-2436, December 2007.

[TY07] A. Teoh and C. T. Yuang, "Cancelable Biometrics Realization With Multispace Random Projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 37, no. 5, pp. 1096-1106, October 2007.

[Wi14] Wikipedia. (2014, July) Permutation. [Online]. http://en.wikipedia.org/wiki/Permutation

[Ya10] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic Random Projection for Biometric Template Protection," in *proceedings Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, 2010, pp. 1-7.