Adaptive Weighted Graph Approach to Generate Multimodal Cancelable Biometric Templates

Gurjit Singh Walia*, Gaurav Jain*, Nipun Bansal, Kuldeep Singh

IEEE Transactions on Information Forensics & Security, 2019

*Equal Contribution

Importance of Research

- Multibiometric systems fail to cater the security requirements of **adversary attacks**, which include both (1) template protection, and (2) robustness to presentation attacks.
- Template protection through cancelable approach often **lack *complete* non-invertibility**.
- **Image quality** often affects the performance
- Multibiometric systems restrict their applicability to **certain biometric characteristics**, with **particular feature extraction methods**.
- We propose to generate cancelable biometric templates by **feature fusion** of fingerprint, face, and iris, using an **adaptive weighted graph based approach**.

Proposed Multibiometric System

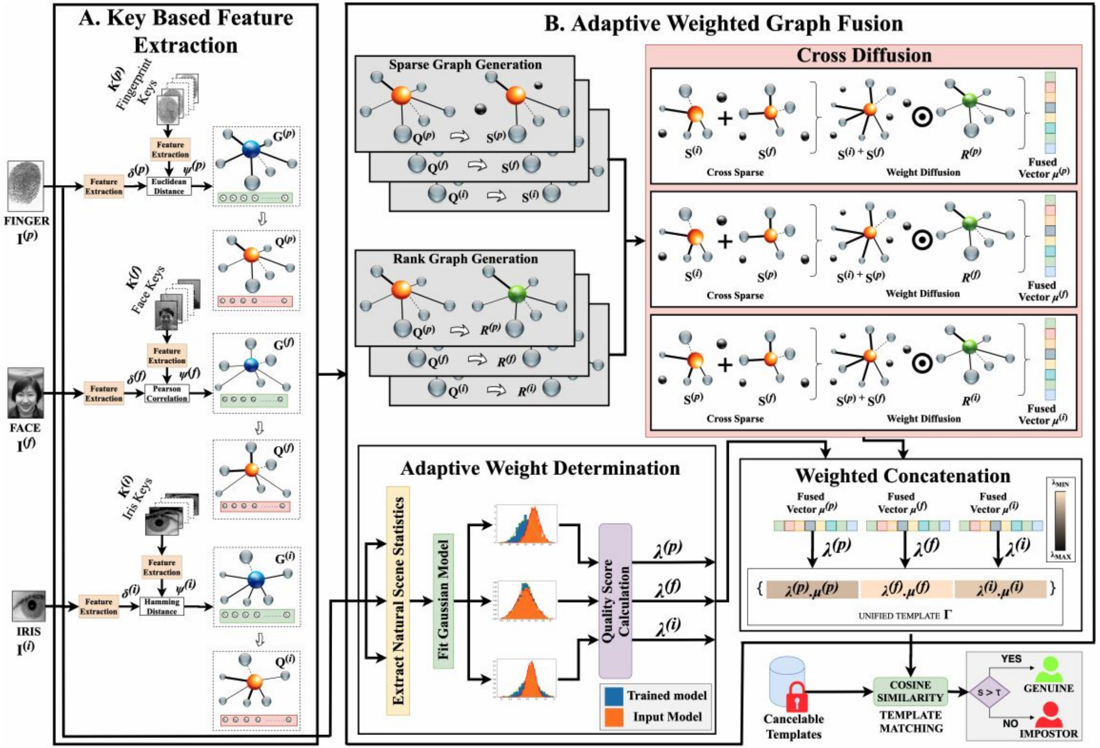

Fig. 1 Overview of the proposed multibiometric system. Normalized graphs constructed through key-based feature extraction is subjected to the proposed cross-diffusion to generate fused vectors. These fused vectors attain weights, determined adaptively using image quality, to generate a cancelable template.

Major Contributions

- **Key-based feature extraction**: is introduced, which not only achieves the generic nature of the proposed features with reduced dimension but also ensures high revocability.

- **Adaptive Weighted Graph Fusion (AWGF)**: is proposed to achieve complete non-invertibility and robustness to presentation attacks.

A. Key-Based Feature Extraction

- Similarity between the input image and all the key images is computed to generate a graph with edge weights equivalent to similarity scores.
- Edge weights are computed using Eq. 2 for fingerprint, Eq. 5 for face, and Eq. 7 for iris.
- This graph is normalised using the anchor based normalisation (Eq. 9) to obtain generic features with reduced dimensions.

Algorithm 1 : Key Based Generic Feature Extraction

Input: $I^{(k)}$, $K_j^{(k)}$ $\forall\ j \in \{1, 2, ..., n\}$
Output: $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$

```
1:  for k ∈ {p, f, i} do
2:      extract raw features for I^(k), denoted as δ^(k)
3:      for j = 1 to n do
4:          extract raw features for K_j^(k), denoted as ψ_j^(k)
5:      end for
6:  end for
7:  for k ∈ {p, f, i} do
8:      for j = 1 to n do
9:          construct G_j^(k) using Eq. 2, Eq. 5, Eq. 7
10:         normalise G_j^(k) to Q_j^(k) using Eq. 9
11:     end for
12: end for
13: return Q^(k) ∈ {Q^(p), Q^(f), Q^(i)}
```

B. Adaptive Weighted Graph Fusion (AWGF)

- It comprises of:
  1. ***Information Mining*** - Extract characteristic information and suppress outliers.
  2. ***Cross Fusion*** - fuse complementary information in a non-linear fashion to achieve non-invertibility.
  3. ***Quality Adaptive Unification*** - incorporate image quality metrics to prevent presentation attacks.

Algorithm 2 Adaptive Weighted Graph Fusion (AWGF)

Input: $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$, κ
Output: Unified Template $\mathbf{\Gamma}$

for $k \in \{p, f, i\}$ **do**
  construct $\mathbf{S}^{(k)}$ from $\mathbf{Q}^{(k)}$ using Eq. 10 given κ
  construct $\mathcal{R}^{(k)}$ from $\mathbf{Q}^{(k)}$ using Eq. 11
end for
for $k \in \{p, f, i\}$ **do**
  compute $\mu^{(k)}$ from $\{\mathbf{S}^{(Z)}\}$, $\mathcal{R}^{(k)}$ using Eq. 12, Eq. 13
  find $\lambda^{(k)}$ using Eq. 14, Eq. 15
end for
find $\mathbf{\Gamma}$ using Eq. 16
return $\mathbf{\Gamma}$

Experimental Results & Discussions

- Proposed approach is evaluated over benchmark multimodal databases in Table I.
- Both quantitative and quantitative validation is performed:
  - Performance Validation:
    - Adaptivity Analysis
    - Fusion Method Comparison
    - Time & Space complexity
  - Privacy & Security Analysis:
    - Non-invertibility
    - Unlinkability
    - Revocability
    - Presentation attack analysis
    - etc...

TABLE I
MULTIMODAL DATABASES USED FOR EXPERIMENTATION.

Database	Fingerprint	Face	Iris
DB-1	SDUMLA-HMT Multimodal Database [36]		
DB-2	MCYT [39]	CAS-PEAL R1 (expression) [40]	IITD PolyU Iris [42]
DB-3	CASIA-Fingerprint V5 [37]	CASIA-FaceV5 [41]	CASIA Iris V3 (Interval) [43]
DB-4	FVC 2006 [38]	CAS-PEAL R1 (accessories) [40]	CASIA Iris V3 (lamp) [43]

Performance Validation

TABLE III
PERFORMANCE EVALUATION AND COMPARISON. AVERAGE DECIDABILITY INDEX (DI), EER (%) AND RECOGNITION INDEX (RI) FOR FUSED TEMPLATES USING STATE-OF-THE-ART FEATURE FUSION TECHNIQUES AT 95% SIGNIFICANCE LEVEL

Performance Metric	Decidability (DI)				EER (%)				Recogniton Index (RI)			
Method/ Database	DB-1	DB-2	DB-3	DB-4	DB-1	DB-2	DB-3	DB-4	DB-1	DB-2	DB-3	DB-4
CCA-FFS I (*f + i*) [45]	2.21 ± 0.2	2.78 ± 0.8	3.01 ± 0.8	3.11 ± 0.3	6.02 ± 1.1	6.09 ± 1.0	6.00 ± 1.1	5.71 ± 0.6	86.31 ± 2.4	76.31 ± 1.6	91.31 ± 2.3	83.58 ± 1.4
CCA-FFS II (*f + i*) [45]	2.79 ± 0.1	2.66 ± 0.5	2.98 ± 0.9	2.96 ± 0.4	6.34 ± 0.9	7.00 ± 1.1	7.50 ± 1.6	6.02 ± 0.9	79.58 ± 1.3	84.04 ± 1.6	77.22 ± 1.3	82.58 ± 2.1
CCA-FFS I (*f + p*) [45]	3.32 ± 0.3	2.60 ± 0.2	2.36 ± 0.8	2.15 ± 0.5	6.04 ± 0.4	6.46 ± 1.0	5.52 ± 1.1	6.49 ± 0.7	77.13 ± 1.6	76.40 ± 1.9	92.84 ± 1.3	88.87 ± 1.1
CCA-FFS II (*f + p*) [45]	1.99 ± 0.6	2.46 ± 0.4	2.10 ± 0.9	2.25 ± 0.8	7.10 ± 1.0	7.02 ± 1.2	7.00 ± 1.3	6.09 ± 1.2	91.13 ± 1.9	84.13 ± 1.5	79.26 ± 1.5	89.88 ± 2.5
RDM (*f + i*) [20]	3.37 ± 0.1	2.31 ± 0.8	2.28 ± 0.3	2.34 ± 0.3	4.55 ± 0.6	4.00 ± 0.3	5.83 ± 1.0	4.79 ± 1.1	85.28 ± 1.2	87.49 ± 1.6	90.40 ± 1.2	78.72 ± 2.2
RDM (*f + p*) [20]	3.91 ± 0.7	2.42 ± 0.4	3.95 ± 0.5	3.19 ± 0.7	3.96 ± 0.4	6.02 ± 0.2	4.21 ± 0.5	4.67 ± 0.7	89.62 ± 1.4	88.84 ± 1.7	92.91 ± 1.8	87.75 ± 1.1
DCT (*f + i*) [46]	2.43 ± 0.2	2.00 ± 0.4	2.22 ± 0.5	2.08 ± 0.1	5.97 ± 1.1	5.68 ± 0.5	6.22 ± 1.3	7.63 ± 0.7	94.66 ± 1.7	89.35 ± 1.3	92.66 ± 0.9	84.47 ± 0.7
DCT (*f + p*) [46]	2.03 ± 0.4	2.05 ± 0.9	2.47 ± 0.4	2.90 ± 0.3	7.76 ± 1.5	5.96 ± 0.6	5.51 ± 1.1	6.17 ± 0.4	77.96 ± 1.9	93.31 ± 1.6	87.09 ± 1.4	83.59 ± 1.8
Ours (*non-adaptive*)	4.68 ± 0.5	5.09 ± 0.5	4.23 ± 0.4	3.97 ± 1.0	3.12 ± 0.3	1.19 ± 0.1	3.05 ± 0.8	3.44 ± 0.4	96.66 ± 2.1	98.09 ± 0.9	95.88 ± 2.0	91.78 ± 1.3
Ours (*adaptive*)	**4.71 ± 0.3**	**5.38 ± 0.5**	**4.72 ± 0.6**	**4.42 ± 1.1**	**2.03 ± 0.9**	**1.00 ± 0.1**	**1.52 ± 0.5**	**2.35 ± 0.7**	**97.98 ± 1.2**	**99.22 ± 0.5**	**96.66 ± 0.8**	**95.57 ± 1.0**

The adaptive AWGF outperforms the non-adaptive version over all four datasets..

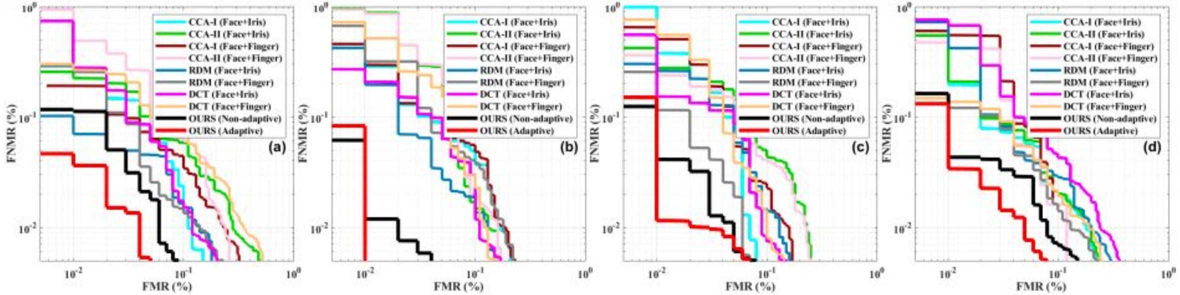

Fig. 3. Detection-Error Tradeoff (DET) Curves, (a) DB-1, (b) DB-2, (c) DB-3, (d) DB-4.

Presentation Attack Analysis

- Experiments are conducted using publicly available benchmark databases.
- Attacks Presentation Classification Error Rate (APCER): ratio of presentation attacks wrongly classified as bona fide or real
- Bona Fide Presentation Classification Error Rate (BPCER): ratio of bona fide presentations wrongly classified as presentation attacks.

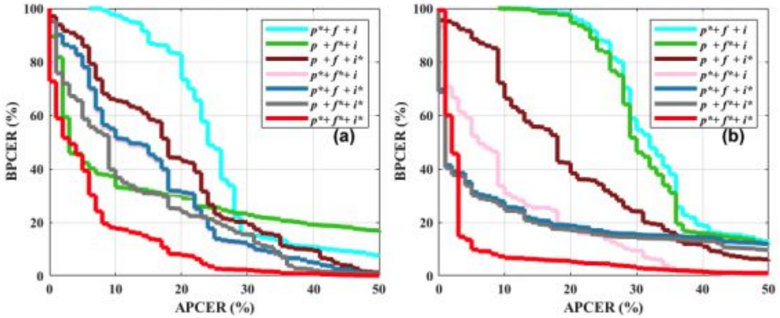

Fig. 9. DET curves for (a) non-adaptive and (b) adaptive AWGF for PAD analysis. k^* = spoofed, k = real, $\forall k \in \{p, f, i\}$

Conclusion & Future Directions

- We proposed a multibiometric system to achieve **high performance along with data protection**.
- **Key images based generic feature extraction** makes template **revocability** a facile procedure, with reduced feature dimension.
- AWGF ensures **complete non-invertibility and unlinkability** of generated biometric templates.
- The proposed system performs favorably against various **security and privacy attacks** and hence suitable for security-critical applications.
- In future, the proposed fusion approach can be improved to inherently **adapt to varying security requirements** through a **dynamic thresholding mechanism**.

References

[20] H. Kaur and P. Khanna, “Random distance method for generating unimodal and multimodal cancelable biometric features,” IEEE Trans. Inf. Forensics Security, vol. 14, 2019.

[36] Y. Yin, L. Liu, and X. Sun, “Sdumla-hmt: a multimodal biometric database,” in Chinese Conference on Biometric Recognition, 2011.

[37] “Casia-fingerprintv5,” http://biometrics.idealtest.org/.

[38] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, “Fingerprint verification competition 2006,” Biometric Technology Today, 2007.

[39] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho et al., “Mcyt baseline corpus: a bimodal biometric database,” IEE Proceedings Vision, Image and Signal Processing, vol. 150, no. 6, pp. 395–401, 2003.

[40] W. Gao, B. Cao, S. Shan, X. Chen, D. Zhou, X. Zhang, and D. Zhao, “The cas-peal large-scale chinese face database and baseline evaluations,” IEEE Trans. Syst., Man, Cybern. A, vol. 38, pp. 149–161, 2008.

[41] “Casia-facev5,” http://biometrics.idealtest.org/.

[42] A. Kumar and A. Passi, “Comparison and combination of iris matchers for reliable personal authentication,” Pattern recognition, vol. 43, 2010.

[43] “Casia iris image database,” http://biometrics.idealtest.org/.

[45] Q.-S. Sun, S.-G. Zeng, Y. Liu, P.-A. Heng, and D.-S. Xia, “A new method of feature fusion and its application in image recognition,” Pattern Recognition, vol. 38, no. 12, pp. 2437 – 2448, 2005.

[46] M. I. Ahmad, W. L. Woo, and S. Dlay, “Non-stationary feature fusion of face and palmprint multimodal biometrics,” Neurocomputing, 2016.