

Processing for template protection

Patrizio Campisi

Dipartimento di Elettronica Applicata,
Università degli Studi “Roma TRE”,
Roma, Italy

campisi@uniroma3.it

www.comlab.uniroma3.it/campisi.htm

Roadmap

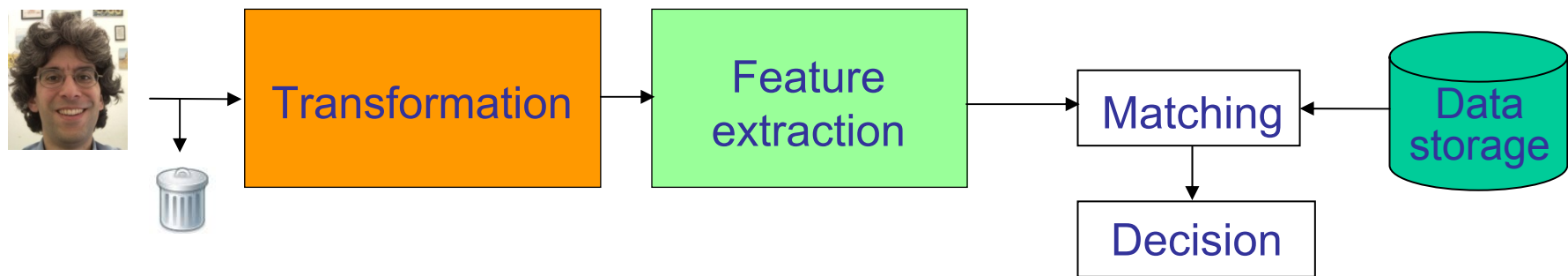
- Biometric template protection:
 - Processing for template protection: state of the art
- BioConvolving (convolution based transformation) approach
 - Security analysis
- BioConvolving: Use of on-line signatures as case study
 - Performance analysis
 - Diversity analysis
- Experimental results
- Conclusions

Biometric template protection

- **Template Protection Schemes Requisites:**
 - **Revocability/Renewability:** it should be possible to revoke a template and generate a new template from the original data;
 - **Diversity:** the stored templates should not allow cross-matching across different databases;
 - **Security:** it should not be possible (or computationally hard) to obtain the original biometric from the secured template;
 - **Performance:** the template protection scheme should not degrade significantly the system performance in terms of FRR and FAR.

Processing for template protection (1/2)

- A transformed version of the original biometrics is stored.
 - The transformation is performed in the **original biometric domain**.



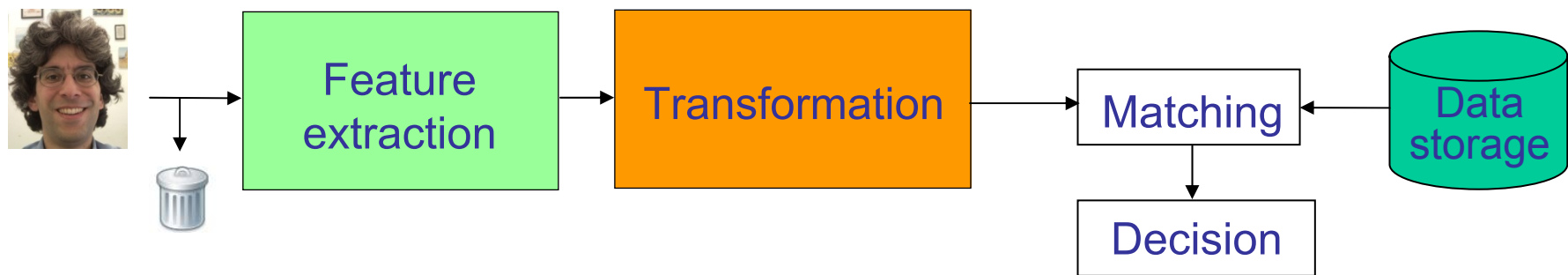
- **Transformation function:**

- invertible,
- non-invertible

- N. Ratha, J. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-based authentication Systems," IBM System Journal, 40, (3), pp. 614-634, 2001.









Processing for template protection (2/2)

- A transformed version of the original biometrics is stored.
 - The transformation is performed in the **feature domain**.



- **Transformation function:**
 - invertible,
 - non-invertible
 - N. Ratha, J. Connell, and R. Bolle, “Enhancing Security and Privacy in Biometrics-based authentication Systems,” IBM System Journal, 40, (3), pp. 614-634, 2001.

Invertible/Non-Invertible transformations

	Invertible	Non-Invertible
Original biometrics discarded		
Revocability Renewability Diversity		
Security		
Design Issues		

Transformation function design: challenges

- **Privacy preserving** of the original biometrics
 - The **recovery** of original biometrics from the transformed data should be computationally **infeasible**.
 - The **transformed data** should **not match** the **original one**.
- **Cross-matching** across different databases should be avoided
 - **Multiple transformations** of the same biometrics should **not match**.

Transformation function design: challenges

- In the transformed domain the **FAR should not increase**
 - The features after transformation should be as representative of the user as the original ones.
- In the transformed domain the **FRR should not increase**
 - The intra-user variability after transformation should not increase.
- **Registration** might be required, for geometric based biometrics, before applying the transformation.
 - Side information not leaking any information about the data should be used.

Processing for template protection: State of the art

- Fingerprints:



- 📖 R. M. Bolle, J. H. Connell, and N. K. Ratha, “*Biometric perils and patches*”, Pattern Recognition 35:2727–2738, 2002.
- 📖 A. B. J. Teoh, D. C. L. Ngo, and A. Goh, “*Biohashing: Two factor authentication featuring fingerprint data and tokenised random number*”, Pattern Recognition 37(11):2245–2255, 2004.
- 📖 N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “*Generating cancelable fingerprint templates*”, IEEE Trans. PAMI, vol. 29, no. 4, pp. 561–572, 2007.
- 📖 S. Chikkerur, N. K. Ratha, J. H. Connell, and R. M. Bolle, “*Generating registration-free cancelable fingerprint templates*”, Proc. IEEE BTAS 2008.

- Voice



- 📖 C. L. Ying and A. B. J. Teoh, “*Probabilistic random projections and speaker verification*”, Lecture Notes Computation Science 4662:445–454, 2007.

Processing for template protection: State of the art

- **Face**

-  M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, “*Cancelable biometric filters for face recognition*”, Proc. ICPR 2004.
-  A. B. J. Teoh, D. C. L. Ngo, and A. Goh, “*Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs*”, IEEE Trans. Pattern Anal. Mach. Intell. 28(12):1892–1901, 2006.

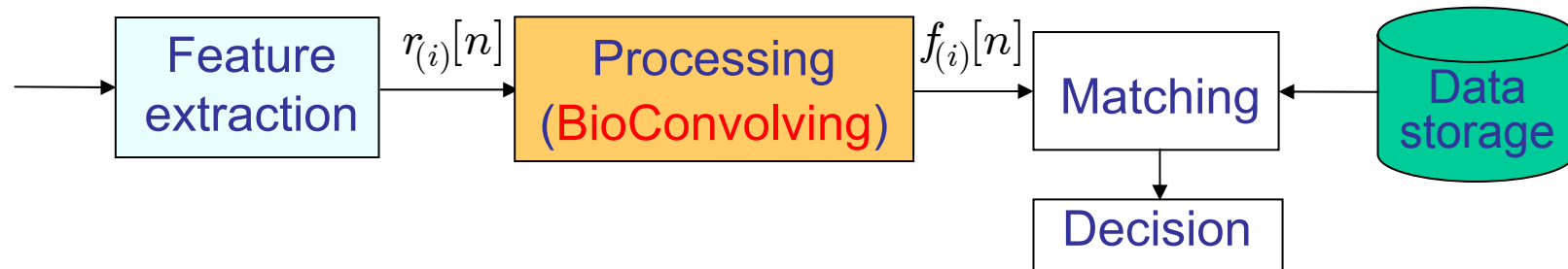
- **Iris**

-  C. S. Chin, A. B. J. Teoh, and D. C. L. Ngo, “*High security iris verification system based on random secret integration*”, Comput. Vis. Image Understanding 102(2):169–177, 2006.
-  Z. Jinyu, N.K. Ratha, J. H. Connell, “*Cancelable iris biometric*”, Proc. ICPR 2008.

Roadmap

- Biometric template protection:
 - Processing for template protection: state of the art
- BioConvolving (convolution based transformation) approach
 - Security analysis
- Use of on-line signatures as case study
 - Performance analysis
 - Diversity analysis
- Experimental results
- Conclusions

BioConvolve⁽¹⁾

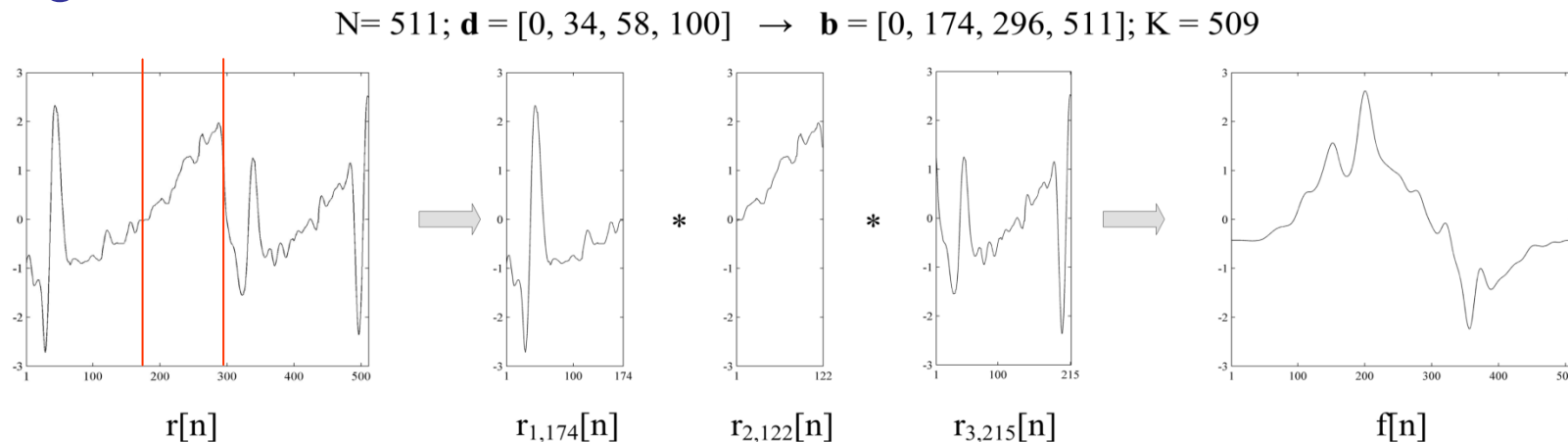


- **Feature set:** set of sequences
- **Processing:** convolution-based transform
- **Matching:**
 - Function modeling (HMM, HMM-UBM),
 - Elastic comparison (DTW).
 - Fusion between different matchers.

⁽¹⁾ E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri "Cancelable Templates for Sequence Based Biometrics with Application to On-line Signature Recognition", IEEE System Man and Cybernetics-Part A, Systems and Humans, vol.40, no.3, May 2010

BioConvolution: Baseline Approach

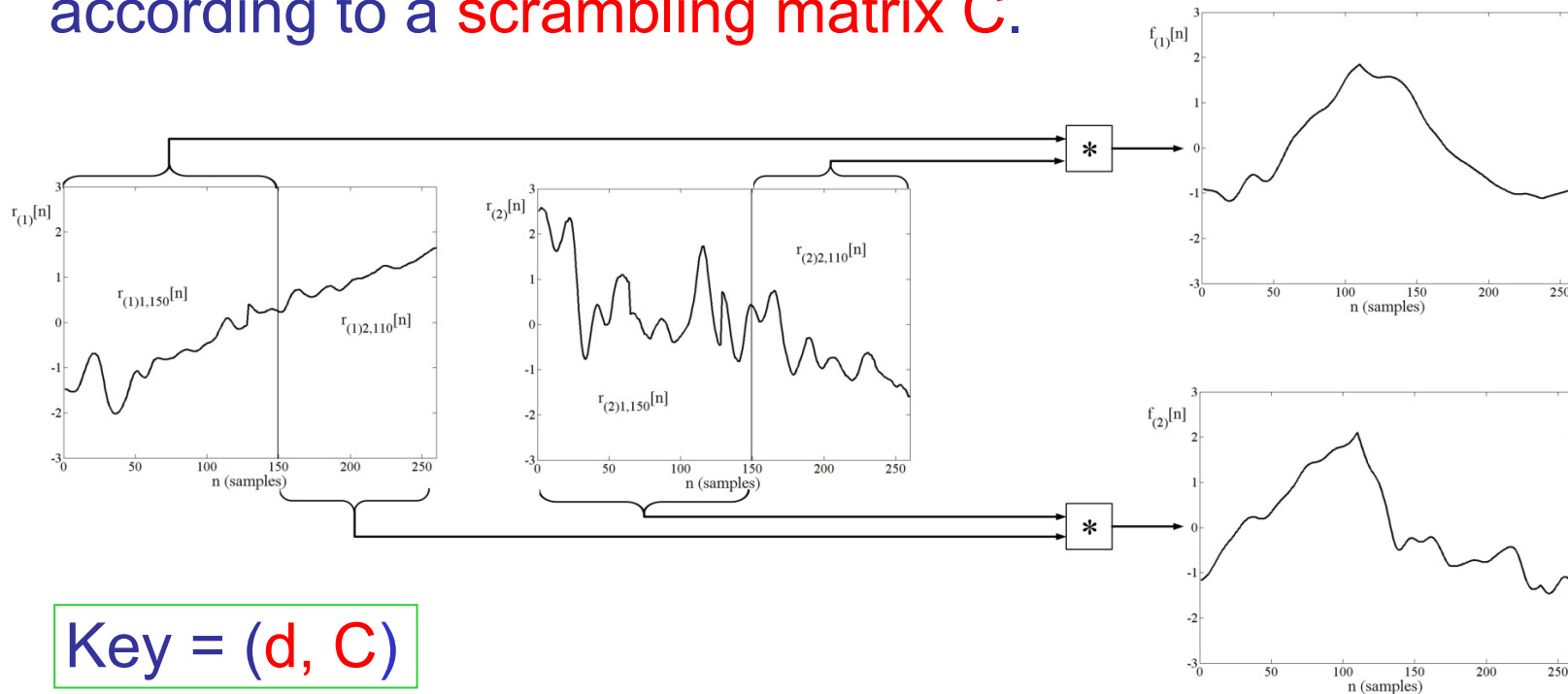
- Each function $r_{(i)}[n]$ is split into w segments according to the same **decomposition key** $\mathbf{d} = [d_0=0, d_1, \dots, d_{w-1}, d_w=N]$.
- Each **transformed function** is obtained **by convolving** the w segments.



Key \mathbf{d} \rightarrow $f_{(i)}[n] = r_{(i),1,N_1}[n] * \dots * r_{(i),w,N_w}[n]$

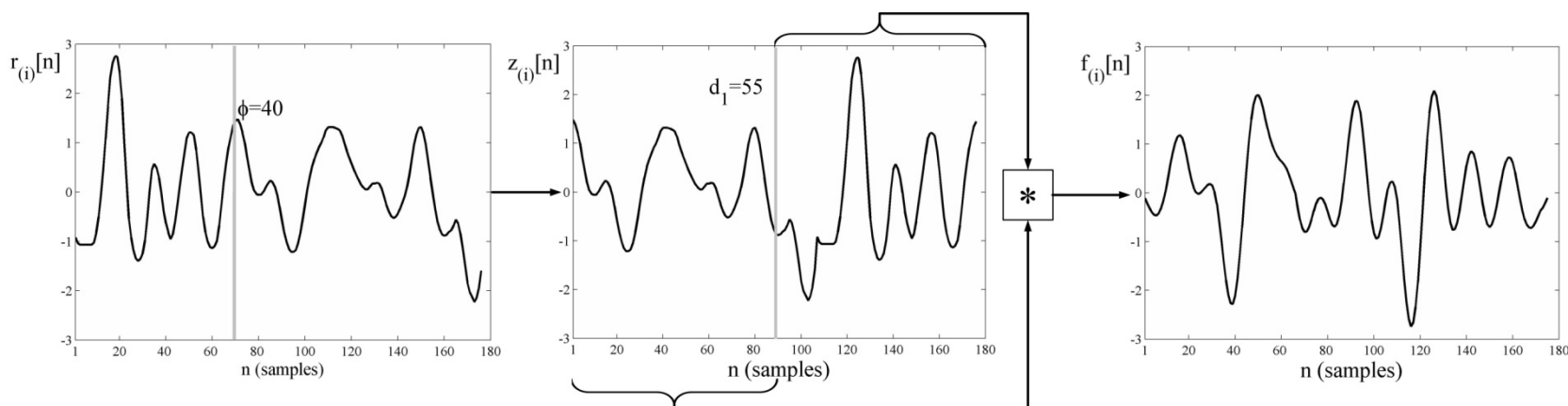
BioConvoluting: Mixing Approach

- Each function is split using the same **decomposition key d** .
- The **transformed functions** are generated by convolving the segments extracted from the different original sequences according to a **scrambling matrix C** .



BioConvolving: Shifting Approach

- Each function is shifted by using a **random shift φ** .
- The transformed functions are generated using the baseline approach.



Key = (φ , d)

Some considerations about security

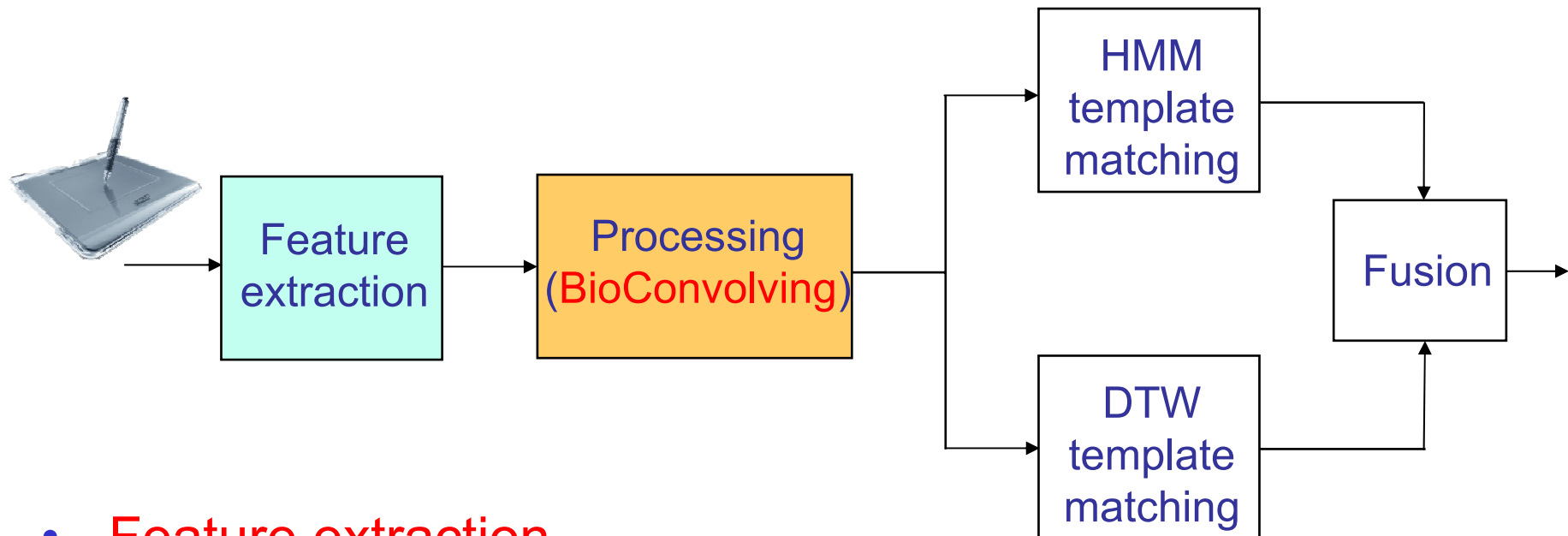
- **Transformation invertibility:**
 - Equivalent to a *blind deconvolution problem* having no a priori knowledge about the original sequence.
- **Record multiplicity attack:**
 - Assumption:
 - two transformed templates obtained from the same original data but with different keys are available to an attacker (worst case scenario).
 - After some math⁽¹⁾:
 - The obtained system of equations admits ∞^1 solutions.

⁽¹⁾ E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, A. Neri "Cancelable Templates for Sequence Based Biometrics with Application to On-line Signature Recognition", IEEE System Man and Cybernetics-Part A, Systems and Humans, vol.40, no.3, May 2010

Roadmap

- Biometric template protection:
 - Processing for template protection: state of the art
 - BioConvolving (convolution based transformation) approach
 - Security analysis
 - Use of on-line signatures as case study
 - Performance analysis
 - Diversity analysis
 - Experimental results
 - Conclusions
-

Signature biometrics: a case study



- **Feature extraction**

- Signatures are acquired using an electronic pad.
- Acquired functions $r_{(i)}[n]$ of length N : horizontal and vertical trajectories, path-tangent angle, velocity, acceleration, log curvature radius, pressure.

Hidden Markov Model based matching^(2,3)

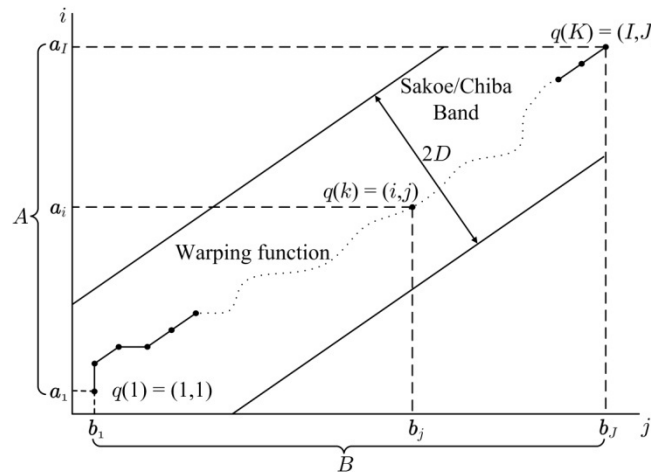
- The transformed functions $f_{(i)}[n]$ (for the baseline, mixing and shifting approach) are modeled using **Hidden Markov Models** (HMM).
- The HMM model parameters of the transformed function are stored in the database.
- The similarity score is calculated using the Viterbi algorithm.

⁽²⁾Maiorana, Martinez-Diaz, Campisi, Ortega-Garcia, Neri, "Template Protection for HMM-based on-line Signature Authentication", *IEEE CVPR 2008, June 2008*.

⁽³⁾Maiorana, Campisi, Ortega-Garcia, Neri, "Cancelable Biometrics for HMM-based Signature Recognition", *IEEE BTAS 08, October 2008*.

Dynamic Time Warping based matching⁽⁴⁾

- Dynamic Time Warping (DTW) finds the best **non-linear alignment** of two sets A and B of different lengths:
 - The overall distance $\Delta_L(A,B)$ between A and B is minimized



$$A = \{a_1, a_2, \dots, a_I\}$$

$$B = \{b_1, b_2, \dots, b_J\}$$

$$L = \{l(k)\} = \{(i(k)), (j(k))\}$$

$$\Delta_L(A,B) = \sum \delta(l(k))$$

- The result of applying DTW gives the dissimilarity score of two signatures.

⁽⁴⁾Maiorana, Campisi, Neri, "Template Protection For Dynamic Time Warping Based Biometric Signature Authentication", DSP 2009, July 2009

Score Fusion

- Score fusion is carried out into two steps:
 - **Score normalization:**

Normalization strategy	Unprotected approach	Baseline Protected approach		
		$W = 2$	$W = 3$	$W = 4$
min-max	2.66	3.91	7.05	7.23
z-score	2.66	3.91	7.05	7.79
median	2.66	3.91	6.77	7.95
double sigmoid	2.48	4.09	6.23	7.44
tanh	2.66	3.91	7.05	7.79

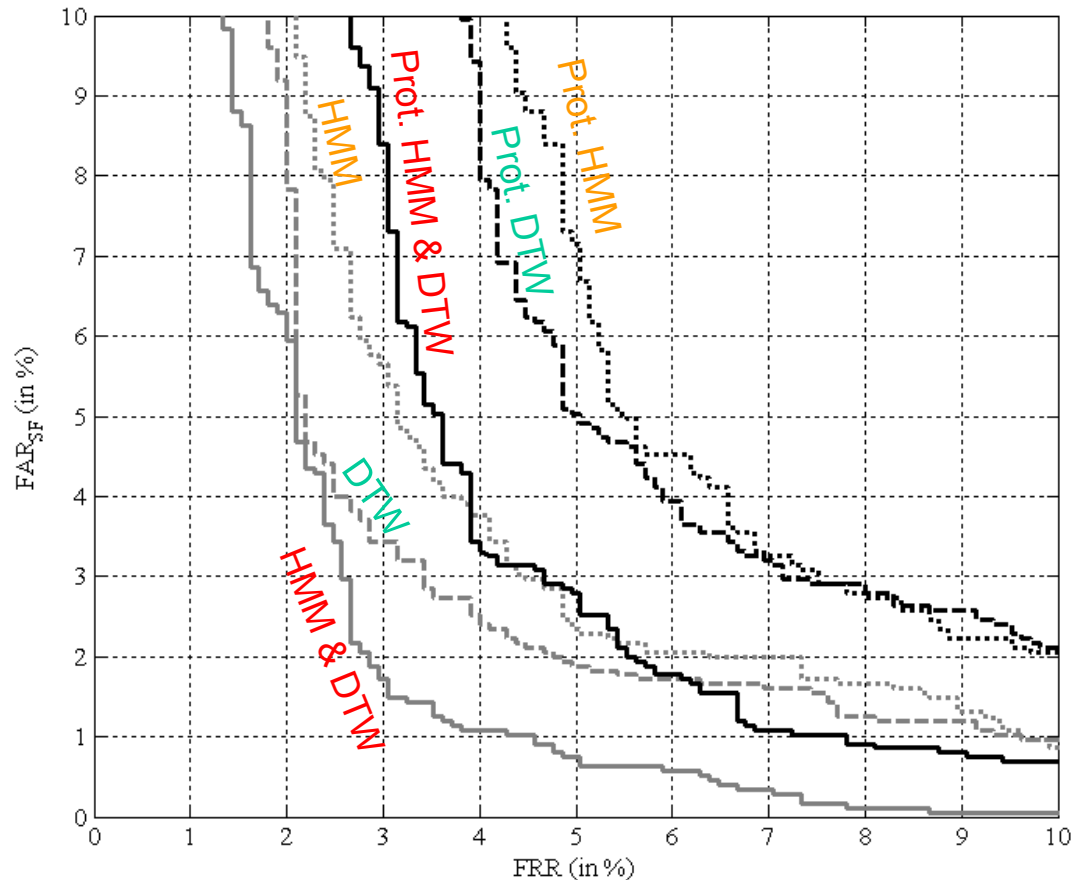
- **Fusion** of the normalized match scores:

Fusion rule	Unprotected approach	Baseline Protected approach		
		$W = 2$	$W = 3$	$W = 4$
sum	2.66	3.91	7.05	7.23
product	2.66	3.95	6.07	7.62
maximum	3.56	4.34	6.60	13.14
minimum	2.70	5.00	10.36	8.17

Performance analysis: Experimental set up

- Public MCYT database of 100 users, with 25 genuine and 25 skilled forgeries captured in 5 different sessions.
- **Enrollment:**
 - 5 signatures from the first session are selected and transformed using a key $\mathbf{d}^{(e)}$
- **FRR:**
 - 20 remaining signatures are used after being transformed using the same key $\mathbf{d}^{(e)}$
- **FAR_{SF} :**
 - Skilled forgeries: transformed using the same key $\mathbf{d}^{(e)}$

Performance analysis: baseline



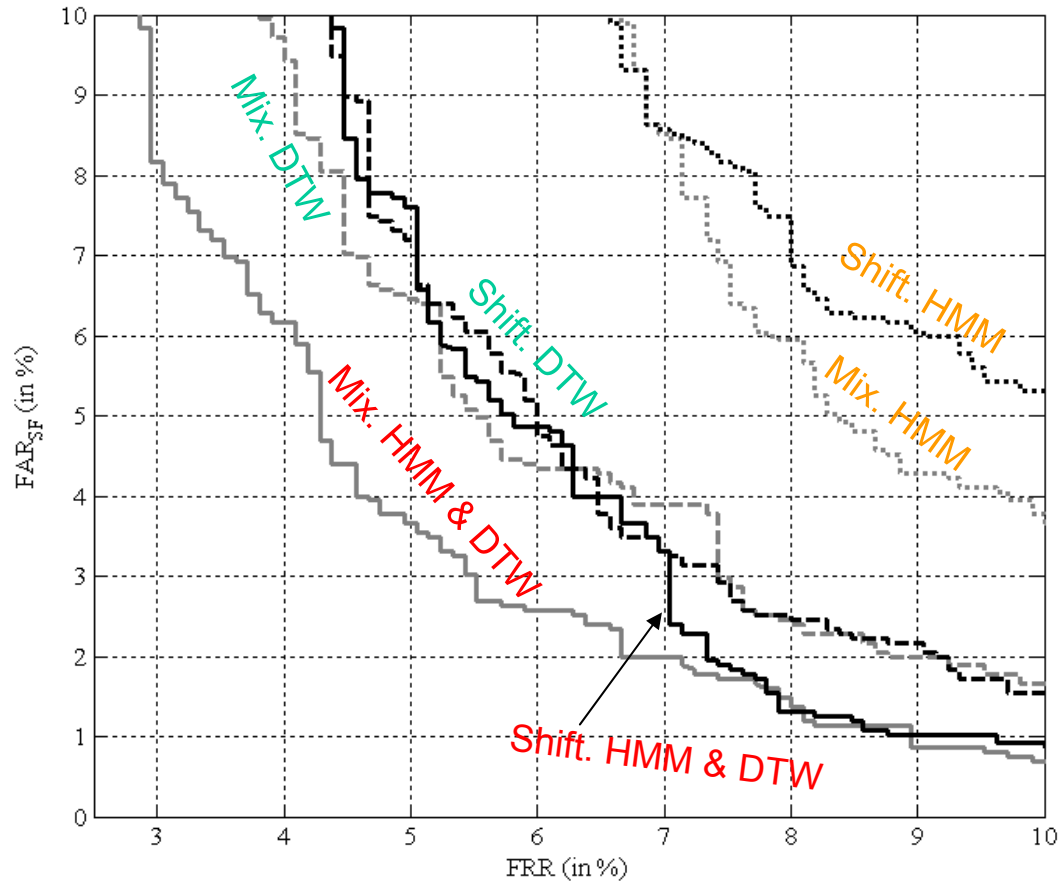
HMM model
 H=16 states
 M=8 Gaussian
 mixture for each
 state

DTW
 D=5%

ERR _{SF} (%)	HMM&DTW	HMM	DTW
Protected	3.9	5.4	5.0
Unprotected	2.6	3.9	3.2

Protection implemented using a baseline approach with $W=2$

Performance analysis: extended approaches



HMM model
 H=16 states
 M=8 Gaussian
 mixture for each
 state

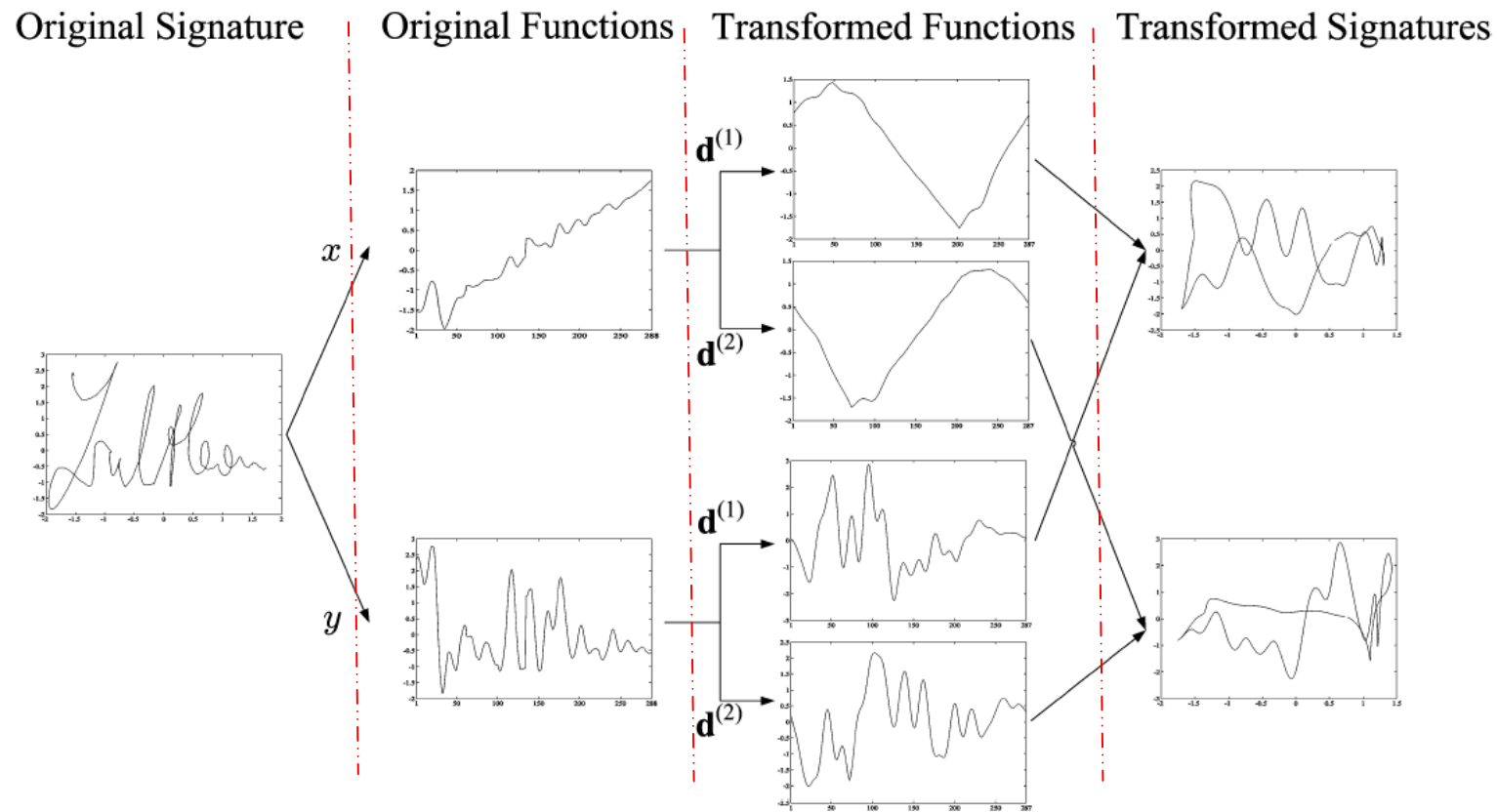
DTW
 D=5%

ERR _{SF} (%)	HMM&DTW	HMM	DTW
Protected Mixing	4.4	7.4	5.3
Protected Shifting	5.4	7.7	5.7

Protected extended approaches implemented using a baseline approach with W=2.

Diversity Analysis (1/2)

- By varying the key \mathbf{d} , we can generate different realizations from a single original function.



Diversity Analysis (2/2)

- Which is the **minimum distance between two keys** to obtain different “enough” replica of the data?
- **Criterion:** replicas of the same signature are different (enough) when they behave like signatures taken from different users.
 - The probability of matching templates generated from the same data with different (enough) keys should be comparable to the FAR_{RF}

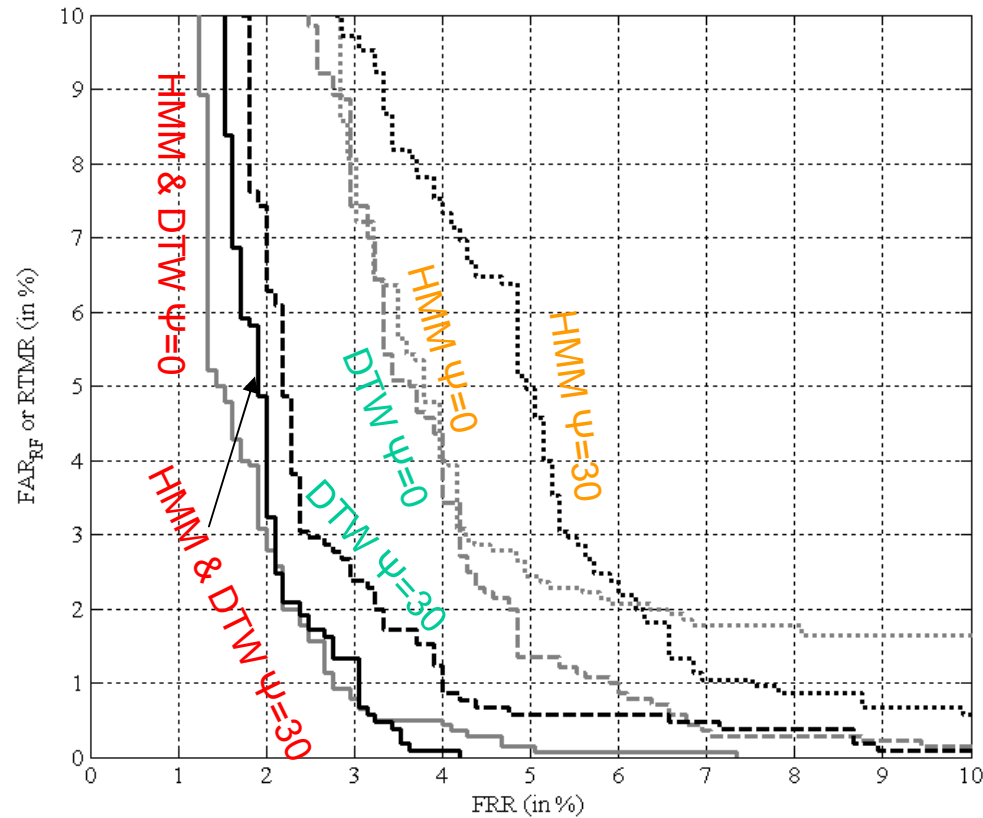
- Measures:

- Baseline: $\Psi(\mathbf{d}^{(1)}, \mathbf{d}^{(2)}) = \sum_{i=1}^{W-1} |d_i^{(1)} - d_i^{(2)}|$

- Mixing: $\Omega(\mathbf{C}^{(1)}, \mathbf{C}^{(2)}) = \text{number of different rows}$

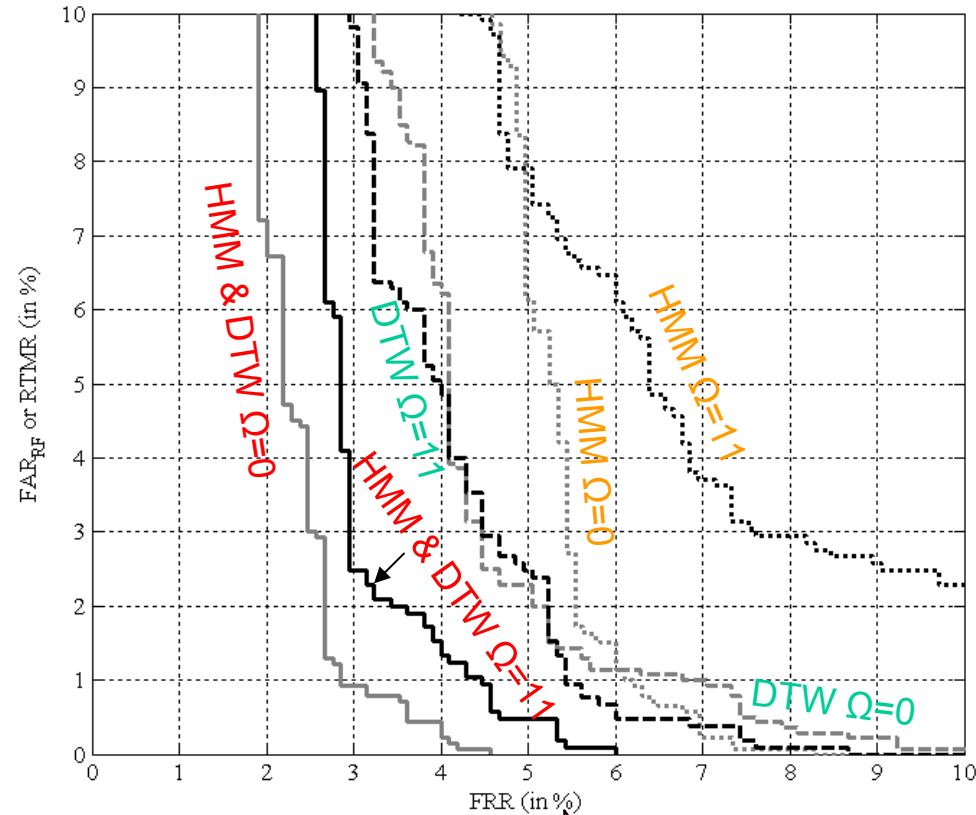
- Shifting: $\Phi(\varphi^{(1)}, \varphi^{(2)}) = |\varphi^{(1)} - \varphi^{(2)}|$

Diversity analysis: baseline approach



Acceptable distance $\Psi(d^{(e)}, d^{(a)}) \geq 30$  Maximum $\Gamma = 4$ different keys ($w=2$)

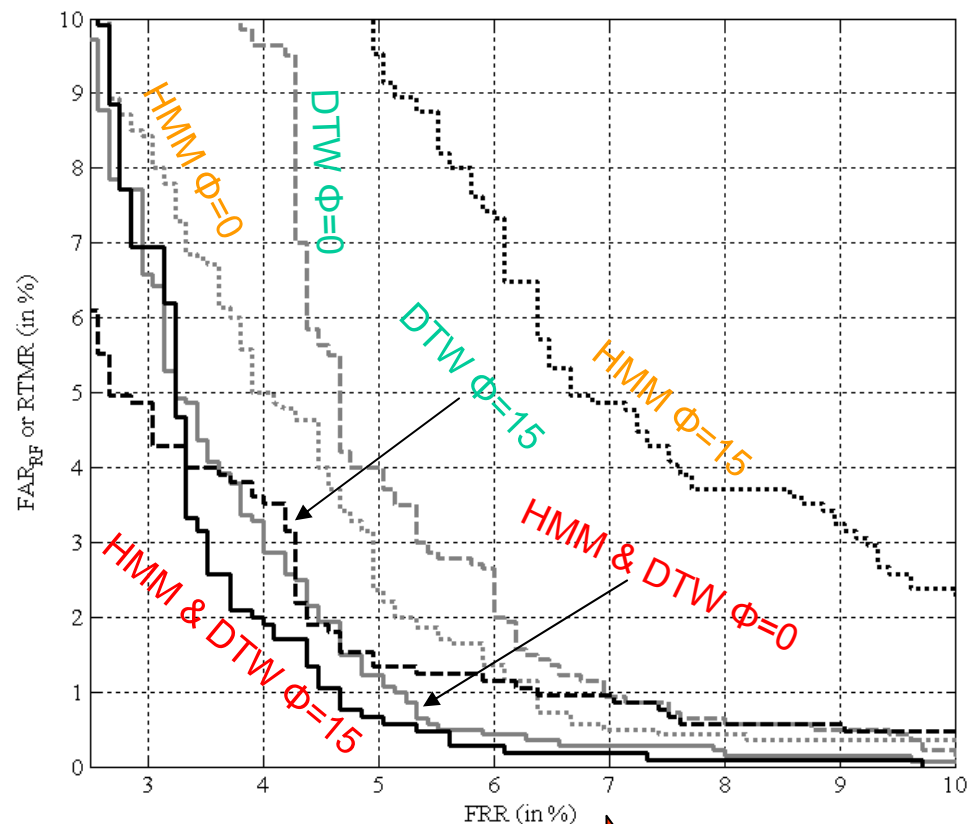
Diversity analysis: Function Mixing



Acceptable distance $\Omega (C^{(e)}, C^{(a)}) \geq 11$  Maximum ~24.000 different keys C

Maximum number of allowed keys (d, C) is $\sim 4 \cdot 24.000 = 96.000$

Diversity analysis: Function Shifting



Acceptable distance Φ ($\varphi^{(e)}$, $\varphi^{(a)}$) ≥ 15 \rightarrow Maximum 7 different keys φ

Maximum number of allowed keys (d , φ) is $4 \cdot 7 = 28$

Conclusions

- **BioConvolving** is a template protection mechanism based on the use of non-invertible transforms
 - **Baseline approach**: convolution among segments of the signature functions
 - **Extended approaches**:
 - Function mixing
 - Function shifting
- **BioConvolving** fulfills the requirements of a template protection scheme.
- **BioConvolving** be applied in principle to any **function-based biometrics**.

References

- E. Maiorana, P. Campisi , J. Fierrez, J. Ortega-Garcia, A. Neri “*Cancelable Templates for Sequence Based Biometrics with Application to On-line Signature Recognition*”, IEEE System Man and Cybernetics-Part A, Systems and Humans, vol.40, no.3, May 2010.
- Maiorana, Martinez-Diaz, Campisi, Ortega-Garcia, Neri, “*Template Protection for HMM-based on-line Signature Authentication*”, IEEE CVPR 2008, June 2008.
- Maiorana, Campisi, Ortega-Garcia, Neri, “*Cancelable Biometrics for HMM-based Signature Recognition*”, IEEE BTAS 08, October 2008.
- Maiorana, Campisi, Neri, “*Template Protection For Dynamic Time Warping Based Biometric Signature Authentication*”, DSP 2009, July 2009.
- Maiorana, Campisi, Neri “*Bioconvolving: Cancelable Templates for a Multi-Biometrics Signature Recognition System*”, IEEE International Systems Conference 2011, Special Session on Privacy and Biometrics, Montreal, April 2011.
- Maiorana, Campisi, Neri, “*Cancelable Biometrics for On-line Signature Recognition*”, in New Technologies for Digital Crime and Forensics: Devices, Applications, and Software, eds. C.T.Li and A. T.S. Ho, IGI 2011.

Thanks for your attention !!

campisi@uniroma3.it

www.comlab.uniroma3.it/campisi.htm