BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/

Funded under the 7th FP (Seventh Framework Programme)

Theme SEC-2011.5.1-1
[Evaluation of identification technologies, including Biometrics]

D8.3: Final dissemination activities

Due date: 31/12/2015
Submission date: 29/02/2016
Project start date: 01/03/2012
Duration: 48 months
WP Manager: Julien Bringer (MORPHO)
Revision: 1

Author(s): S. Marcel (IDIAP), A. Anjos (IDIAP), M. Gomez-Barrero (UAM), J. Fierrez (UAM), K. Mitrokotsa (CHALMERS), C-H. Chan (UNIS), J. Bringer (MORPHO), C. Karabat (TUBITAK), B. Topçu (TUBITAK), A. Merle (CEA), E. Kindt (KUL) and N. Tekampe (TU-VIT)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D8.3: Final dissemination activities

Abstract:

This deliverable is a final report on the dissemination activities carried out in the project. First it reviews shortly the audience of the project website. Second it builds an inventory of scientific publications (international conferences, journals and books) and scientific events. It also presents examples of dissemination in news/press and the BEAT related workshops or main actions organized. Finally the deliverable provides a short list of actions planned for this final year although the project will be completed.

Contents

1 Website Analytics

In the following, we report some web statistics using Google Analytics on two of our websites:

- the main BEAT project website: `https://www.beat-eu.org/`,
- the BEAT platform website: `https://www.beat-eu.org/platform`.

With respect to the project website, we note also that the publication page `https://www.beat-eu.org/publications` was deprecated to refer instead to this deliverable.

1.1 BEAT main website

The figure 1 shows the web statistics of the BEAT main website from April 2012 to February 2016. Indeed the BEAT website was operational on the first month of the project (March 2012) and the statistics started the following month.

As it can be observed the BEAT project website attracted regular visitors during the whole project with in average more than 100 sessions per weeks and to date a bit more than 12000 visitors. We also observe an increase of traffic early 2013. We assume that this is correlated with the face and speaker recognition competitions (`https://www.beat-eu.org/evaluations`) that BEAT organized in conjunction with the International Conference on Biometrics (ICB2013). A second increase of traffic occurred late 2013. We assume that this is correlated with a tutorial on spoofing and anti-spoofing (`http://www.idiap.ch/~marcel/professional/BTAS_2013.html`) given by IDIAP at the IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2013).

1.2 BEAT platform website

The figure 2 shows the web statistics of the BEAT platform website from late 2015 to February 2016. Indeed the BEAT platform website was made available very early for beta testing, actually already in 2014, but the web statistics were added later when we started to organize tutorials for BEAT platform users.

As we can observe the BEAT platform website attracted a variable number of visitors. This is due to various dissemination actions (project proposals, mailing lists, presentations and demonstrations). Nevertheless, we observe a bit more than 1500 visitors and 2000 sessions in only 4 month which represents an average of 50 sessions per days. Comparing to the BEAT main website, it is interesting to notice that in average a session visits about 7 pages and stays 7 minutes as opposed to the 2 pages and 1.5 minutes on the BEAT main website.

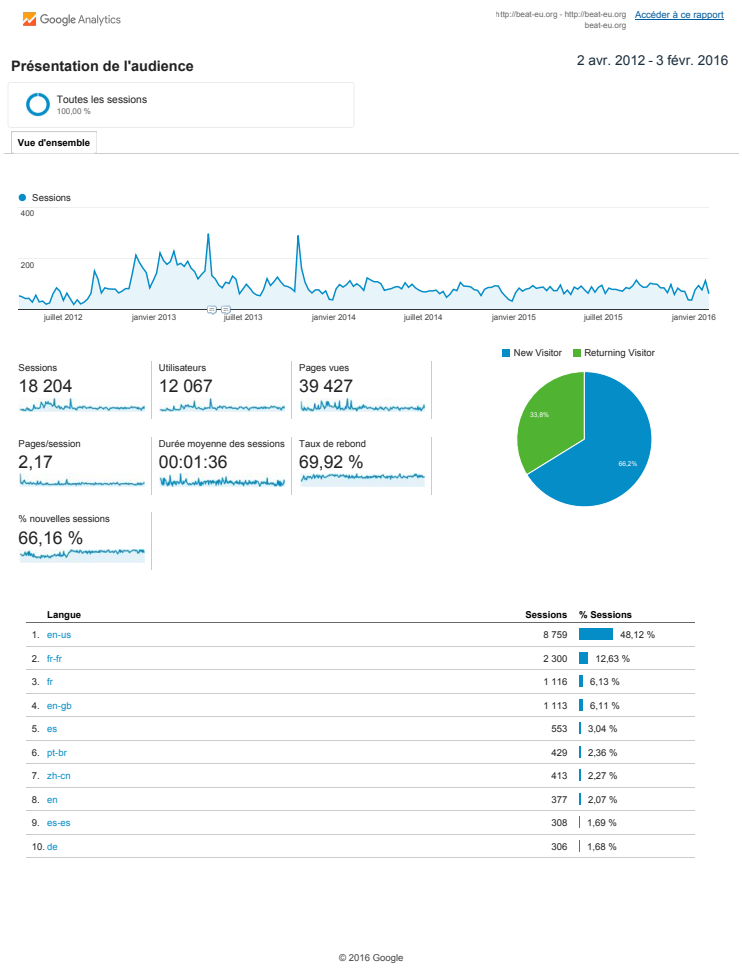

Figure 1: Google Analytics of the BEAT website.

2 Current or achieved dissemination activities

In the following, we report all the dissemination activities which BEAT partners, jointly or independently each others, are currently conducting or conducted successfully. Some of these dissemination activities include scientific publications in journals or conferences and are sumarized in the table below.

	IDIAP	UAM	UNIS	EPFL	CHA	TUBITAK	CEA	MORPHO	KUL	TUVIT
conferences	9	18	11	1	4	6	2	5	0	1
journals	3	12	12	0	0	2	0	3	2	0
books	2	1	4	0	0	0	0	1	1	0
events	11	5	4	0	3	9	3	3	8	2

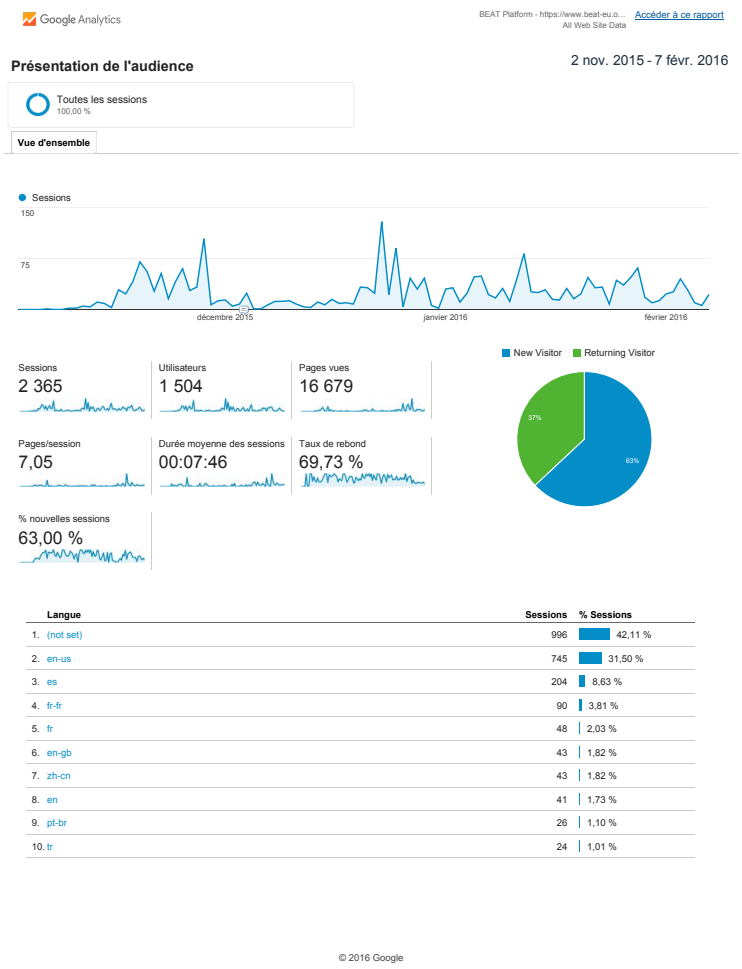

Figure 2: Google Analytics of the BEAT platform.

2.1 Accepted papers in conferences

List of papers with a reference to BEAT.

2.1.1 IDIAP

"SPEAR: An open source toolbox for speaker recognition based on Bob", E. El Khoury, L. El Shafey and S. Marcel, Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2014

[`http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6853879`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

This paper is directly relevant to WP3 "Evaluation of Biometric Performance" and WP7 "Integration and Deployment". The paper presents an open-source implementation of a speaker recognition toolchain developed in the context of the WP3 and the WP7 for inclusion on the BEAT platform. As a matter of fact speaker recognition algorithms are available on the BEAT platform.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Face Anti-Spoofing Based on General Image Quality Assessment", J. Galbally and S. Marcel, IEEE International Conference on Pattern Recognition (ICPR), 2014

[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6976921]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper explores the use of image quality assessment metrics for the task of face anti-spoofing.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Hierarchical speaker clustering methods for the NIST i-vector Challenge", E. El Khoury, L. El Shafey, M. Ferras and S. Marcel, Odyssey: The Speaker and Language Recognition Workshop, 2014

[http://publications.idiap.ch/index.php/publications/show/2839]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper presents a novel speaker recognition algorithm using the SPEAR toolkit mentioned above and ready or possible inclusion on the BEAT platform.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Can face anti-spoofing countermeasures work in a real world scenario ?", T. de Freitas Pereira, A. Anjos, J. Mario de Martino and S. Marcel, International Conference on Biometrics, 2013

[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6612981]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper studies the generalization of a set of face anti-spoofing algorithms on several spoofing databases.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was jointly performed with colleagues from "Universidade Estadual de Campinas" (UNICAMP) in Brazil. Indeed UNICAMP is also studying spoofing and anti-spoofing in face recognition. Hence we collaborated to explore how our separately developed algorithms where performing on common benchmarks. This collaboration resulted in this publication.

"Complementary Countermeasures for Detecting Scenic Face Spoofing Attacks", A. Anjos, J. Komulainen, A. Hadid, M. Pietikainen and S. Marcel, International Conference on Biometrics, 2013

[`http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6612968`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper proposes a method to fuse multiple anti-spoofing algorithms and measures its improvement compared to the use of anti-spoofing algorithm independently.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was jointly performed with colleagues from the University of Oulu (UOULU) in Finland. Indeed UOULU is also studying spoofing and anti-spoofing in face recognition. Hence we collaborated to explore how the fusion of separately developed algorithms was improving for the task of anti-spoofing. This collaboration resulted in this publication.

"Bob: A Free Signal Processing and Machine Learning Toolbox for Researchers", A. Anjos, L. El Shafey, R. Wallace, M. Günther, C. Mccool and S. Marcel, 20th ACM Conference on Multimedia Systems (ACMMM), 2013

[`http://dl.acm.org/citation.cfm?id=2396517`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP7 "Integration and Deployment". The paper presents the BOB open-source signal processing and machine learning toolbox. This library is a core component of the BEAT platform. It was designed

and developed with the aim to allow reproducible research. As a matter of fact, BOB is actually installed on the BEAT platform to provide algorithms of the platform with basic or advanced features.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"On the vulnerability of finger vein recognition to spoofing", P. Tome and S. Marcel, IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2014.

[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7029416]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper presents the first reproducible study on finger vein spoofing with an open finger vein sensor and a novel spoofing database for that task. The study shows that it is possible to forge a spoofing attack for finger vein using printed veins on paper in a particular way, and that this spoofing attack is successful, to some extent, to be recognized as a genuine enrolled user.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"On the Vulnerability to Palm Vein Recognition to Spoofing Attacks", P. Tome and S. Marcel, International Conference on Biometrics (ICB), 2015.

[http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7139056]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper presents the first reproducible study on palm vein spoofing with an open palm vein sensor and a novel spoofing database for that task. The study shows that it is possible to forge a spoofing attack for palm vein using printed veins on paper in a particular way, and that this spoofing attack is successful, to some extent, to be recognized as a genuine enrolled user.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks", P. Tome and S. Marcel and al., International Conference on Biometrics (ICB), 2015.

[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7139067]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper presents the results of the first international competition on finger vein anti-spoofing. The same finger vein database used for the evaluation of spoofing was also used for developing and testing finger vein anti-spoofing.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  Given that we organized an international competition several research teams outside the consortium were competing on the same task and data. Results from this competition are presented in this paper.

2.1.2 UAM

"Security Evaluation of i-Vector Based Speaker Verification Systems Against Hill-Climbing Attacks", M. Gomez-Barrero, J. Gonzalez-Dominguez, J. Galbally and J. Gonzalez-Rodriguez, Int. Speech Communication Association Conference (InterSpeech), 2013

[http://hdl.handle.net/10486/663061]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper explores the impact of hill-climbing attacks to speaker recognition systems.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Multimodal Biometric Fusion: a Study on Vulnerabilities to Indirect Attacks", M. Gomez-Barrero, J. Galbally, J. Fierrez and J. Ortega-Garcia, Iberoamerican Congress on Pattern Recognition (CIARP), 2013

[http://hdl.handle.net/10486/664007]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper explores the impact of hill-climbing attacks to multimodal biometric systems.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"Face Anti-Spoofing Based on General Image Quality Assessment", J. Galbally and S. Marcel, IAPR/IEEE Int. Conf. on Pattern Recognition (ICPR), 2014

[http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6976921]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper explores the impact of direct attacks to face biometric and develops new anti-spoofing methods based on image quality measures.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters", M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez and C. Busch, IAPR/IEEE Int. Conf. on Pattern Recognition (ICPR), 2014

[http://hdl.handle.net/10486/664664]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper presents a new method to protect face templates that enables privacy preservation.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  This work was mainly conducted by M. Gomez-Berrero, a PhD student at UAM, during a research stay with Prof. Dr. C. Busch at University of Darmstadt (Germany). Prof. Busch is a renowned expert in biometric security, which helped with his expertise using cutting edge methods (in this case Bloom Filters).

"Towards predicting good users for biometric recognition based on keystroke dynamics", A. Morales, J. Fierrez and J. Ortega-Garcia, European Conference on Computer Vision (ECCV), 2014

[http://hdl.handle.net/10486/665359]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper develops methods to characterize different subjects classify them in classes depending their individual performance for biometric authentication.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"Generation of Enhanced Synthetic Off-line Signatures Based on Real On-line Data", M. Diaz-Cabrera, M. Gomez-Barrero, A. Morales, M. A. Ferrer and J. Galbally, IAPR International Conference on Frontiers in Handwriting Recognition (ICFHR), 2014

[http://hdl.handle.net/10486/663865]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". This paper proposes a novel method for the generation of synthetic offline signatures with application to performance evaluation.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  This work was done in collaboration with the IDeTIC lab at Universidad Las Palmas de Gran Canaria (Spain). Prof. Dr. M. A. Ferrer is a renowned expert in signature and handwriting based biometrics, and helped here with his expertise on off-line signatures.

"Towards Cancelable Multi-Biometrics based on Adaptive Bloom Filters: A Case Study on Feature Level Fusion of Face and Iris", C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally and J. Fierrez, International Workshop on Biometrics and Forensics (IWBF), 2015

[http://hdl.handle.net/10486/667126]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper presents a new method to protect multimodal face and iris templates that enables privacy preservation.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  This work was mainly conducted by M. Gomez-Berrero, a PhD student at UAM, during a research stay with Prof. Dr. C. Busch at University of Darmstadt (Germany). Prof. Busch is a renowned expert in biometric security, which helped with his expertise using cutting edge methods (in this case Bloom Filters).

"Enhanced On-Line Signature Verification Based on Skilled Forgery Detection Using Sigma-LogNormal Features", M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia and R. Plamondon, IEEE/IAPR International Conference on Biometrics (ICB), 2015

[http://hdl.handle.net/10486/667298]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance" and WP4 "Evaluation of Vulnerabilities". The paper proposes a novel scheme, based on the Kinematic Theory of rapid human movements to improve the performance and robustness to skilled forgeries of on-line signature verification systems.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was mainly conducted by M. Gomez-Barrero, a PhD student at UAM, in collaboration with Prof. Dr. Plamondon from Universite de Montreal (Canada). Dr. Plamondon is a renowned expert in signature and handwriting analysis and processing, and helped here with his experience in proposing the skilled forgeries detector.

"Optimal Feature Selection and Inter-Operability Compensation for On-Line Biometric Signature Authentication", R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, IEEE/IAPR International Conference on Biometrics (ICB), 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7139047]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper describes a two-stage method for the device compensation and interoperability for on-line signature verification.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Pose Variability Compensation using Projective Transformation for Forensic Face Recognition", E. Gonzalez-Sosa, R. Vera-Rodriguez, J. Fierrez, P. Tome and J. Ortega-Garcia, International Conference of the Biometrics Special Interest Group (BIOSIG), 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7314615]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper analysis the impact of the projective transformation for the compensation of pose distortion present in surveillance images in forensic scenarios.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"e-BioSign Tool: Towards Scientific Assessment of Dynamic Signatures under Forensic Conditions", R. Vera-Rodriguez, J. Fierrez, J. Ortega-Garcia, A. Acien and R. Tolosana, IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7358756]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper describes the design, acquisition process and a baseline evaluation of e-BioSign, a new database of dynamic signature and handwriting on mobile devices.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Keystroke Dynamics Recognition based on Personal Data: A Comparative Experimental Evaluation Implementing Reproducible Research", A. Morales, M. Falanga, J. Fierrez, C. Sansone and J. Ortega-Garcia, IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7358772]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance" and WP7 "Integration and Deployment". The paper proposes a new benchmark for keystroke dynamics recognition on the basis of fully reproducible research, implemented on the BEAT platform. **Includes Attestation of experiments conducted on the BEAT platform**.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  Part of this work was carried out by M. Falanga, a MSc student at University of Naples Federico II (Italy), during a research stay with Dr. A. Morales at UAM. Prof. Dr. C. Sansone is a renowned expert in the fields of pattern recognition and graph matching, which helped with his expertise on graph matching applied to keystroke dynamics.

"Increasing the Robustness of Biometric Templates for Dynamic Signature Biometric Systems", R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, Annual International Carnahan Conference on Security Technology, 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7389687]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper studies the impact of not considering information related to the X and Y coordinates and their derivatives on signature verification systems.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Score Normalization for Keystroke Dynamics Biometrics", A. Morales, E. Luna, J. Fierrez and J. Ortega-Garcia, Annual International Carnahan Conference on Security Technology, 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7389686]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper analyses the effects of score normalization on keystroke dynamics authentication systems.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Update Strategies for HMM-Based Dynamic Signature Biometric Systems", R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, IEEE Int. Workshop on Information Forensics and Security (WIFS), 2015

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7368583]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The main goal of this work is to study system configuration update strategies of time functions-based systems for scenarios where the number of training signatures available is variable, taking into account the lap of time between them (inter-session variability).

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"Variable-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics", M. Gomez-Barrero, J. Galbally and J. Fierrez, Int. Workshop on Biometrics and Forensics, 2016

[Not yet published, will be available soon at IEEE Xplore]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper presents a new method to protect variable-length templates based on Homomorphic Encryption that enables privacy preservation.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"A Review of Iris Anti-Spoofing", J. Galbally and M. Gomez-Barrero, Int. Workshop on Biometrics and Forensics, 2016

[Not yet published, will be available soon at IEEE Xplore]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper presents a survey on anti-spoofing methods for iris biometrics.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

2.1.3 UNIS

"Blur kernel estimation to improve recognition of blurred faces", Chi Ho Chan and J. Kittler, 19th IEEE International Conference on Image Processing (ICIP), 2012

[`http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6467278`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP3 Evaluation of Biometric Performance. This paper proposes an efficient blind deconvolution method to deblur face images for face recognition. The method involves a salient edge map construction,

blur kernel estimation and face image deconvolution. The kernel estimation method can be used to synthese the blurred face image for face recognition evaluation.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"A discriminative parametric approach to video-based score-level fusion for biometric authentication", N. Poh, J. Kittler, F. Alkoot, 21st International Conference on Pattern Recognition (ICPR), 2012

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6460633]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 Evaluation of Biometric Performance. It investigates a discriminative video-based score-level fusion mechanism, which enables an existing biometric system to further harness the riches of temporarily sampled biometric data using a set of distribution descriptors
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation: Dr. Alkoot contributed to the work during his visit to CVSSP. n/a

"A facial symmetry prior for improved illumination fitting of 3D morphable model", Guosheng Hu, Pouria Mortazavian, Josef Kittler and William J. Christmas, International Conference on Biometrics (ICB), 2013

[http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6613000]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The paper is addressing the problem of 3D face model fitting to 2D images for pose and illumination invariant face recognition. The work is directly relevant to WP3. It provides a method of geometric normalization of face images of arbitrary pose. The symmetry prior improves the fitting performance. It helps to disambiguate skin texture from illumination.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Feature Level Multiple Model Fusion Using Multilinear Subspace Analysis with Incomplete Training Set and Its Application to Face Image Analysis", Zhen-Hua Feng, Josef Kittler, William J. Christmas and Xiaojun Wu, Multiple Classifier Systems (MCS), 2013

[http://link.springer.com/chapter/10.1007%2F978-3-642-38067-9_7#]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The paper is addressing the problem of face recognition using tensor 2D face model, which can represent multiple factors of variability, including pose and illumination. It focuses on the problem of missing entries in the tensor representation and how to reconstruct the missing values. The work is directly relevant to WP3. It facilitates pose and illumination invariant face recognition.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Robust face recognition by an albedo based 3D morphable model", G Hu, CH Chan F Yan, J Kittler and W Christmas, in Biometrics (IJCB), 2014 IEEE International Joint Conference on, 2014.

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6996223]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 Evaluation of Biometric Performance. This paper proposes an effective methods for pose and illumination invariant face recognition. Unlike the traditional idea of separating the albedo and illumination contributions using a 3DMM, we propose a novel Albedo Based 3D Morphable Model (AB3DMM), which removes the illumination component from the images using illumination normalization in a preprocessing step.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"A multiresolution 3D morphable face model and fitting framework", P Huber, G Hu, R Tena, P Mortazavian, P Koppen, WJ Christmas, R atsch M, J Kittler, 11th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, 2016

[http://www.patrikhuber.ch/files/3DMM_Framework_VISAPP_2016.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The work is directly relevant to WP3. It facilitates pose and illumination invariant face recognition. In this paper, we present the Surrey Face Model, a multi-resolution 3D Morphable Model that we make available to the public for non-commercial purposes. The model contains different mesh resolution levels and landmark point annotations as well as metadata for texture remapping. Accompanying the model is a lightweight open-source C++ library designed with simplicity and ease of integration as its foremost goals. In addition to basic functionality, it contains pose estimation and face frontalisation algorithms. With

the tools presented in this paper, we aim to close two gaps. First, by offering different model resolution levels and fast fitting functionality, we enable the use of a 3D Morphable Model in time-critical applications like tracking. Second, the software library makes it easy for the community to adopt the 3D Morphable Face Model in their research, and it offers a public place for collaboration

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Fitting 3D morphable models using local features", P Huber P, Z Feng Z, WJ Christmas, J Kittler, M Raetsch, IEEE International Conference on Image Processing (ICIP), 2015

[http://arxiv.org/pdf/1503.02330.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The work is directly relevant to WP3. It facilitates pose and illumination invariant face recognition. It proposes a novel fitting method that uses local image features to fit a 3D Morphable Model to 2D images. To overcome the obstacle of optimizing a cost function that contains a non-differentiable feature extraction operator, we use a learning-based cascaded regression method that learns the gradient direction from data. The method allows to simultaneously solve for shape and pose parameters. Our method is thoroughly evaluated on Morphable Model generated data and first results on real data are presented. Compared to traditional fitting methods, which use simple raw features like pixel color or edge maps, local features have been shown to be much more robust against variations in imaging conditions. Our approach is unique in that we are the first to use local features to fit a Morphable Model. Because of the speed of our method, it is applicable for real-time applications. Our cascaded regression framework is available as an open source library
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Toward an Attack-sensitive Tamper-resistant Biometric Recognition with a Symmetric Matcher: A Fingerprint Case Study", N. Poh, R. Wong, G-L Marcialis, IEEE Symposium on Computational Intelligence in Biometrics and Identity Management, 2014

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7015460]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The work is directly relevant to WP4. In this study, we consider zero-effort impostor attack (referred to as the Z-attack), nonzero-effort impostor attack such as presentation attack or spoofing (S-attack), and other categories of attack

involving tampering at the template level (U- and T-attacks). In order to elucidate the impact of all possible attacks, we (1) introduce the concepts of source of origin and symmetric biometric matchers, and (2) subsequently group the attacks into four categories. These views not only improve the understanding of the nature of different attacks but also turn out to ease the design of the classification problem. Following this analysis, we design a novel classification scheme that can take full advantage of the attack-specific data characteristics. Two realizations of the scheme, namely, a mixture of linear classifiers, and a Gaussian Copula-based Bayesian classifier, turn out to outperform a strong baseline classifier based on SVM, as supported by fingerprint spoofing experiments.

- Authors outside the consortium (yes [X] / no []) if yes explain their participation: This work is collaborated with colleagues with "University of Cagliari" in Italy.

"Handling Session Mismatch by Fusion-based Co-training: An Empirical Study using Face and Speech Multimodal Biometrics", N. Poh, J. Kittler, and A. Rattani, IEEE Symposium on Computational Intelligence in Biometrics and Identity Management, 2014

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7015447]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The work is directly relevant to WP3. In this study, we explore a novel semi-supervised training strategy known as fusion-based co-training that generalizes the classical co-training such that it can use a trainable fusion classifier. Our experiments on the BANCA face and speech database show that this proposed strategy is a viable approach. In addition, we also address the resolved issue of how to select the decision threshold for adaptation. In particular, we find that a strong classifier, including a multimodal system, may benefit better from a more relaxed threshold whereas a weak classifier may benefit better from a more stringent one.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation: This work is collaborated with a colleague with "Michigan State University" in US.

"Antiforensic-resistant Likelihood Ratio Computation: A Case Study Using Fingerprint Biometrics", N. Poh, N. Suki, A. Iorliam, the 22nd European Signal Processing Conf. (EUSIPCO) 2014

[http://www.eurasip.org/Proceedings/Eusipco/Eusipco2014/HTML/papers/1569925119.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

The work is directly relevant to WP3. we propose an anti-forensic resistant likelihood ratio computation that renders the strength of evidence to a level that is proportional to the trustworthiness of the trace, such that a highly credible evidence will bear its full strength of evidence whilst a highly suspicious trace can have its strength of evidence reduced to naught. Using simulation as well as a spoof fingerprint database, we show that the existing likelihood ratio computation is extremely vulnerable to an anti-forensic threat whereas our proposed computation is robust to it, thereby striking the balance between the utility and threat of a trace.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Do Biometric Images Follow the Bensford's Law?", A. Iorliam, A TS Ho, N. Poh and Y. Q. Shi, 2nd International Workshop on Biometrics and Forensics 2014

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6914261]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The work is directly relevant to WP3. We study one particular aspect of tampering: image manipulation. In the forensics literature, Benfords law has been reported to be very effective in detecting tampering of natural images. In this paper, our motivation is to examine whether biometric images will follow the Benfords law and whether or not they can be used to detect potential malicious tampering of biometric images. We find that, the biometric samples do indeed follow the Benfords law; and the method can detect tampering effectively, with Equal Error Rate (EER) of 0.55% for single compressed face images, 2.7% for single compressed fingerprint images, 4.3% for double compressed face images and 3.7% for double compressed fingerprint images.
- Authors outside the consortium (yes [X] / no []) if yes explain their participation: This work is collaborated with a colleague with "New Jersey Institute of Technology" in US.

2.1.4 EPFL

"Outsourced Pattern Matching", S. Faust, C. Hazay and D. Venturi, Proceedings of the 40th International Colloquium Automata, Languages, and Programming (ICALP), 2013.

[https://eprint.iacr.org/2014/662.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP5 "Evaluation of Privacy Preservation". The paper investigates the problem of securely outsourcing pattern matching

computations to a potentially untrusted server. While such an approach naturally has numerous advantages in cost and functionality, the outsourcing mechanism crucially needs to enforce privacy of the outsourced data and integrity of the computation. This paper provides an appropriate model for the problem at hand and presents a novel and provably secure scheme achieving the defined security notions.

- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was jointly performed with colleagues from Bar-Ilan Univeristy in Israel and Aarhus University in Denmark. The joint work in this paper actually considers a more general problem which is known as secure delegatable computation in cryptography. The potential application for privacy-preserving pattern matching, hence, for the scope of WP5 in the BEAT project, has been the motivation for this collaborative research and publication.

2.1.5 CHALMERS

"On the Leakage of Information in Biometric Authentication", E. Pagnin, C. Dimitrakakis, A. Abidin, A. Mitrokotsa. In Proceedings of Indocrypt 2014, New Delhi, India, December 2014.

[http://link.springer.com/chapter/10.1007%2F978-3-319-13039-2_16]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP5 "Evaluation of Privacy Preservation". The paper investigates the leakage of information of a biometric authentication protocol privacy-preserving or not when a matching template is at the disposal of the adversary.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE", A. Abidin, A. Mitrokotsa, In Proceedings of the IEEE Workshop on Information Forensics and Security 2014 (WIFS 2014), Atlanta, USA, December 2014. [http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7084304&tag=1]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP5 "Evaluation of Privacy Preservation". In this paper, we study the security of two recently proposed privacy-preserving biometric authentication protocols that employ packed somewhat homomorphic encryption schemes based on ideal lattices and ring-LWE, respectively. We

present a simple attack algorithm that enables a malicious computation server to learn the biometric templates in at most 2N-? queries, where N is the bit-length of a biometric template and ? the authentication threshold. The main enabler of the attack is that a malicious computation server can send an encryption of the inner product of the target biometric template with a bitstring of his own choice, instead of the securely computed Hamming distance between the fresh and stored biometric templates. We also discuss possible countermeasures to mitigate the attack using private information retrieval and signatures of correct computation.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Security of a Privacy-Preserving Biometric Authentication Protocol Revisited", A. Abidin, K. Matsuura, A. Mitrokotsa. In Proceedings of the 13th International Conference on Cryptology and Network Security (CANS 2014), Heraklion, Greece, October 2014. [http://link.springer.com/chapter/10.1007%2F978-3-319-12280-9_19]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This paper is directly relevant to WP5 "Evaluation of Privacy Preservation". In this paper, we present an attack algorithm that can be employed to mount a number of attacks on the protocol under investigation. We then propose an improved version of the Bringer et al. protocol that is secure in the malicious (or active) insider attack model and has forward security.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Attacks on Privacy-Preserving Biometric Authentication", A. Abidin, E. Pagnin, A. Mitrokotsa. In Proceedings of the 19th Nordic Conference on Secure IT Systems (NordSec 2014), Poster, Tromso, Norway, October 2014. [http://publications.lib.chalmers.se/publication/209989-attacks-on-privacy-preserving-biometric-authe

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP5 "Evaluation of Privacy Preservation". In this paper, we present an attack algorithm that can be employed to mount a number of attacks against multiple protocols for privacy preserving in biometric authentication.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

2.1.6 TUBITAK

"Biohashing with fingerprint spectral minutiae," Berkay Topcu, Cagatay Karabat, Hakan Erdogan, Berrin Yanikoglu, International Conference of the Biometrics Special Interest Group (BIOSIG) , vol., no., pp.1,12, 5-6 Sept. 2013.

[http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6617169]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.1 Privacy preservation techniques" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.2 Reference Privacy Preservation System. This paper offers new biohashing method for fingerprints by using spectral minutiae technique. Since biohashing has been selected as the reference privacy preservation system in the project, this paper directly contributes to D5.2.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  TUBITAK has contracts with academician from universities. Assoc. Prof. Dr. Hakan Erdogan and Assoc. Prof. Dr. Berrin Yanikoglu work for Sabanci University but they also worked as an advisor to TUBITAK in the area of biometrics, security and privacy preservation techniques. Dr. Cagatay Karabat and Berkay Topcu worked with Prof. Hakan Erdogan and Prof. Berrin Yanikoglu in this paper within this concept.

"Biohashing with Local Zernike Moments for face verification," Berkay Topcu, Cagatay Karabat, Hakan Erdogan, Signal Processing and Communications Applications Conference (SIU), 2014 22nd , vol., no., pp.1642,1645, 23-25 April 2014.

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6830561]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.1 Privacy preservation techniques" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.2 Reference Privacy Preservation System. This paper offer new biohashing method for face images by using local zernike moments. Since biohashing has been selected as the reference privacy preservation system in the project, this paper directly contributes to D5.2.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  TUBITAK signs contract with academician from universities. Assoc. Prof. Dr. Hakan Erdogan works for Sabanci University but he also worked as an advisor to TUBITAK in the area of biometrics. Dr. Cagatay Karabat and Berkay Topcu worked with Prof. Hakan Erdogan in this paper within this concept.

"How to assess privacy preservation capability of biohashing methods?: Privacy metrics," Cagatay Karabat, Berkay Topcu, Signal Processing and Communications Applications Conference (SIU), 2014 22nd , vol., no., pp.2217,2220, 23-25 April 2014.

[http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6830705]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is relavant to "Task 5.2 Metrics for privacy preservation" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.5 Description of metrics for the evaluation of privacy preservation and D5.6 Metrics for the evaluation of privacy preservation. This paper introduces new privacy metrics for biohashing methods (reference privacy preservation system). It also describes limitation of the metrics when evaluating privacy preservation.
- Authors outside the consortium (yes [] / no [X]) if yes explain their participation: N/A.

"Privacy Evaluation of Biohashing Methods", Cagatay Karabat, NIST International Biometric Performance Testing Conference, 2014.

[http://biometrics.nist.gov/cs_links/ibpc2014/presentations/10_tuesday_karabat_Biohash_Privacy_Evaluation_Cagatay_Karabat_v0.1.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is relavant to "Task 5.2 Metrics for privacy preservation" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.5 Description of metrics for the evaluation of privacy preservation and D5.6 Metrics for the evaluation of privacy preservation. This paper defines several protection goals e.g. diversification, unlinkability and privacy leakage. Then, it introduces new privacy metrics for biohashing methods (reference privacy preservation system). It includes simulation results for face and fingerprint images.
- Authors outside the consortium (yes [] / no [X]) if yes explain their participation: N/A.

2.1.7 CEA

"BEAT: Biometrics Evaluation and Testing", Alain Merle, International Conference on Common Criteria (ICCC), 2012.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This presentation is entirely related to development of evaluation methodology developped in WP6.
- Authors outside the consortium (yes [ ] / no [X])

"BEAT: a Methodology for Common Criteria evaluations of Biometrics systems", A. Merle , J. Bringer, J. Fierrez, N. Tekampe, International Conference on Common Criteria (ICCC), 2015.

[https://www.iccc15.org.uk/]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This presentation is entirely related to status (at the time of the presentation) of evaluation methodology developped in WP6.
- Authors outside the consortium (yes [ ] / no [X])

2.1.8 TUViT

"BEAT: a Methodology for Common Criteria evaluations of Biometrics systems", A. Merle , J. Bringer, J. Fierrez, N. Tekampe, International Conference on Common Criteria (ICCC), 2015.

[https://www.iccc15.org.uk/]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This presentation is entirely related to status (at the time of the presentation) of evaluation methodology developped in WP6.
- Authors outside the consortium (yes [ ] / no [X])

2.1.9 MORPHO

"Studying Leakages on an Embedded Biometric System Using Side Channel Analysis", Mael Berthier, Yves Bocktaels, Julien Bringer, Hervé Chabanne, Taoufik Chouta, Jean-Luc Danger, Mélanie Favre, and Tarik Graba, COSADE, 2014.

[http://dx.doi.org/10.1007/978-3-319-10175-0_19]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This article is directly relevant to WP4 "Evaluation of Vulnerabilities". It describes the study of indirect attacks on embedded biometric comparison based on a combination of side channel analysis and hill climbing attacks.
- Authors outside the consortium (yes [X] / no []) if yes explain their participation: The authors outside of the consortium collaborated with MORPHO during the French ANR BMOS project in order to develop an embedded implementation of fingerprint comparison and contributed to the research of side channel analysis of the related power consumption traces.

"Side channel analysis on an embedded hardware fingerprint biometric comparator & low cost countermeasures", Taoufik Chouta, Tarik Graba, Jean-Luc Danger, Julien Bringer, Mael Berthier, Yves Bocktaels, Mélanie Favre, Hervé Chabanne, HASP@ISCA, 2014.

[http://doi.acm.org/10.1145/2611765.2611771]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This article is directly relevant to WP4 "Evaluation of

Vulnerabilities". It describes the study of new indirect attacks on embedded biometric comparison based on a combination of side channel analysis and hill climbing attacks.

- Authors outside the consortium (yes [X] / no []) if yes explain their participation: The authors outside of the consortium collaborated with MORPHO during the French ANR BMOS project in order to develop an embedded implementation of fingerprint comparison and contributed to the research of side channel analysis of the related power consumption traces.

" Shuffling is not sufficient: Security analysis of cancelable iriscodes based on a secret permutation", Julien Bringer, Hervé Chabanne, and Constance Morel, IJCB, 2014.

[http://dx.doi.org/10.1109/BTAS.2014.6996280]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This work has been made during WP5 works on investigating privacy metrics and the robustness of some existing schemes. The paper describes an analysis of a cancelable iris-based scheme and gives recommandations for enhancing privacy.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

" Balancing is the Key - Performing Finger Vein Template Protection using Fuzzy Commitment", Mélanie Favre, Sylvaine Picard, Julien Bringer and Hervé Chabanne, ICISSP, 2015.

[http://dx.doi.org/10.5220/0005241403040311]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This work has been made during WP5 survey on reference privacy preserving system. The article describes the application, with the needed adaptation, of the well-known fuzzy commitment technique to fingervein protection. We started this study after realizing that it had never been made in the literature.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Security analysis of Bloom filter-based iris biometric template protection", Julien Bringer, Constance Morel and Christian Rathgeb, ICB, 2015.

[http://dx.doi.org/10.1109/ICB.2015.7139069]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This work has been made during WP5 works on privacy metrics for biometric privacy preserving system. The article describes the study of an existing scheme from ICB 2013, and introduces different strategies

to threaten the privacy properties of the scheme by exploiting the unperfect randomness of biometric data. This underlines the importance of taking in account the biometric properties when analysing a scheme and that privacy evaluation should also include different kind of experts. This is also related to the discussions in ISO SC37 on 30136 project on privacy testing.

- Authors outside the consortium (yes [X] / no []) if yes explain their participation: The author outside of the consortium collaborated with MORPHO as he is one of the co-author of the ICB 2013 scheme. This collaboration enabled us to consider a practical parameterizing of the scheme.

2.2 Accepted papers in journals

List of papers with a reference to BEAT.

2.2.1 IDIAP

"Biometrics Evaluation under Spoofing Attacks", I. Chingovska, A. Anjos and S. Marcel, IEEE Transactions on Information Forensics and Security, 2014.

[http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6879440]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper proposes a novel methodology and metrics for the evaluation of biometrics systems under spoofing attacks. The proposed metric is applied to the task of face anti-spoofing but it can be generalized to any biometric modalities. This metric is implemented with the BOB toolkit allowing seemless integration within the BEAT platform when required.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"BEAT biometrics evaluation and testing", S. Marcel, Biometric Technology Today, 2014.

[http://www.sciencedirect.com/science/article/pii/S0969476513700146]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to the whole project as it presents the main challenges and objectives of the BEAT project.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

2.2.2 UAM

"Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms", J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez and J. Ortega-Garcia, Computer Vision and Image Understanding, 2013

[http://dx.doi.org/10.1016/j.cviu.2013.06.003]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper studies vulnerabilities in iris recognition systems to various attacks conducted with synthetically generated data.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  Part of this work was conducted by Dr. Galbally in a research stay with Prof. Dr. Ross at West Virginia University (USA). Dr. Ross is a renowned expert in fingerprint and iris biometrics, and helped here with his experience in generating synthetic irises.

"The DooDB Graphical Password Database: Data Analysis and Benchmark Results", M. Martinez-Diaz, J. Fierrez and J. Galbally, IEEE Access, 2013

[http://dx.doi.org/10.1109/ACCESS.2013.2281773]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper describes a database and a related benchmark for evaluating the performance and security of biometric systems based on handwritten data.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

"A novel hand reconstruction approach and its application to vulnerability assessment", M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez and J. Ortega-Garcia, Information Sciences, 2014

[http://dx.doi.org/10.1016/j.ins.2013.06.015]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper describes a new method to synthetically generate hand data, and also applies that new method to various experimental scenarios to evaluate the vulnerability of state-of-the-art systems to attacks performed with such kind of synthetic data.

- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was done in collaboration with the IDeTIC lab at Universidad Las Palmas de Gran Canaria (Spain). Prof. Dr. M. A. Ferrer is a renowned expert in hand based biometrics, and helped here with his expertise on synthetic handshape generation.

"Efficient software attack to multimodal biometric systems and its application to face and iris fusion", M. Gomez-Barrero, J. Galbally and J. Fierrez, Pattern Recognition Letters, 2014

[http://dx.doi.org/10.1016/j.patrec.2013.04.029]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". The paper studies vulnerabilities of multimodal biometric systems to indirect attacks, and evaluates some countermeasures to such attacks like score quantization.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition", J. Galbally, S. Marcel and J. Fierrez, IEEE Trans. on Image Processing, 2014

[http://dx.doi.org/10.1109/TIP.2013.2292332]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". In addition to reviewing the state of the art in vulnerabilities against direct attacks, this paper proposes new anti-spoofing methods based on quality measures with application to iris, fingerprint, and face biometrics.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Mobile Signature Verification: Feature Robustness and Performance Comparison", M. Martinez-Diaz, J. Fierrez, R. P. Krish and J. Galbally, IET Biometrics, 2014

[http://dx.doi.org/10.1049/iet-bmt.2013.0081]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

This paper is directly relevant to WP3 "Evaluation of Biometric Performance". The paper analyses the effects of using handheld devices on the performance of automatic signature verification systems, comparing the discriminative power of global and local signature features between mobile devices and pen tablets.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Biometric Anti-spoofing Methods: A Survey in Face Recognition", J. Galbally, S. Marcel and J. Fierrez, IEEE Access, 2015

[http://dx.doi.org/10.1109/ACCESS.2014.2381273]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities". A survey of the state-of-the-art on anti-spoofing methods for face verification is presented in this paper.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"On-Line Signature Recognition Through the Combination of Real Dynamic Data and Synthetically Generated Static Data", J. Galbally, M. Diaz-Cabrera, M. A. Ferrer, M. Gomez-Barrero, A. Morales and J. Fierrez, Pattern Recognition, 2015

[http://dx.doi.org/10.1016/j.patcog.2015.03.019]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance" and WP4 "Evaluation of Vulnerabilities". This paper proposes the combination of real dynamic data and synthetic static data for signature verification, in order to improve the system's accuracy and robustness to skilled forgeries.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  This work was done in collaboration with the IDeTIC lab at Universidad Las Palmas de Gran Canaria (Spain). Prof. Dr. M. A. Ferrer is a renowned expert in signature and handwriting based biometrics, and helped here with his expertise on off-line signatures.

"Feature exploration for biometric recognition using millimetre wave body images", E. Gonzalez-Sosa, R. Vera-Rodriguez, J. Fierrez, M. Moreno-Moreno and J. Ortega-Garcia, EURASIP Journal on Image and Video Processing, 2015

[http://dx.doi.org/10.1186/s13640-015-0084-3]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". This paper proposes a new biometric recognition system based on the information of the silhouette of the human body.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Facial Soft Biometric Features for Forensic Face Recognition", P. Tome, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, Forensic Science International, 2015

[http://dx.doi.org/10.1016/j.forsciint.2015.09.002]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". This paper proposes a functional feature-based approach useful for real forensic caseworks, based on the shape, orientation and size of facial traits.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Synthesis of Large Scale Hand-Shape Databases for Biometric Applications", A. Morales, M. A. Ferrer, R. Cappelli, D. Maltoni, J. Fierrez and J. Ortega-Garcia, Pattern Recognition Letters, 2015

[http://dx.doi.org/10.1016/j.patrec.2015.09.011]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". This paper proposes and analyses a novel methodology for hand-shape image synthesis, with application to machine learning classification improvement based on synthetic training sets and scalability.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  Part of this work was conducted by Dr. Morales in a research stay with Prof. Dr. Maltoni at Universita di Bologna (Italy). Dr. Maltoni is a renowned expert in fingerprint and hand biometrics, and helped here with his experience in generating synthetic hand-shapes.

"Graphical Password-based User Authentication with Free-Form Doodles", M. Martinez-Diaz, J. Fierrez and J. Galbally, IEEE Trans. on Human-Machine Systems, 2016 (to appear)

[http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7362167]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 "Evaluation of Biometric Performance". This paper proposes and analyses the performance of free-form doodles pictured with the finger over smartphone screens for biometric authentication.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

2.2.3 UNIS

"Generalizing DET curves across application scenarios", Norman Poh and Chi Ho Chan, IEEE Transactions on Information Forensics and Security, 2015. [http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7109884]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3 and WP4. The paper proposes an algorithm that is capable of generalising a biometric performance curve in terms of Detection Error Trade-off (DET) or equivalently Receiver's Operating Characteristics (ROC), by allowing the user (system operator, policy-maker, biometric researcher) to explicitly set the proportion of data differently. This offers the possibility for the user to simulate different operating conditions that can better match the setting of a target application. We demonstrated the utility of the algorithm in three scenarios, namely, estimating the system performance under varying quality; spoof and zero-effort attacks; and cross-device matching. Based on the results of 1300 use-case experiments, we found that the quality of prediction on unseen (test) data, measured in terms of coverage, is typically between 60% and 80%, which is significantly better than random, that is, 50%.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"An Algorithm to Estimate the Biometric Performance Change Over Time", Norman Poh, Josef Kittler, Chi-Ho Chan, and Medha Pandit, IET Biometrics, 2015. [http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2014.0107]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3. The paper presents an algorithm that models the rate of change of biometric performance over time on a subject-dependent basis. It is called "homomorphic users grouping algorithm" or HUGA.

Although the model is based on very simplistic assumptions that are inherent in linear regression, it has been applied successfully to estimate the performance of talking face and speech identity verification modalities, as well as their fusion, over a period of more than 600 days. Our experiments carried out on the MOBIO database show that subjects exhibit very different performance trends. While the performance of some users degrades over time, which is consistent with the literature, we also found that for a similar proportion of users, their performance actually improves with use. The latter finding has never been reported in the literature. Hence, our findings suggest that the problem of biometric performance degradation may be not as serious as previously thought, and so far, the community has ignored the possibility of improved biometric performance over time. The findings also suggest that adaptive biometric systems, that is, systems that attempt to update biometricv templates, should be subject-dependent.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Full ranking as local descriptor for visual recognition: A comparison of distance metrics on S_n", Chi-Ho Chan, Fei Yan, Josef Kittler and Krystian Mikolajczyk, Pattern Recognition, 2015. [`http://www.sciencedirect.com/science/article/pii/S0031320314004002`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3. The paper proposes to use the full ranking of a set of pixels as a local descriptor. In contrast to existing methods which use only partial ranking information, the full ranking encodes the complete comparative information among the pixels, while retaining invariance to monotonic photometric transformations. The descriptor is used within the bag-of-visual-words paradigm for visual recognition. It can be a facial descriptor for face recognition.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Class-specific kernel fusion of multiple descriptors for face verification using multiscale binarized statistical image features", S Rahimzadeh-Arashloo and J Kittler, IEEE Trans Information Forensics and Security, 9(12):2100-2109, 2015. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6905848`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

This paper is directly relevant to WP3. This paper addresses face verification in unconstrained settings. For this purpose, first, a nonlinear binary class-specific kernel discriminant analysis classifier (CS-KDA) based on spectral regression kernel discriminant analysis is proposed. By virtue of the two-class formulation, the proposed CS-KDA approach offers a number of desirable properties such as specificity of the transformation for each subject, computational efficiency, simplicity of training, isolation of the enrolment of each client from others and increased speed in probe testing. Using the proposed CS-KDA approach, a regional discriminative face image representation based on a multiscale variant of the binarized statistical image features is proposed next. The proposed component-based representation when coupled with the dense pixel-wise alignments provided by a symmetric MRF matching model reduces the sensitivity to misalignments and pose variations, gauging the similarity more effectively. Finally, the discriminative representation is combined with two other effective image descriptors, namely the multiscale local binary patterns and the multiscale local phase quantization histograms via a kernel fusion approach to further enhance system accuracy. The experimental evaluation of the proposed methodology on challenging databases demonstrates its advantage over other methods.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Random cascaded regression copse for robust facial landmark detection", Z-H Feng, P Huber, J Kittler, W Christmas and X-J Wu, IEEE Signal Processing Letters, 22(1):76-80, 2015. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6877655`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3. This paper proposes a random cascaded-regression copse (R-CR-C) for robust facial landmark detection. Its key innovations include a new parallel cascade structure design, and an adaptive scheme for scale-invariant shape update and local feature extraction. Evaluation on two challenging benchmarks shows the superiority of the proposed algorithm to state-of-the-art methods..
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Cascaded collaborative regression for robust landmark detection trained using a mixture of synthetic and real images with dynamic weighting", Z-H Feng, G Hu, J Kittler, W Christmas and X-J Wu, IEEE Trans Image Processiong, 24(11):3425-3440, 2015. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7126999`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3. A large amount of training data is usually crucial for successful supervised learning. However, the task of providing training samples is often time-consuming, involving a considerable amount of tedious manual work. In addition, the amount of training data available is often limited. As an alternative, in this paper, we discuss how best to augment the available data for the application of automatic facial landmark detection. We propose the use of a 3D morphable face model to generate synthesized faces for a regression-based detector training. Benefiting from the large synthetic training data, the learned detector is shown to exhibit a better capability to detect the landmarks of a face with pose variations. Furthermore, the synthesized training data set provides accurate and consistent landmarks automatically as compared to the landmarks annotated manually, especially for occluded facial parts. The synthetic data and real data are from different domains; hence the detector trained using only synthesized faces does not generalize well to real faces. To deal with this problem, we propose a cascaded collaborative regression algorithm, which generates a cascaded shape updater that has the ability to overcome the difficulties caused by pose variations, as well as achieving better accuracy when applied to real faces. The training is based on a mix of synthetic and real image data with the mixing controlled by a dynamic mixture weighting schedule.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features", S Rahimzadeh Arashloo, J Kittler and W Christmas, IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp 2396-2407. 2015. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163625`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4. In this paper, an effective countermeasure against face spoofing attacks based on a kernel discriminant analysis approach is presented. Its success derives from different innovations. First, it is shown that the recently proposed multiscale dynamic texture descriptor based on binarized statistical image features on three orthogonal planes (MBSIF-TOP) is effective in detecting spoofing attacks, showing promising performance compared with existing alternatives. Next, by combining MBSIF-TOP with a blur-tolerant descriptor, namely, the dynamic multiscale local phase quantization (MLPQ-TOP) representation, the robustness of the spoofing attack detector

can be further improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a fast kernel discriminant analysis (KDA) technique. It avoids the costly eigen-analysis computations by solving the KDA problem via spectral regression.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Detection of Face Spoofing Using Visual Dynamics", S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N.k Suki, and A. T.S. Ho, IEEE Trans. on Information Forensics and Security, Special Issue on Biometric Spoofing and Countermeasures, 10(4), 762-777, 2015. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7047832`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4. This paper proposes a classification pipeline consisting of DMD, Local Binary Patterns(LBP), and Support Vector Machines (SVM) with a histogram intersection kernel. A unique property of DMD is its ability to conveniently represent the temporal information of the entire video as a single image with the same dimensions as those images contained in the video. The pipeline of DMD+LBP+SVM proves to be efficient, convenient to use, and effective. In fact only the spatial configuration for LBP needs to be tuned. The effectiveness of the methodology was demonstrated using three publicly available databases: print-attack, replay-attack, and CASIA-FASD, attaining comparable results with the state of the art, following the respective published experimental protocols.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"On the Use of Discriminative Cohort Score Normalization for Unconstrained Face Recognition", M. Tistarelli, Y. Sun, and N. Poh, IEEE Trans. on Information Forensics and Security, 2014. [`http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6918523`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP3. In this paper, a picture-specific cohort normalization approach, based on polynomial regression, is proposed to enhance the robustness of face matching under challenging conditions. A careful analysis is presented to better understand the actual discriminative power of a given cohort set. In particular, it is shown that the cohort polynomial regression alone conveys some discriminative information on the matching face pair, which is just marginally worse than the raw matching score. The influence of the cohort

set size in the matching accuracy is also investigated. Further, tests performed on the Face Recognition Grand Challenge ver 2 database and the labeled faces in the wild database allowed to determine the relation between the quality of the cohort samples and cohort normalization performance. Experimental results obtained from the LFW data set demon- strate the effectiveness of the proposed approach to improve the recognition accuracy in unconstrained face acquisition scenarios.

- Authors outside the consortium (yes [X] / no []) if yes explain their participation: This work is collaborated with colleagues from "University of Sassari" in Italy.

  n/a

2.2.4 TUBITAK

"THRIVE: Threshold Homomorphic Encryption Based Secure and Privacy Preserving Biometric Verification System," Cagatay Karabat, Mehmet Sabir Kiraz, Hakan Erdogan, Erkay Savas, EURASIP Journal on Advances in Signal Processing, vol. 2015:71, pp.1-18, 2015, doi: 10.1186/s13634-015-0255-5.

[http://www.asp.eurasipjournals.com/content/pdf/s13634-015-0255-5.pdf]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.1 Privacy preservation techniques" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.4 Advanced Privacy Preservation System. This paper develops new secure and privacy preserving biometric authentication system by using threshold homomorphic system. It analyzes security and privacy gaps of the reference privacy preservation systems and offer a new and advanced system. The paper directly contributed to the D5.4 Advanced Privacy Preservation System.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  TUBITAK has contracts with academician from universities. Assoc. Prof. Dr. Hakan Erdogan and Prof. Dr. Erkay Savas work for Sabanci University but they also worked as an advisor to TUBITAK in the area of biometrics, security and privacy preservation techniques. Dr. Cagatay Karabat and Berkay Topcu worked with Prof. Hakan Erdogan and Prof. Erkay Savas in this paper within this concept.

2.2.5 MORPHO

"Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends", J. Bringer, H. Chabanne and A. Patey, IEEE Signal Processing Magazine, 2013.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This paper directly corresponds to WP5 works on establishing the list of state-of-the-art advanced privacy-preserving schemes. This paper provides a survey on techniques based on secure multiparty computation and consequently this emphasizes our contributions to D5.3: Description of Advanced Privacy-Preservation Techniques.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

"Protection des données biométriques pour le respect de la vie privée", J. Bringer, H. Chabanne and A. Patey, Revue de l'Électricité et de l'Électronique, 2013.

[https://www.see.asso.fr/node/5210]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This paper is a French introduction of innovative techniques that can be used for protecting biometric data. Part of the article is dedicated to secure multiparty computation and thus related to previous paper and to D5.3: Description of Advanced Privacy-Preservation Techniques.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

2.2.6 KULEUVEN

"Why research may no longer be the same: about the territorial scope of the Proposed Data Protection Regulation", E. Kindt, International peer reviewed legal journal-Computer Law and Security Report, 2016.

- Correspondence of this paper with the BEAT research for D9.2 and 9.2 explaining some of the issues of the territorial scope of the new data protection regulation. It discusses the consequences of the choice to drop the physical criterion of "equipment". The use of platforms, such as the BEAT platform, could therefore in some cases no longer be covered by the EU data protection regulations.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Zin/onzin van biometrische toegangscontrole vanuit privacybescherming", E. Kindt, Private Veiligheid, 2014, Nr. 58–59, pp. 23–28.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  The author was invited to give her views on biometric access control in this specialized journal for police and law enforcement authorities. The results of BEAT on spoofing attacks contributed to a moderate approach.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

2.3 Accepted books or book chapters

List of papers with a reference to BEAT.

2.3.1 IDIAP

"Introduction", N. Erdogmus and S. Marcel, Handbook of Biometric Anti-Spoofing, 2014

[http://realtime.springer.com/doi/10.1007/978-1-4471-6524-8_1]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The chapter presents an general introduction to the problem of spoofing with real case examples.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Evaluation Methodologies", I. Chingovska, A. Anjos and S. Marcel, Handbook of Biometric Anti-Spoofing, 2014

[http://realtime.springer.com/doi/10.1007/978-1-4471-6524-8_10]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The chapter proposes a simplified version of the novel methodology and metrics for the evaluation of biometrics systems under spoofing attacks published as a journal paper (IEEE TIFS).
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

2.3.2 UAM

"Fingerprint Anti-spoofing in Biometric Systems", J. Galbally, J. Fierrez, J. Ortega-Garcia and R. Cappelli, Handbook of Biometric Anti-Spoofing, 2014

[http://link.springer.com/chapter/10.1007/978-1-4471-6524-8_3]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The chapter presents an overview of fingerprint anti-spoofing.
- Authors outside the consortium (yes [X] / no []) if yes explain their participation:

  Dr. R. Cappelli is a renowned expert in the field of fingerprint recognition, and helped with his expertise in compiling the state-of-the-art in this area.

2.3.3 UNIS

"An Analysis of Biometric Performance Change Over Time: A Multimodal Perspective", Norman Poh, Josef Kittler, Chi-Ho Chan and Medha Pandit, Age factors in Biometric Processing, 2014

[`http://www.theiet.org/resources/books/telecom/age_factors.cfm`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP3. The chapter presents an algorithm that models the rate of change of biometric performance over time on a subject-dependent basis. It is called "homomorphic users grouping algorithm" or HUGA. Although the model is based on very simplistic assumptions that are inherent in linear regression, it has been applied successfully to estimate the performance of talking face and speech identity verification modalities, as well as their fusion, over a period of more than 600 days. Our experiments carried out on the MOBIO database show that subjects exhibit very different performance trends. While the performance of some users degrades over time, which is consistent with the literature, we also found that for a similar proportion of users, their performance actually improves with use. The latter finding has never been reported in the literature. Hence, our findings suggest that the problem of biometric performance degradation may be not as serious as previously thought, and so far, the community has ignored the possibility of improved biometric performance over time. The findings also suggest that adaptive biometric systems, that is, systems that attempt to update biometric templates, should be subject-dependent.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"State-of-the-Art LBP Descriptor for Face Recognition", Chi ho Chan, Josef Kittler and Norman Poh, Local Binary Patterns: New Variants and Applications, 2014

[`http://realtime.springer.com/doi/10.1007/978-1-4471-6524-8_10`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP3. The chapter offers some insights into the merits of various face representation and classifier methods, as well as their role in dealing with the challenges of face biometric.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Illumination Invariant Face Recognition: A Survey", Chi Ho Chan, Xuan Zou, Norman Poh, and Josef Kittler, Face Recognition in Adverse Conditions, 2014

[http://www.igi-global.com/chapter/illumination-invariant-face-recognition/106980]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP3. Illumination variation is one of the well-known problems in face recognition, especially in uncontrolled environments. This chapter presents an extensive and up-to-date survey of the existing techniques to address this problem. This survey covers the conventional passive techniques that attempt to solve the illumination problem by studying the visible light images, in which face appearance has been altered by varying illumination, as well as the active techniques that aim to obtain images of face modalities invariant to environmental illumination. .
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

"Fusion of Face Recognition Classifiers under Adverse Conditions", Norman Poh, Chi Ho Chan, and Josef Kittler, Face Recognition in Adverse Conditions, 2014

[http://www.igi-global.com/chapter/fusion-of-face-recognition-classifiers-under-a106983]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This book chapter is directly relevant to WP3. A face acquired by recognition systems is invariably subject to environmental and sensing conditions, which may change over time. This may have a significant negative impact on the accuracy of recognition algorithms. In the past, these problems have been tackled by building in invariance to the various changes, by adaptation, and by multiple expert systems. More recently, the possibility of enhancing the pattern classification system robustness by using auxiliary information has been explored. In

particular, by measuring the extent of degradation, the resulting sensory data quality information can be used to combat the effect of the degradation phenomena. This can be achieved by using the auxiliary quality information as features in the fusion stage of a multiple classifier system, which uses the discriminant function values from the first stage as inputs. Data quality can be measured directly from the sensory data. Different architectures are suggested in this chapter for decision making using quality information. Examples of these architectures are presented and their relative merits discussed. The problems and benefits associated with the use of auxiliary information in sensory data analysis are illustrated on the problem of personal identity verification used in biometrics.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

  n/a

2.3.4 MORPHO

"Secure Two-Party Computation and Biometric Identification", Julien Bringer, Hervé Chabanne, Alain Patey, book chapter of Biometric Security, David Chek Ling Ngo, Andrew Beng Jin Teoh and Jiankun Hu (eds), Cambridge Scholars Publishing, 2015

[`http://www.cambridgescholars.com/biometric-security`]

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This submission is a synthesis of the progresses that have been made, included by Morpho during the course of BEAT project, on secure computation for biometric recognition. This is fully related to WP5, more specifically D5.4: Advanced Privacy Preservation System.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation: n/a

2.3.5 KULEUVEN

"Wat brengt de nieuwe Verordening Algemene Gegevensbescherming ? Een eerste kritische analyse", E.Kindt, in Recht in Beweging, 2016, VRG (ed.), Antwerpen - Apeldoorn, Maklu, 2016, pp. 489-506.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  In this book chapter, the author discusses the new major new developments in General data protection for the Belgian legal counsels and attorneys. This research was made possible by the BEAT project and links to the research done in WP9 for the deliverables 9.1, 9.2. and 9.3.

- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

"Legal Aspects: Biometric data, Evidence Rules and Trusted Identities", E. Kindt, Chapter 12 from the "Handbook of Biometric Anti-Spoofing", 2014, pp 217–231.

[http://link.springer.com/chapter/10.1007%2F978-1-4471-6524-8_12]

- Correspondence of this book chapter with the BEAT research relating to spoofing attacks. The author connected these findings with the legal rules on evidence and trusted identities under the EU regulations on digital signatures.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

2.4 Completed events: talks, presentations, competitions or standards

2.4.1 IDIAP

"License agreement signed between Idiap & ECs Joint Research Center to experiment BEAT platform", IDIAP, 2016

[http://www.biometrics-center.ch/news/idiap-eu-signed-agreement]

IDIAP and JRC signed a licence agreement for JRC to test and possibly deploy the BEAT platform on JRC datasets.

"ISO/IEC JTC1 SC37 Biometrics", IDIAP, 2016

[https://www.biometrics-center.ch/jtc1-sc37-martigny2015]

The Idiap Research Institute and the Swiss Center for Biometrics Research and Testing, co-founded by Idiap, the canton of Valais and the city of Martigny, will welcome - for the first time - , from January 11-19, the international delegations of ISO standards in the field of biometrics.

"Speaker Anti-spoofing Competition", "P. Korshunov and S. Marcel", (ongoing)

[http://www.biometrics-center.ch/testing/btas-2016-speaker-anti-spoofing]

Despite the growing usage and increasing reliability of the speaker verification systems, they are shown to be vulnerable to spoofing attacks. In a spoofing attack, an invalid user attempts to gain access to the system by presenting counterfeit (fake) speech sample(s) as the evidence of a valid user. Counterfeit speech can be synthesized from text, converted using speech of another person, or simply replayed using some playback device such as a mobile phone.

The participants in this anti-spoofing competition will propose countermeasures to protect an automatic speaker verification (ASV) system against spoofing attacks. Essentially, these countermeasures should effectively separate real (genuine) speech

recordings from spoofed speech (attacks). AVspoof database will be used in the competition. The participants will be provided two non-overlapping sets (each containing real and spoofed data subsets) for training and calibration of their countermeasure techniques. The submitted techniques will be evaluated on a separate independent independent testing set, which, besides the attacks present in AVspoof database, will also include additional unknown attacks.

"1st Competition on Counter Measures to Finger Vein Spoofing Attacks", "P. Tome and S. Marcel", 2015

[http://www.biometrics-center.ch/testing/icb-2015-fingervein-anti-spoofing]

Despite the reliability and the wide usage of the finger vein recognition systems in many environments where security is vital, they are still vulnerable to direct sensory attacks i.e. spoofing attacks. In a spoofing attack, an invalid user may gain access to the system by presenting counterfeit biometric evidence of a valid user. The finger vein recognition is an growing technology where the advanced spoofing attacks are emerging. Unfortunately, the number of databases and anti-spoofing systems are still limited or unknown. Furthermore, the number of baseline anti-spoofing systems whose source code is publicly available for comparison and reproducible research, is even more limited. The objective of this competition is to challenge the proposed anti-spoofing algorithms on spoofing attacks.

"Spoofing challenge", "S. Marcel", 2013

[https://www.tabularasa-euproject.org/evaluations/tabula-rasa-spoofing-challenge-

In 2013, the BEAT and TABULA RASA EU projects jointly organized a Spoofing Challenge and invited researchers to develop ingenious attack plans and to deceive various biometric authentications systems of different modalities. With large participation of researchers, visitors and contestants, the challenge has successfully raised awareness about spoofing vulnerabilities of biometric systems and additionally, it has given way to many different and creative ways to attack the systems. One of the most notable novel form of attack proposed by the invited researchers was the use of make-up in face recognition to deceive the anti-spoofing measures.

"Competition on face recognition in mobile environment using the MOBIO database", "M. Güenther"

[http://www.biometrics-center.ch/testing/icb-2013-face-recognition-mobio]

In the context of BEAT project, the Biometric group at the Idiap Research Institute organized the second competition on face recognition for the 2013 International Conference on Biometrics (ICB-2013). Researchers in biometrics were invited to participate in this competition. This will help them to evaluate the progress made in the last couple of years.

From this competition, it was measured that the best performing simple system does not rely on hand-designed features, but learns the extracted features with a convolutional neural network. The fusion systems perform comparably as well on

the development set, but these good results cannot generalize to the evaluation set. Unfortunately, the reproducibility of the results was limited since only one participant provided source code.

"Competition on speaker recognition in mobile environment using the MOBIO database", "E. Khoury"

[http://www.biometrics-center.ch/testing/icb-2013-speaker-recognition-mobio]

In the context of BEAT project, the Biometric group at the Idiap Research Institute organized the second competition on text independent speaker recognition for the 2013 International Conference on Biometrics (ICB-2013). Researchers in Biometrics were invited to participate to this competition. This will help them to evaluate the progress made in the last couple of years.

This evaluation produced several interesting findings. First, the use of total variability modeling followed by a score fusion provided the best performances. Second, the use of external but suitable data to train the background models as well as gender-dependent features can be helpful.

"Reproducible Biometrics Evaluation and Testing with the BEAT platform", "S. Marcel"

[http://www.nist.gov/itl/iad/ig/ibpc2014.cfm]

We presented the BEAT platform to the NIST International Biometric Performance Testing Conference in 2014. The BEAT platform was perceived as a potential tool for future evaluation by NIST and we are looking into continuing to promote the BEAT platform at NIST and in the US.

"Spoofing, the BEAT project and its legacy", "S. Marcel"

[http://www.bva.bund.de/EN/Tasks/Visa_Information_System/VIS_User_Conference_2014.html]

We were invited to present at the FRONTEX VIS User Conference the work from BEAT in spoofing, on the BEAT platform and on the Swiss Center for Biometrics Research and Testing that is aimed to sustain the BEAT platform after the end of the BEAT project. Most notably the BEAT platform raised again some attention in particular from EC representatives and border guards as a tool to maintain research biometric databases and to perform independent evaluations.

"Spoofing and Anti-Spoofing in Biometrics", "S. Marcel"

We were invited to present our work on spoofing and anti-spoofing at the FRONTEX Research Workshop on Vulnerabilities and Countermeasures in First Line Border Checks. Interestingly, the work on spoofing has attracted some attention. Indeed, some of the police representative were simply not aware of spoofing as a risk and asked for more details.

"The BEAT project", "S. Marcel", EAB RESEARCH PROJECTS CONFERENCE (EAB-RPC) 2014

[http://eab.org/events/program/69]

We presented the BEAT project and the BEAT platform at the first Research Project conference, a jointly organized event between the major EU projects in biometrics to present research results and to discuss the benefit of this research for our European society. Once again the BEAT platform attracted much attention in particular in the Forensic community where the platform could solve a major problem in biometric database distribution.

2.4.2 UAM

"KBOC: Keytroke Biometrics Ongoing Competition", UAM, 2016.

[https://sites.google.com/site/btas16kboc/]

KBOC is an official competition of the IEEE Eighth Intl. Conf. on Biometrics: Theory, Applications, and Systems (BTAS 2016) organized by UAM. The competition includes a public benchmark involving 3600 keystroke sequences from 300 users simulating a realistic scenario in which each user types his own sequence (given name and family name) and 3600 impostor attacks (users who try to spoof the identity of others). Two modes of participation have been organized: 1) *Ongoing*, exploiting the full potential of the BEAT Platform; and 2) *Offline*, in which participants will receive blind data to recognize using their own computing infrastructure. By late January 2016, ten participants have been already registered to the competition.

"From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems", "J. Galbally"

[https://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Galbally]

We presented BEAT research activities on analyzing new vulnerabilities of iris recognition systems, related to WP4. Big interest from media like BBC or CNN was attracted.

"Evaluation of Biometric Performance", "J. Fierrez"

[http://www.eab.org/events/program/69]

We presented the BEAT project activities around WP3 (Evaluation of Biometric Performance) at the first Research Project conference, a jointly organized event between the major EU projects in biometrics to present research results and to discuss the benefit of this research for our European society.

"Indirect Attacks on Biometric systems", "J. Fierrez"

[http://eab.org/events/program/81]

We were invited to present our work on indirect attacks to biometric systems at the Norwegian Biometrics Laboratory Annual Workshop 2015, at Gjovik University College. The work, directly related to WP4, attracted attention among the attendees, which included post-graduate students and researchers.

"The BEAT project", "J. Fierrez"

[http://www.eab.org/events/program/79]

We presented the BEAT project and the BEAT platform at the second Research Project conference, a jointly organized event between the major EU projects in biometrics to present research results and to discuss the benefit of this research for our European society. Once again the BEAT platform attracted much attention.

2.4.3 UNIS

"Training workshop for IEEE Certified Biometrics Professional (IEEE CBP)", "N. Poh", 2013

[http://www.ieee.org/education_careers/education/continuing_education/certified_biometrics_program.html]

In 2012, the IEEE CBP program, held in in Kuala Lumpur, Malaysia, was developed to help meet the training, hiring, and evaluation needs of professionals and organizations throughout the biometrics industry.

"Biometric Evaluation and Testing Using the BEAT Platform", "N. Poh"

[http://www.biometricschool.org/]

We presented the BEAT project and the BEAT platform at the second of Biometric School (Winter Edition). In the tutorial, we intorduce BEAT platform to the targeted participants with diverse background. The participants include engineers graduate and post-graduate students, academicians, entrepreneurs, project managers, and government officers who need to understand the strengths and limitations of biometrics, as well as new-comers to the field.

"Biometric Menagerie", "N. Poh"

[https://www.youtube.com/watch?v=YDLXHfxEcEs]

This talk is presented in Biometrics Working Group Meeting Number 64 held in 2014. It is directly relevant to WP3.

"System Design and Performance Assessment: A Biometric Menagerie Perspective", "N. Poh"

[http://youtu.be/-UpKBAaKP0U,http://youtu.be/3HrbpERLZLo]

This talk is a tutorial in International Joint Conference on Biometrics held in 2014. It is directly relevant to WP3.

2.4.4 CHALMERS

"Authentication in Constrained Settings", "A. Mitrokotsa"

[http://www.cosic.esat.kuleuven.be/crossfyre/workshop_program.shtml]

CrossFyre is an international workshop on cryptography, robustness, and provably secure Schemes for female young researchers that took place at KU Leuven in June 2013. We presented the BEAT project and the challenges of privacy-preserving biometric authentication. We have received a lot of interest from the audience and interesting questions.

"Authentication in Constrained Settings", "A. Mitrokotsa"

[http://www.seg.inf.uc3m.es/seminars.html]

We have given an seminar at the University Carlos III Madrid and the computer security lab. The seminar was attended by master, doctoral students as well as senior researchers and professors. We have presented the challenges in achieving accurate authentication when the credentials used are noisy while we need to provide privacy guarantees. The BEAT project was also presented. We have received interesting questions and a discussion was initiates on topics related to privacy-preserving biometric authentication.

"Privacy Preserving Biometrics", "A. Mitrokotsa"

[http://www.eab.org/events/program/25?ts=1420416000063]

In the European Biometrics Symposium that took place in Brussels, at CENCENELEC Meeting Center, on the 15 February 2013, A. Mitrokotsa has presented a tutorial on privacy-preserving biometric authentication systems; the main challenges in this domain and the limitations of existing mechanisms. The presentation was received very enthusiastically the audience and an interesting discussion was initiated.

2.4.5 TUBITAK

"In2Societies 2012 Brokerage Event", "Cagatay Karabat, Oktay Adalier"

[https://www.beat-eu.org/news/fp7-beat-project-present-at-in2societies-2012-even
[http://in2s.meeting-mojo.com]

The In2Societies 2012 Brokerage event has been organized at 5 October 2012 in Brussels/Belgium. The event brought together 300 researchers and organizations involved in Security research, Socio-economic Sciences & Humanities (SSH) and Information & Communication Technologies (ICT), with the desire and capability to help overcome a wide range of challenges. During In2Societies 2012, we had the opportunity to present the challenges and the progress of the FP7 BEAT Project to Security and ICT professionals..

"Biometrics and e-ID in EU-funded Projects", "Cagatay Karabat"

[http://cs.sabanciuniv.edu/en/news_detail/52388]

Dr. Cagatay Karabat has made a presentation at Sabanci University on security and privacy aspects of biometric and FP7 BEAT project at 30 October 2013 in Istanbul/Turkey. The audiences were professors and master and PhD students in Sabanci

University. There was a very fruitful brainstorming discussion after the presentation on recent developments in the area of privacy preserving biometric systems with participants.

"Evaluation of Privacy Preservation", "Berkay Topcu"

[http://eab.org/events/program/69]

The EAB (European Association for Biometrics) and the EU-projects FIDELITY, FastPass, BEAT, Future-ID, INGRESS, are jointly organizing a Research Project Conference (EAB-RPC), to present research results and in order to discuss the benefit of this research for our European society. Moreover experts from the biometric community will discuss on a panel Ethical and Privacy Issues of Biometrics and Identity Management. Berkay Topcu from TUBITAK made a presentation on evaluation of privacy preservation for biometrics at EAB Research Projects Conference 2014 in Darmstadt/Germany on 8-9 September 2014. This presentation was directly related to the outputs of "WP5 - Evaluation of Privacy Preservation". The feedback received from the participants was that the outputs of WP5 are very good and the project may get benefit from close collaboration on privacy metrics and privacy preservation systems with standardization bodies.

"Euro ID and ID World International Congress 2014", "Cagatay Karabat"

[https://www.messefrankfurt.com/frankfurt/en/besucher/welcome/messeveranstaltungemessen/technology-production/euro-id-engl-2014.html]

The Euro ID exhibition and the ID World International Congress are two leading events in the field of ID-Technologies. Biometrics as one of the key building block for identity technogies was taken an important place in this event. Euro ID and ID World International Congress 2014 was held on the 18-20 November 2014 in Frankfurt/Germany. Cagatay Karabat from TUBITAK attended the event to discuss the outputs of "WP5 - Evaluation of Privacy Preservation" with the expert group and he made a presenation (named "Role of Biometrics in e-Government Application: Security and Privacy Aspects") on FP7 BEAT project outputs. The participants were experts in the area of biometrics and identity applications in the area of e-government applications. This presentation was directly related to the outputs of "WP5 - Evaluation of Privacy Preservation" and it is a dissemination activity under "WP8 - Dissemination and Exploitation". The feedback was very useful for further developments especially on usage of biometrics in the e-government application.

"Brokerage Event on Security and Privacy Aspects of Biometrics", "Cagatay Karabat"

TUBITAK has organized joint brainstorming meetings on "security and privacy preservation techniques for biometrics" with s own different research groups and other researchers outside the BEAT consortium in Brussels/Belgium on 8-11 June 2015. Cagatay Karabat from TUBITAK has made presentation on the BEAT project outputs. This presentation was directly related to the outputs of "WP5 - Evaluation

of Privacy Preservation" and it is a dissemination activity under "WP8 - Dissemination and Exploitation". As an outcome, a new paper has been submitted within the scope of the scope of advanced privacy preservation. The outcomes of these meetings have been used for further work beyond D5.4 Advanced Privacy Preservation system.

"Biometrics Vulnerability Assessment Expert Group Workshop and Biometrics & Identity 2015 Conference", "Cagatay Karabat"

[http://www.biometricsandidentity.com] [http://www.biometricsandidentity.com/resources/updateable/pdf/BIOM2015_advance_programme.pdf] [http://www.biometricsinstitute.org/events.php/561/bvaeg-biometrics-vulnerability-workshop]

Biometrics Vulnerability Assessment Expert Group (BVAEG) Workshop was held on the 12 October 2015, just the day before the Biometrics & Identity 2015 Conference (13-15 October 2015) in London/UK. This event focused on practical application of vulnerability detection. Cagatay Karabat from TUBITAK attended the event to discuss the outputs of "WP5 - Evaluation of Privacy Preservation" with the expert group. Biometrics & Identity 2015 Conference was a three days of great practical advice, tips and solutions for using biometric technology for managing identity and increasing efficiency within government and commercial applications. In a packed conference programme, speakers involved in large-scale projects will mix with those from mainstream customer-facing applications such as mobiles and payments to give a comprehensive insight into current projects and future challenges and how biometrics will fit into your plans for the future. Cagatay Karabat from TUBITAK attended the conference and make a presentation (named "Security and Privacy Preservation Solutions of FP7 BEAT Project") on FP7 BEAT project outputs in the session named "How to balance security, and data protection while creating a more seamless customer journey". This presentation was directly related to the outputs of "WP5 - Evaluation of Privacy Preservation" and it is a dissemination activity under "WP8 - Dissemination and Exploitation". The feedback received from the participants was that the outputs of WP5 are very good and the project may get benefit from close collaboration on security and privacy preservation systems with biometric market players.

"Security and Privacy Preservation Approach of BEAT", "Cagatay Karabat"

TUBITAK has organized joint brainstorming meetings on "privacy preservation techniques for biometrics" with its own different research groups and other researchers outside the BEAT consortium in Brussels/Belgium on 2-6 November 2015. Cagatay Karabat from TUBITAK has made presentation on the BEAT project outputs. This presentation was directly related to the outputs of "WP5 - Evaluation of Privacy Preservation" and it is a dissemination activity under "WP8 - Dissemination and Exploitation".As an outcome, a new paper has been submitted within the scope of security and privacy preservation metrics for biometrics. The outcomes of these meetings have been used for further work beyond D5.6 Metrics for the evaluation of privacy preservation.

"Cyber Security & Privacy Innovation Forum", "Cagatay Karabat"

[http://www.cspforum.eu/2015] [https://www.cspforum.eu/2015/other-exhibitors/beat]

Cyber Security & Privacy Innovation Forum 2015 was organized by DG CONNECT (Unit H4 Trust & Security) and CSP Forum on 28-29 April 2015 in Brussels, Belgium. This event was an opportunity for all projects funded under European Commission, DG CNECT (Unit H4 Trust & Security), to showcase their projects activities and outputs to the wider community. A dedicated exhibition space for the FP7 BEAT project (poster board, table, 2 chairs, power supply) has been reserved. TUBITAK has designed and published a big poster and a number of leaflets as well for the BEAT project. Cagatay Karabat from TUBITAK attended the event and disseminated the results of the BEAT project in the event. This was an activity under "WP8 - Dissemination and Exploitation". The feedback was on cybersecurity aspects on biometrics applications and they are useful for further developments.

"ISO/IEC JTC1/SC37 Biometrics Meetings and European Biometrics Symposium", "Cagatay Karabat"

[http://www.biometrics-center.ch/jtc1-sc37-martigny2015] [http://www.eab.org/events/program/108]

ISO/IEC JTC1/SC37 Biometrics was organized in Martigny/Switzerland on 11-19 January 2016. Cagatay Karabat from TUBITAK has attened preliminary meetings of the working groups in order to disseminate results of the BEAT project and discuss with international expert for further steps in order to ensure sustainability. uropean Association for Biometrics (EAB) in cooperation with Idiap has organized a workshop on Research and Standards on Biometric presentation Attacks in Martigny/Switzerland on19 January 2016. Leading experts made presentations about current status in R&D on the detection and prevention of presentation attacks for various biometric modalities. Cagatay Karabat from TUBITAK attended the event made a presentation on Security and Privacy Aspects of Biometrics in order to disseminate results of the BEAT project. This was an activity under "WP8 - Dissemination and Exploitation" in order to present the work in "WP5 - Evaluation of Privacy Preservation". The feedback was quite positive and they are useful for further developments for improving biometrics systems by using emerging crypto tools.

2.4.6 CEA

Common Criteria evaluation of biometric systems, EAB presentation, A. MERLE, 2013.

This event was organised by the European Association for Biometrics (EAB)for its members. BEAT was presented and a specific focus was done on the interest for

having a Common Criteria evaluation methodology developed and applied to biometrics systems. Interest was expressed and some participants have been following the BEAT project later.

Standards & Certifications: Common Criteria evaluations, EAB RESEARCH PROJECTS CONFERENCE (EAB-RPC), A. MERLE, 2014

[http://eab.org/events/program/69]

A specific presentation of the evaluation methodology (WP6) was made at the first Research Project conference, a jointly organized event between the major EU projects in biometrics to present research results and to discuss the benefit of this research for our European society. Major interest was expressed by the participants.

"BEAT Project, Biometrics for High-Value Services (July 1st, Paris), Opportunities, Obstacles and Breakthroughs, Common meeting: Natural Security, Biometrics Institute, Mobey forum, A. Merle, 2015

BEAT was invited to present the evaluation methodology to this event coorganised by the Natural Security Alliance, the Biometrics Institute and the MOBEY Forum and focusing on the use on biometrics for banking applications. The interest was high and bilateral contacts have been initiated after this event ("Groupement des Cartes Bancaires", the French authority manging the security of the payment systems).

2.4.7 TUViT

Presentation of the project status on BioSig conference, C. Noetzel, September, 8th, 2014

The current status of the project has been presented at BioSig conference in Darmstadt, Germany. Focus has been laid on the evaluation of vulnerabilities.

Nils Tekampe, Presentation Attack Detection: Towards a structured approach for tailored metrics, 2014

This overview of the work performed in the area of metrics for Presentation Attack Detection has been published on the B.E.A.T. website and also submitted into ISO/IEC SC 37 for consideration in the standardization activities around ISO/IEC 30107.

[https://www.beat-eu.org/publications/index.php/attachments/single/41]

2.4.8 MORPHO

"IT Security Standards ISO/IEC SC27", "L. Merrien"

We had been invited to present an overview of ISO SC27 standards and on-going works related to biometrics at a session on Standards, at Biometrics 2012, London. This was particularly an opportunity to present the link between those SC27 projects and BEAT activities. The general feedback of the attendees was an interest for the project and for being further informed of the future achievements of BEAT and related standards.

"BEAT: a Methodology for Common Criteria evaluations of Biometrics systems", "J. Bringer" BEAT results on CC evaluation of biometric systems and expected planning for next months have been presented during the ISO SC27 meeting in October, 2015, in Jaipur (India) to the WG3 (security evaluation working group) participants. Overall interest for this topic has been expressed by the attendees and several questions highlighted the need for further discussions. During this meeting, a study period on performance evaluation has been also suggested based on BEAT contributions.

"Better know your limits and adversaries: A practical view on various template protection and key binding schemes", "J. Bringer" [http://www.cs.haifa.ac.il/~orrd/PrivDay/] Various BEAT results on privacy and security analysis made during WP5, together with lessons learned, were presented during this workshop, called Privacy Enhancing Technologies for Biometric Data, in January 2016. Several attendees were very interested to continue the discussion after the presentation to learn more about the current trends on privacy of biometric template protection schemes.

2.4.9 KULEUVEN

"De nieuwe Verordening gegevensbeschermingsrecht: wat (ge)biedt de toekomst", "E. Kindt", at Actualia in de sectoren van de intellectuele rechten, informatietechnologie en het mediarecht-Actualits dans les secteurs des droits intellectuels, la technologie de linformation et le droit des medias, 20 November 2015, Leuven, Belgium.

KU Leuven organized this academic conference in Leuven about new information technologies and intellectual property. The speaker presented its findings on the study of the new General Data Protection Regulation (GDPR) as researched in the BEAT project as well. The audience was the Belgian legal community.

"Privacy and Data Protection Law: An Introduction", "E. Kindt", Training School, Cost Action IC1206, De-identification for privacy protection in multimedia content.

This presentation explained about the new GDPR to researchers of the biometric community and the consequences. This was made in part possible by the BEAT research, which also discusses biometric data and research under the new GDPR.

Invited panelist " New perspective on Privacy and Biometrics with the New EU Regulation", "E. Kindt", at the European Association for Biometrics Research Projects Conference (EAB-RPC), Darmstadt, Fraunhofer IGD, 7-8 September 2015.

[http://eab.org/events/program/79]

This presentation explained about the new GDPR to researchers of the biometric community and the consequences. This was made in part possible by the BEAT research, which also discusses biometric data and research under the new GDPR.

"Use of biometric data for forensics: great promises, great legal pitfalls", "E. Kindt", International Workshop on Biometrics and Forensics (IWBF),3-4 March2015, Gjovik, Norway.

[https://sites.google.com/site/iwbf2015/]

The BEAT participant was invited to give this talk in order to share BEAT results on legal aspects with the research community studying biometric research in forensics.

"Expert committee on biometrics", "E. Kindt", Invited expert by Rathenau, 2 December 2014, Utrecht, the Netherlands.

[https://www.rathenau.nl/nl/publicatie/dicht-op-de-huid]

This independent research institution in the Netherlands invited the researcher for giving her views for a publication being prepared by Rathenau. Various other experts from police, government, invited as well. The use of the BEAT platform also in areas where no direct access to the data is desired, was discussed as well. The interview and expert meeting resulted in a publication: "Janssen, A., Kool, L. and Timmer, J., Dicht op de huiu". "Gezichts- en emotieherkenning n Nederland", Rathenau Instituut, 2015.

Panel "Ethical and Privacy issues of Biometrics and Identity Management", "E. Kindt", Invited Chair at the European Association for Biometrics Research Projects Conference (EAB-RPC), Darmstadt, Fraunhofer IGD, 8-9 September 2014.

[http://www.eab.org/events/program/69]

This panel at the international conference at which BEAT was presented as a project as well, lead to a panel at the end of the day in which privacy aspects of biometric data processing in various projects, including BEAT, were discussed with the public and among experts. The BEAT participant was invited to compose the panel and lead the discussions.

Invited panelist "Automated Border Control (ABC) and Smart Borders", "E. Kindt" Identities at the borders, Biometrics Institute, Brussels , 29 April 2014.

[http://www.biometricsinstitute.org/events.php/444/2nd-identities-at-the-borders-

This panel convened experts at this international conference focusing on the use of biometrics for safe border crossing.

Invited expert CPDP panel "Privacy practices in Biometric Applications", "E. Kindt", CPDP, Reforming Data Protection: the Global Perspective, Januari, Brussels, 2014.

[http://www.cpdpconferences.org/Resources/CPDP2014_Programme.pdf]

This panel at the well known international privacy conference in Brussels was dedicated to biometric data and the participant was invited based on previous work and publications also resulting from BEAT (see above).

2.5 Submitted papers in conferences

2.5.1 UAM

"Fixed-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics", M. Gomez-Barrero, J. Galbally, E. Maiorana, P. Campisi and J. Fierrez, Int. Conf. on Biometrics, 2016.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper presents a new method to protect fixed-length templates that enables privacy preservation.
- Authors outside the consortium (yes [x] / no [ ]) if yes explain their participation:

  This work was mainly conducted by M. Gomez-Berrero, a PhD student at UAM, during a research stay with Prof. Dr. P. Campisi at Universita Roma Tre (Italy). Prof. Campisi is a renowned expert in biometric security, which helped with his expertise using cutting edge methods (in this case Homomorphic Encryption).

2.5.2 TUBITAK

"Measurable Security and Privacy for Biometrics" Cagatay Karabat submitted to the 28th International Biometric Conference 2016.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.2 Metrics for privacy preservation" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.6 Metrics for the evaluation of privacy preservation. This paper analyses unpredictability, which is one of the most important features of privacy preservation. This is a further work upon the D5.6 Metrics for the evaluation of privacy preservation.
- Authors outside the consortium (yes [] / no [X]) if yes explain their participation: N/A.

"Unpredictability Assessment of Biometric Hashing Under Naive and Advanced Threat Conditions", Berkay Topcu, Cagatay Karabat, Hakan Erdogan submitted to he 2016 European Signal Processing Conference (EUSIPCO 2016).

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.1 Privacy preservation techniques" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.4 Advanced Privacy Preservation System. This paper makes further research on information leakage for biometric hashing systems (which are reference privacy preservation system in the BEAT project) under different threat conditions. Thus, security and privacy preservation limits of these methods are worked. This is a further work upon the D5.4 Advanced Privacy Preservation System.

- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  TUBITAK has contracts with academician from universities. Assoc. Prof. Dr. Hakan Erdogan works for Sabanci University but he also worked as an advisor to TUBITAK in the area of biometrics, security and privacy preservation techniques. Dr. Cagatay Karabat and Berkay Topcu worked with Prof. Hakan Erdogan in this paper within this concept.

2.6 Submitted papers in journals

2.6.1 IDIAP

"On the use of client identity information for face anti-spoofing", I. Chingovska and A. Anjos, IEEE Transactions on Information Forensics and Security, Special Issue on Spoofing and Countermeasures, 2015.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" including spoofing. The paper proposes a novel approach for anti-spoofing based on generative modelling of client specific information as opposed to the use of regular discriminative methods.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:
  n/a

2.6.2 UAM

"Multi-Biometric Template Protection Based on Homomorphic Encryption", M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi and J. Fierrez, IEEE Trans. on Information Forensics and Security, 2016.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:
  This paper is directly relevant to WP4 "Evaluation of Vulnerabilities" and WP5 "Evaluation of Privacy Preservation". The paper presents a new method to protect multi-biometric systems based on fixed-length templates that enables privacy preservation.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:
  This work was mainly conducted by M. Gomez-Berrero, a PhD student at UAM, during a research stay with Prof. Dr. P. Campisi at Universita Roma Tre (Italy). Prof. Campisi is a renowned expert in biometric security, which helped with his expertise using cutting edge methods (in this case Homomorphic Encryption).

2.6.3 TUBITAK

"Practical Security and Privacy Attacks Against Biometric Hashing Using Sparse Recovery," Berkay Topcu, Cagatay Karabat, Matin Azadmanesh, Hakan Erdogan, submitted to ," submitted to EURASIP Journal on Advances in Signal Processing.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  This paper is relavant to "Task 5.1 Privacy preservation techniques" of "WP5 - Evaluation of Privacy Preservation" and more specifically it is directly linked with D5.4 Advanced privacy preservation system. This paper performs several attacks against the reference privacy preservation system (biohashing method) in order to analyze its possible security and privacy flaws. This security and privacy analysis are very critical input for D5.4.
- Authors outside the consortium (yes [X] / no [ ]) if yes explain their participation:

  TUBITAK has contracts with academician from universities. Assoc. Prof. Dr. Hakan Erdogan works for Sabanci University but he also worked as an advisor to TUBITAK in the area of biometrics, security and privacy preservation techniques. Dr. Cagatay Karabat and Berkay Topcu worked with Prof. Hakan Erdogan and his PhD student Matin Azadmanesh (who was also funded by TUBITAK according to the agreement between TUBITAK and Prof. Hakan Erdogan) in this paper within this concept.

2.6.4 MORPHO

"Security analysis and improvement of some biometric protected templates based on Bloom filters", Julien Bringer, Constance Morel and Christian Rathgeb, "Best of Biometrics 2015" Special Issue of the Image and Vision Computing Journal, Elsevie, 2015.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project: This work has been made during WP5 works on privacy metrics for biometric privacy preserving system. The article is an extension of our ICB 2015 paper and describes the study of an existing scheme from ICB 2013, and several variants of this scheme, and introduces different strategies to threaten the privacy properties of those schemes by exploiting the imperfect randomness of biometric data. This underlines the importance of taking in account the biometric properties when analysing a scheme and of thorough privacy evaluation. The paper additionally introduces a enhanced construction based on secure multiparty computation.
- Authors outside the consortium (yes [X] / no []) if yes explain their participation: The author outside of the consortium collaborated with MORPHO as he is one of

the co-author of the ICB 2013 scheme. This collaboration enabled us to consider a practical parameterizing of the scheme and to cover the new variants.

2.7 Submitted books or book chapters

2.7.1 KULEUVEN

"Wat brengt de nieuwe Verordening Algemene Gegevensbescherming ? Een eerste kritische analyse", E.Kindt, in Recht in Beweging, VRG (ed.), Maklu, 2016.

- Correspondence of this paper to the BEAT results and how much it is directly relevant to the project:

  In this book chapter, the author discusses the new major new developments in General data protection for the Belgian legal counsels and attorneys. This research was made possible by the BEAT project.
- Authors outside the consortium (yes [ ] / no [X]) if yes explain their participation:

2.8 News and Press release

All press and news related to BEAT activities are listed on the BEAT project website (`https://www.beat-eu.org/news`) and on the Swiss Center for Biometrics Research and Testing website (`http://www.biometrics-center.ch/news`). We provide below a snapshot of these press and news.

"How do we create standards ISO ?", IDIAP, Swiss TV, 2016.

[`http://www.idiap.ch/scientific-research/news/how-do-we-create-standards-iso`]

It is a Swiss premiere. The Idiap Research Institute in Martigny receives this week delegates from all around the world that have the task of creating the famous ISO standards. They will discuss about the standards in the domain of biometrics. The Idiap researcher Sébastien Marcel explains the procedure and the stakes of this scientific meeting.

"ISO Biometrics standards", IDIAP, Swiss Radio, 2016.

[`http://www.idiap.ch/scientific-research/news/sebastien-marcel-head-of-the-swiss-`

This short interview talks about Standards in Biometrics on Swiss radio.

"Can Biometrics Defeat Cyberterrorists?", IDIAP, Science Channel, Through the Wormhole with Morgan Freeman, 2014.

[`http://www.biometrics-center.ch/news/can-biometrics-defeat-cyberterrorists`]

At Switzerland's Idiap Research Institute, one man is on the front lines of the fight against cyberterrorism. He's an expert in biometrics. The more individual the biometric, the more difficult it is to attack.

"Vulnerabilities of iris recognition", UAM, BBC News / CNN / WIRED, 2012.

[http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-bla

[http://www.bbc.com/news/technology-18997580]

[http://www.wired.com/2012/07/reverse-engineering-iris-scans/all/]

The talk elaborates that the binary code used in biometrics databases to represent scanned iris images do not contain enough information to allow the original iris image to be reconstructed, but there are procedures to reconstitute the original images from binary templates. Experiments show that although they wouldnt fool a human biometrics expert, the reconstructed images may be good enough to fake out an iris recognition system.

"Europe hopes to set framework for biometric standards", BEAT consortium, BiometricUpdate, 2012. [http://www.biometricupdate.com/201209/europe-hopes-to-set-framewo

A new Biometrics Evaluation and Testing (BEAT) project has been launched and is funded by the European Commission, under the Seventh Framework Programme, in order to set a framework for systematically evaluating the performance of biometric technologies using several metrics and criteria.

"New Idiap biometrics applications is born!", IDIAP, Idiap press release, 2014.

[https://www.idiap.ch/scientific-research/news/new-idiap-biometrics-applications-

The Idiap research institute and the University of Applied Sciences and Arts Western Switzerland jointly developed a prototype of mobile finger-vein sensor for portable or embedded biometrics applications. Most of the technologies for finger-vein capture are based on a transmission technique of Near-Infrared Light (NIR), while the developed prototype is based on a reflexion technique using an innovative configuration of NIR illumination. This work was jointly funded by the European project FP7 BEAT, the HES-SO project VERA and the Swiss Center for Biometrics Research and Testing.

"Research and doctorate defence", KUL, 2012.

Press coverage at the KU Leuven public website, as well as in Dutch and Belgian legal journals such as Computerrecht, Privacy en Informatie (P&I) and Nieuw Juridisch Weekblad (NJW) about the research and doctorate defence before the examination commission at the Faculty of Law of the KU Leuven on 14 May 2012 on the legal aspects of biometric data processing and subsequent publication with Springer. The Processing of Biometric Data. A Comparative Legal Analysis. This was picked up on some websites as well.

2.9 BEAT workshops and main actions

In this section, we review the main actions we organized or co-organized to disseminate the main outcomes from the BEAT project during workshops or other events.

"European Biometrics Symposium on Presentation Attack Detection in Martigny", IDIAP, 2016

[http://www.eab.org/events/program/108]

In cooperation with the European Association for Biometrics (EAB) we organized the EAB annual Symposium in Martigny Switzerland on Jan 19 2016 afternoon after the meetings of the ISO/IEC JTC1 SC37 Biometrics. The Symposium focused on Presentation Attacks and Presentation Attack Detection and hence on the BEAT project that revealed the two main outcomes: (1) a methodology for Common Criteria evaluations of biometric systems, (2) the BEAT platform as a tool for the characterization of biometric performance.

"EAB Research Project Conference", all partners, 2014, 2015 and 2016 (planned).

2014: [http://www.eab.org/events/program/69]

2015: [http://www.eab.org/events/program/79]

2016: [http://eab.org/events/program/104]

Biometrics and Identity Management are key research topics that are currently investigated in a number EU-projects running under the seventh Framework program. International research is dealing with innovative solutions for secure and privacy compliant biometrics and federated identity management. The EAB and the EU-projects FIDELITY, FastPass, BEAT, Future-ID, INGRESS, are jointly organizing a Research Project Conference (EAB-RPC), to present research results and in order to discuss the benefit of this research for our European society. Moreover experts from the biometric community will discuss on a panel Ethical and Privacy Issues of Biometrics and Identity Management. Furthermore a second panel will be devoted to discuss and identify future research topics in the Horizon2020 research program.

"Tutorial on the BEAT platform", IDIAP, FG and BTAS conferences, 2015

[http://www.idiap.ch/~marcel/professional/FG_2015.html]

[http://www.idiap.ch/~marcel/professional/BTAS_2015.html]

This tutorial presents the BEAT platform for online reproducible research, introducing concepts and providing an initial hands-on experience. The BEAT platform allows novice and advanced researchers to: (1) benchmark systems and components; (2) run comparative evaluations; (3) attest (certify) toolchains; (4) provide educational material for new-comers in pattern recognition and (5) optimize algorithms and systems. All these tasks can be accomplished without installing additional software on the users computer, running exclusively from the web browser. The BEAT platform naturally enforces important research aspects such as reproducibility and component re-use.

"Reproducible research in Biometrics: Moving to the BEAT", S. Marcel from IDIAP, Keynote ICB 2015.

[http://icb2015.org/keynote-speakers]

Research in Biometrics is overwhelmed by the constant influx of new algorithms and techniques promising improved performance, generalization and robustness. However, reproducibility of results is often an overlooked feature accompanying publications and benchmark evaluations. The main reasons behind such a gap arise from natural complications in research and development of Biometrics: the distribution of biometric data is a sensitive issue for most countries and organisations; software frameworks are difficult to install and maintain; test protocols may involve a potentially large set of intricate steps which are difficult to handle.

In this keynote, we first explained and demonstrated why reproducible research is important and beneficial. Next we reviewed recent work in reproducible biometrics ranging from face and speaker recognition to spoofing and anti-spoofing. However, given the raising complexity of research challenges and the constant increase in data volume, the conditions for achieving reproducible research in the domain are also increasingly difficult to meet. To bridge this gap, we present a biometry-independent platform for Biometrics research, development and certification. By making use of such a system, academic, governmental or industrial organizations enable users to easily and socially develop processing toolchains, re-use data, algorithms, workflows and compare results from distinct algorithms and/or parameterizations with minimal interaction. The keynote presented the BEAT platform (`https://www.beat-eu.org/platform/`) and discussed some of its key features.

"Swiss Center for Biometrics Research and Testing", IDIAP, 2014.

[`http://www.biometrics-center.ch`]

The Swiss Center for Biometrics Research and Testing is an instrument proposed and created by Idiap to take over the legacy from the BEAT project and more particularly to maintain the BEAT platform and to distribute publicly the BEAT deliverable D6.5 "Toward Common Criteria evaluations of biometric systems". The Swiss Center for Biometrics Research and Testing is described in more details in the deliverable D8.6.

3 Planned dissemination activities

In the following, we briefly report some dissemination activity which BEAT partners, jointly or independently each others, are planning to conduct.

3.1 IDIAP

- (Planned) Organization of a tutorial on the BEAT platform at ICB2016.
- (Planned) Submission of a journal paper on the BEAT platform.
- (Planned) Presentation of the BEAT project to the EAB Research Project conference.

3.2 UAM

- (Planned) Submission of conference proposal to BlackHat USA 2016
- (Planned) Submission of papers to ICPR 2016 and CVPR Workshop on Biometrics 2016
- (Planned) Submission of papers to IEEE Trans. on Information Forensics and Security
- (Planned) Continuation of KBOC Keystroke Biometrics Ongoing Competition on the BEAT Platform during 2016
- (Planned) Presentation of BEAT project results to the Japan Identification Systems Association (JAISA), OKI Software, and the Japanese National Institute of Advanced Industrial Science and Technology (AIST) in March 2016
- (Planned) Presentation of BEAT project results at the third EAB Research Project Conference in September 2016

3.3 EPFL

- (Planned) participation to the BEAT Workshop during the EU Research Project Conference

3.4 CHALMERS

- (Planned) Submission of papers to CANS, SAC and other security related conferences and journals

3.5 TUBITAK

- (Planned) Submission of a paper to the NIST International Biometric Performance Testing Conference, 2016.
- (Planned) Talks on BEAT at various events on biometrics, security and privacy.

3.6 MORPHO

- (Planned) Submission of papers to BTAS, ICB (or IJCB), IFS, WIFS, or embedded security (CARDIS, COSADE) conferences/journals

3.7 KULEUVEN

- (Planned) Co-promotorship of master thesis of law student studying use of BEAT platform for forensic research.

  This academic year 2016-2017, a student will be offered an internship at the Dutch NFO for studying legal aspects of the use of biometric data on the BEAT platform for forensic use. He will be co-supervised by a researcher-lecturer of the BEAT consortium.

- (Planned) Guest lectures on the use of data for research purposes.

  During this academic year and the year 2016-2017, further research on the use of data for research will be supervised. The knowledge and research of the BEAT project will be taken further in this context, expecially with regard to the new General Data Protection Regulation for research.