MAX SNIJDER PASSED AWAY

(This text is reproduced with permission of EAB board).

Max Snijder passed away on Friday, 27 April 2018. He served as secretary for the Management Board of the European Association for Biometrics since its foundation. Our thoughts are now with his family but in deep mourning we will continue his work. Based on his operational experience (e.g. with the deployment of Biometrics at Schiphol) in early 2000, he was instrumental in establishing the European Biometrics community. After a career as entrepreneur in the not-for-profit sector Max became one of the pioneers of biometrics in the Netherlands. After several years of extensive experience with numerous biometric projects like Privium at Schiphol Airport, he founded the European Biometrics Group in 2004, a consulting firm focusing on biometrics technology and its application. He wrote numerous reports for instance for The Scientific Council for Government Policy (WRR) and several articles for magazines and newspapers. Max, like no one else, knew how to convince the European Commission of important and useful projects in the field of biometrics. BioTesting Europe or BEST Network are examples of this. Their steadiness was very important to him.

Max Snijder was one of the co-founders of the European Association for Biometrics and served in the Management Board as its secretary from its very beginning in November 2011.

He devoted his energy to the purpose of bringing together the fragmented knowledge and experience in the field of biometrics. For Max it was important that the EAB is an organization open to representatives from many backgrounds like academia, governments, companies and not for profit organizations. Max was a principled man regarding biometrics and security, he was worried about far-reaching technical control of society but stayed a realist.

Many people characterize Max as a friendly, independent, open person. Next to that, Max was a very talented musician, mastered a few instruments and played violin in the Bach Ensemble Amsterdam. Also, Max has played for many years in upper veterans field-hockey leagues in the Netherlands, his last year even in the top league.

In the last year the fight against a serious disease consumed all his energy - but he continued to work for EAB until very recently. We will miss Max very much. In deep mourning we will continue his work.

Alexander Nouak, Christoph Busch, Manus Fleskens, FarzinDeravi and Rasa Karbauskaite
Researchers create photo filter that disables facial recognition
At the University of Toronto, Professor Parham Aarabi and graduate student Avishek Bose are using neural-network based constrained optimization to produce small perturbation that, when added to an input face image can fool pre-trained face detector. They use and adversarial training approach involving two neural networks with opposite objectives.

Face, iris and pulse biometrics close in on fingerprint tech
According to a new report from ABI Research, face, iris and pulse-based biometric authentication systems will increasingly eat away at the market share of fingerprint technologies. Falling cost of iris recognition and increasing accuracy of face recognition are major factors for the predictions. Further, use of face recognition in mobile devices and policies around utilization of biometrics in banking and telecom sectors adds to adoption of the technology.

Human plus machine – face recognition at its best
A team of scientists from the National Institute of Standards and Technology in the US and three universities including UNSW Sydney have studied to compare face recognition performance of forensic facial examiners, super-recognisers, and computer algorithms. The forensic facial examiners are trained for the task, whereas the super-recognisers are have natural ability for face identification. The study revealed that a combination of human and computer decision-making is most accurate.

Ottawa expands program to collect fingerprints, photos from foreign nationals coming to Canada
Canada is expanding a program to collect biometric data from foreign nationals entering the country. The program's expansion from 30 to about 150 countries will strengthen immigration system with the ability to quickly and accurately establish a traveller's identity, says Immigration Minister Ahmed Hussen. Experts are warning of the potential for heightened risks to privacy.

Apple® granted patents for device with ultrasonic fingerprint
Apple's newly granted patent covers their invention relating to an ultrasonic touch sensor that identifies various aspects of a touch on a device. The sensor may be configured to identify biometric information, such as fingerprint, associated with the touch. By identifying the fingerprint associated with a touch, the identity of the user can be verified, which may be useful for authorizing a transaction or performing a security operation.

New Zealand uses face recognition tools to control problem gambling
The face recognition system is expected to be used for access control. It will keep a tab on people accessing gaming rooms. Problem gamblers who have asked to be barred from certain venues can voluntarily add their photos, and on attempting to access those venue, the staff is alerted. At present, 15 gaming venues are utilising the software; six more venues are planning to install. "It would allow the venue to take action in quiet and respectful ways.", says Paula Snowden, Problem Gambling Foundation.

Apple is trademarks of Apple Inc., registered in the U.S. and other countries.
**Question:** Can you envisage successful techniques in building ensembles of deep networks? How straightforward could be to achieve complementarity and more generally what approaches could be successful in practice?

**Josef:** There is strong experimental evidence that ensembles of deep networks outperform single networks. This is rather surprising, as any deep neural network can be considered as an ensemble. However, different networks in an ensemble offer different solutions to the same problem. Their fusion simply provides a better estimate of support for the respective hypotheses, and in this sense, it is bound to produce a better solution. The issue of accuracy and diversity is still an open problem.

**Question:** Do you believe that classical statistical approaches and the deep learning approaches can co-exist? Or, is the end-to-end network the natural upgrade (and replacement) over the classical statistical techniques?

**Josef:** There are horses for courses. It is doubtful that deep learning solutions will always be appropriate for all decision-making problems encountered in future. We may face the problem of lack of data for training, or engineering design constraints that will preclude the use of a deep learning solution. In any case, even if a deep learning method is successful, the final decision-making reverts to simple statistical rules such as the nearest mean classifier in the resulting feature space. Thus in my opinion, classical methods will continue to co-exist with the latest deep neural network approaches.

**Question:** How do you consider the alternative approaches to deep learning, for instance those based on ensembles of deep forests? Do you think they might be more efficient (setup effort/accuracy of results) compared with deep neural networks?

**Josef:** This question is a variant of the previous query. Extending the scope from statistical methods to shallow machine learning approaches in the above answer, the same response applies.

**Question:** Which do you consider to be the most important issues to be solved in biometrics, i.e. that will occupy research in the forthcoming years?

**Josef:** There are probably many topics that warrant research focus in the future. With my own interest in face recognition in mind, there is the need to improve the capability of unconstraint face recognition to enable more successful surveillance technology that can cope with face images of CCTV quality. It is still challenging to recognize faces of low resolution, subject to blur, from top down camera views typically captured by CCTV installations. There is also the need to improve the capability of soft biometrics that come to play when face data is not available or unusable. The fusion and seamless integration of multi-modal biometrics (face, soft biometrics, gait, and voice) is also on the cards. The improving face recognition technology will also have to be matched with more resilient countermeasures to various forms of biometric system attack.

**Question:** What would you suggest to a young researcher approaching machine learning topics?

**Josef:** Please do not get disheartened by the rapidly growing field. There are many issues to tackle and many phenomena to understand. There is a room for everybody, but beware of working on your own. A critical mass and good facilities are needed to remain competitive.

Josef Kittler is awarded the title Distinguished Professor of the University of Surrey since 2004. Among his several achievements and honors, it is worth mentioning the KS Fu Prize 2006, by the International Association for Pattern Recognition, for outstanding contributions to Pattern Recognition. At present he is a member of the KS Fu Prize Committee of IAPR.
New Database by IIIT Delhi: Unconstrained Fingerphoto Database (UNFIT)

During the CVPR 2018 workshop on biometrics, IIIT Delhi has presented UNFIT the first public unconstrained finger photo database. A fingerphoto is an image of the frontal part of a finger captured by a smartphone camera. This dataset works to create a user friendly, cost effective alternative, and overcome the typical challenges of unconstrained acquisition environments such as multiple fingers, background, orientation, deformation, and user-cooperation. The proposed baseline uses deep learning-based segmentation, CompCode, and ResNet50. 3450 images from 115 subjects with the finger location of every finger annotated made up the dataset. In an unconstrained environment, finger photos were taken for the database with a segmentation algorithm. VGG SegNet and FCN 8 were the classification networks used to perform fingerphoto segmentation. CompCode and ResNet provided further baseline results of fingerphoto authentication. Ten finger photo images were captured from each subject totaling 1150 images. 45 different smartphones were used to take the finger photos; some used online data collection apps like Facebook Messenger or WhatsApp while others used offline procedures. The different mechanisms in phones such as auto-focus or flash allowed for intensity, scale, rotation, translation, background, blur, and illumination to be added to the variations in the database. To combat these obstacles a deep learning method was used to segment the foreground finger photos. A GUI based segmentation tool in MATLAB called Piotr Dollar's toolbox was used to manually annotate each image. It located and annotated the finger regions by using rectangular rotating bounding boxes. All of the ground truth annotations and the database are made publicly available.

Figure 1–Sample images of UNFIT representing challenges typically encountered in an unconstrained environment.

Fingerprint Segmentation

Finger photo segmentation and matching benchmarks for finger photo segmentation and authentication. The UNFIT database had a total of 3450 images which were evenly split into the train and test subsections in a subject disjoint manner. Uniqueness in a fingerprint comes from the ridge valley pattern, therefore the paper attempts to remove any background information that would affect the images. The framework for fingerphoto segmentation makes use of the VGG SegNet architecture to achieve a “tight bound on the finger photo”. A layer of smoothening (32x32 blockwise) is added to help increase the number of foreground pixels. The VGGSegNet has decoder, encoder networks and Softmax classification layer which would predict if the test pixel was a foreground pixel and classify the image accordingly. This algorithm is similar to the VGG FCN 8 in which FCN (fully trained convolutional network) is adapted with 32x32 block wise smoothening as well. The VGG SegNet encoder was given an image with the size 224x224x3 and the output of this image was a multi-channel image (14x14x512). The decoder output was given to the Softmax layer to perform binary classification on each image pixel. The binary mask with white pixels represented a presence of a finger and the black pixels were non-finger regions. The FCN was also given 224x224x3 size images and masks of the size 224x224x3, in which 0 meant presence of background and 1 was represented by foreground. The training datasets were augmented and then used for fine tuning the deep architectures. Image augmentation involved rotation, mirror flip, blurred and intensity changes to the training set. This was also comparable with the skin color-based segmentation which converted the original RGB image to YCbCr and HSV color space.

Segmentation Performance Metrics

There were 3 metrics that were used to test the performance of the finger photo segmentation.

- $SA = \frac{CCB}{TB}$
- $FSA = \frac{CCFB}{TFB}$
- $BSA = \frac{CCBB}{TBB}$
Feature Extraction and Matching

There are two algorithms that were used: CompCode and ResNet50. CompCode uses Gabor filters with $J$ different orientations varying by $\pi/2$. These features are extracted with Gabor filter $G_{rad}$ and are matched using the Hamming distance to get a distance score. The segmented images were first resized to a size of 400x400 and then the CompCode was extracted. They also used ResNet50 architecture to get feature representation which was matched with cosine similarity. The ROC curve was used to present the verification results.

Figure 2: The step by step process of the segmentation framework using VGG SegNet and then 32 x 32 block-wise smoothing.
The recent threats to user data privacy, and the revealed abuses, have attracted and raised the public attention on the problem of data protection. In the era of services going online, personal data of users has become a powerful weapon to dominate the market, and bigger corporations are collecting more information than ever, often infringing user privacy. In addition, companies are increasingly implementing biometrics-based authentication, so that user biometric data has become a potential target of data collection. In this scenario, biometric identifiers deserves a special attention. Actually, their safeguard has been a concern, though in restricted administrative contexts, since the times of Pay by Touch's bankrupt and consequent uncertain fate of customers' biometric data. In the early 2000s, this company was a pioneer in proposing consumer biometric technologies. It proposed a system enabling users to link various accounts (credit cards, checking accounts, etc.) to their fingerprints. After subscribing the service, it was possible access accounts or make a payment with the simple touch of a finger. The novelty achieved a wide success, and consumers in the order of millions signed up. Unfortunately, after a few years, by late 2007, the company was caught in controversies taking to final bankruptcy and, and end of all operations in in March 2008. This event spurred Illinois to pass in 2008 the Illinois Biometric Information Privacy Act (BIPA), the first state law in U.S. governing the collection, use, safeguarding, and storage of biometric information (Illinois Biometric Privacy Act, 740 ILCS 14/1 et seq.). It is interesting to notice that the act clearly points out a specific characteristic of biometric information that especially calls for its protection: “Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” (BIPA 740 ILCS 14/5(c)). In practice, permanence of a biometric identifier is considered a favouring characteristic for the technology, however, it becomes a threat if this data is compromised. As another controversial point, the prescribed rules are limited to biometric identifiers and information derived from them (biometric information), with the following definition: “Biometric identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.” (BIPA 740 ILCS 14/10(c)). Nowadays, this seems a too restrictive definition, given the spread of biometric research related to more and more potentially identifying traits. Notwithstanding this, other U.S. states that later passed similar laws adopted an even less threatening formulation, possibly due to the action of interested lobbies. In 2009 Texas passed the “Capture or Use Biometric Identifier Act”, and some time later, in early 2017, Alaska, Connecticut, Montana, New Hampshire, and Washington (legislation effective from July 2017) each proposed their own laws on similar topics. Differently from the others, Utah's statute restricts the use of biometric information only in colleges and other schools. Interested readers can find more information in the document “Illinois's Biometric Information Privacy Act Spurs Similar Legislation Around the Country” at

https://www.lockelord.com/newsandevents/publications/2017/11~/media/162040E9E735479BB887E49BD0C91EF0.ashx. In practice, it appears that 50 different – although similar in some points – laws about data privacy hold in U.S. This is a problem for companies with a nationwide or even global target market. All 50 laws, plus some introduced by the Congress, require to implement and maintain reasonable security procedures and practices to safeguard personal information. However, details are often very different. To this respect, it is enlightening to have a look at the “Summary of U.S. State Data Breach Notification Statutes” by Davis Wright Tremaine LLP (https://www.dwt.com/statedatabreachstatutes/).

In the described context, some suggest that a good choice may be to apply the newborn EU's General Data Protection Regulation (GDPR) which is already changing the scenario of data protection in Europe. Also in this case, it is interesting to have a look to “Data breach notification: 10 ways GDPR differs from the US privacy model” by PwC (https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html). It appears immediately a broader definition of “personal data” as any data that can be directly or indirectly associated with a
living individual. This also includes many items excluded by BIPA. Moreover, GDPR is tougher regarding points such as, for example, the risk threshold for reporting, circumstances requiring the government notification, and also what consumers must be told about a breach. According to Veridium, adopting the GDPR “will not put companies in compliance with all the different state standards”, being those so different from each other, but operating under stricter requirements would allow a safer data management. Given this, notwithstanding the GDPR was adopted by the EU in 2016 giving companies 24 months, until May 25 of this year, to be compliant with the data collection and protection law, neither the firms nor the intended regulators are fully prepared yet.

China is a third stakeholder that is mandatory to consider together with U.S and EU. The Chinese government recently released the final version of a new national standard on personal information protection. It was set to take effect May 1, 2018, but even in this case it is not clear how the standard will be implemented. What is clear is that it has some similarities with the European Union’s General Data Protection Regulation (GDPR). For example, while the GDPR applies to specific types of data, the definition of “sensitive personal information” under the Chinese standard seems even more encompassing. It extends protection to any personal data that “would cause harm to persons, property, reputation, and mental and physical health if lost or abused”. From one side, the Chinese standard contains more rigorous requirements on what kinds of information must be included in privacy notices (“one by one”) and on security testing. On the other side, it seems to allow for silent consensus in some cases, which is a controversial modality that GDPR addresses more explicitly. Overall, the Chinese regulation seems closer to GDPR than to U.S. rules, and this may pose puzzling requirements on practitioners.

As a summary observation, it is to underline that data privacy and security are inspiring even more fragmentation and market barriers that forbid flows across borders. For instance, China and Vietnam require that data is stored in servers within national borders. This makes international interoperability a growing challenge. While this is critical for commerce and industry, it is not clear yet how it can affect the circulation of data for research purposes.
General Framework to Evaluate Unlinkability in Biometric Template Protection Systems

Marta Gomez-Barrero*, Javier Galbally†, Christian Rathgeb*, Christoph Busch*
*da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany, 
†European Commission - DG-Joint Research Centre, E3, Italy, (javier.galbally@ec.europa.eu).

Unprotected storage of biometric reference templates poses severe privacy threats, e.g., identity theft, cross-matching or limited renewability. This has been reflected within the EU General Data Protection Regulation 2016/679 [1], where biometric data are defined as sensitive data.

To preserve the privacy of the individuals accordingly, the ISO/IEC IS 24745 on biometric information protection [2] requires that “knowledge of the transformed biometric reference cannot be used to determine any information about the generating biometric sample(s) or features” (i.e., need for irreversible templates). But not only that, the ISO/IEC standard continues by stating “[... and] the stored biometric references should not be linkable across applications or databases” (i.e., need for unlinkable). In order to comply with such requirements, researchers have proposed multiple template protection techniques [3].

In this context, a standardised benchmark protocol for biometric template protection (BTP) schemes, in terms of recognition accuracy, security and privacy, is necessary to properly evaluate the performance of these techniques [4]. However, little attention has been paid to the objective evaluation of the template’s unlinkability [4]. In fact, there is still no general framework to assess, in an objective way, the unlinkability of biometric templates, since the existing articles share some common shortcomings, including: unrealistic assumptions on uniformity of biometric data and the development of non general approaches for specific systems [5]–[7]. The consideration of unlinkability as a binary decision [5], [6], [8]–[11], the lack of a quantitative measure [12]–[14] or the use of metrics employed for verification accuracy evaluations, not suitable for the unlinkability evaluation [6], [7], [9]–[11], [15].

Due to the aforementioned limitations, no standardised unlinkability metric has been included in the current ISO/IEC 30136 project on performance testing of BTP schemes [16].

The general framework for unlinkability assessment proposed in the present article addresses the existing shortcomings of previous methods and offers the following advantages:

- No assumptions are made on the data, neither on independence nor on uniformity.
- Only a classification function, named as “linkage function”, is assumed to exist, in order to assess the non-binary nature of the unlinkability property [7].
- The proposed metrics evaluate unlinkability based on score distributions obtained from the linkage function, independently of what the function is. This allows for a general metric, since it can be computed for any Lebesgue integrable linkage function.
- Also a local unlinkability measure for each linkage score is proposed, in order to allow a more thorough evaluation.
- Being able to use the same metric independently of the linkage function has the advantage of allowing to monitor the changes in a system’s unlinkability when different functions are used to compare the templates.

A Python implementation of the metrics is available through the da/sec website (https://dasec.h-da.de/research/biometrics/unlinkability/) and the da/sec Github account (https://github.com/dasec/unlinkability-metric).

I. PROPOSED METRICS

From an analytic perspective, unlinkability can be defined as a gradual property of the templates:

**Definition of unlinkability:** two templates are *fully linkable* if there exists some method to decide that they were extracted, with all certainty, from the same biometric instance. Two templates are *linkable to a certain degree* if there exists some method to decide that it is more likely that they were extracted from the same instance than from different instances.

It thus follows that this property is fully related to the *method* (i.e., linkage function) used to decide if two templates stem from the same instance.

A. Local Measure $D_{s1} (s)$: System Score-Wise Linkability

$D_{s1} (s) ∈ [0, 1]$ evaluates the unlinkability of a system for each *specific linkage score* $s = LS (T_1, T_2)$. As such, this metric is appropriate to analyse within one system in which parts of the linkage score domain it fails to provide unlinkability. If for a specific score $s_1$, a system yields $D_{s1} (s_1) = 1$, it means that, in case the linkage function produced $s_1$, we would be able to link both templates $T_1$ and $T_2$ to the same instance with almost all certainty. On the other hand, $D_{s1} (s_1) = 0$ should be interpreted as full unlinkability for that particular score $s_1$. In other words, if $s_0$ were produced by the linkage function, it would be more likely that both templates stemmed from different instances, hence failing to link them to a single data subject. All intermediate values of $D_{s1} (s)$ between 0 and 1 report an increasing degree of unlinkability.

The key on the success of linking to templates lies on determining whether, given a score $s$, it is more likely that two templates stem from mated samples ($H_m$) than from non-mated samples ($H_{nm}$): $p (H_m | s) > p (H_{nm} | s)$. Therefore,
such linkability can be accounted for in terms of the following difference of conditional probabilities:

$$D_M(s) = p(H_m|s) - p(H_{nm}|s)$$

However, these two conditional probabilities are unknown. Hence, we start the computation from the likelihood ratio

$$LR(s) = \frac{p(s|H_m)}{p(s|H_{nm})}$$

between the known probabilities.

Denoting \( \omega = p(H_m)/p(H_{nm}) \) as the ratio between the unknown prior probabilities of the Mated samples and Non-mated samples distributions, we can define \( D_M(s) \) as a two-part function of \( s \) as follows:

$$D_M(s) = \begin{cases} 0 & \text{if } LR(s) \cdot \omega \leq 1 \\ \frac{LR(s) \cdot \omega}{1 + LR(s) \cdot \omega} - 1 & \text{if } LR(s) \cdot \omega > 1 \end{cases}$$

where \( D_M(s) = 0 \) for \( s \) such that \( LR(s) \cdot \omega \leq 1 \) (i.e., unlinkable score values where \( p(H_m|s) \leq p(H_{nm}|s) \)). If the prior probabilities \( p(H_m) \) and \( p(H_{nm}) \) are available, use them to compute \( \omega \). Otherwise, we can assume that \( p(H_m) = p(H_{nm}) \), and thus set \( \omega = 1 \).

B. Global Measure \( D_{GM}^M \): System Overall Linkability

It is also useful to have an estimation of the unlinkability of the whole system, which may allow a fairer benchmark of the unlinkability level of two or more systems. For this purpose, we introduce the global metric \( D_{GM}^M \in [0,1] \), which gives an estimation of the global linkability of a system, independently of the score. This way, if a system has \( D_{GM}^M = 1 \) (i.e., case in which both the Mated samples and Non-mated samples distributions have no overlap), it means that it is fully linkable for all the scores of the Mated samples distribution domain. Similarly, \( D_{GM}^M = 0 \) means that the system is fully unlinkable for the whole score domain (i.e., full overlap of the distributions). That is, independently of the score produced by the linkage function, it is equally probable that the two templates stem from the same instance \( (H_m) \) than from different instances \( (H_{nm}) \). All intermediate values of \( D_{GM}^M \) between 0 and 1 report an increasing degree of linkability.

Therefore, we are interested in measuring how likely it is to get a score stemming from the Mated samples distribution. This can be achieved computing the difference \( p(H_m \cap s) - p(H_{nm} \cap s) \) and integrating it. Regarding the success on linking templates, we are only interested in the probabilities stemming from the Mated samples distribution, and two templates can be linked only if \( p(H_m|s) > p(H_{nm}|s) \). Hence, we define \( D_{GM}^M \) as

$$D_{GM}^M = \int p(s|H_m) \cdot (p(H_m|s) - p(H_{nm}|s)) \, ds$$

$$p(H_m|s) > p(H_{nm}|s)$$

$$= \int p(s|H_m) \cdot D_M(s) \, ds$$

This way, the final value of \( D_{GM}^M \) depends on: i) the domain of scores where the system is linkable; ii) how linkable the system is in that domain of scores; and iii) how probable it is that such scores are produced. Therefore, this new global measure assigns different levels of linkability to intermediate scenarios, not fully unlinkable or fully linkable.

II. PROPOSED LINKABILITY EVALUATION PROTOCOL

It should be noted that, in practice, linkability is defined as the ability to link templates across different applications (i.e., stored in databases used by different applications). With this in mind, the proposed protocol runs as follows:

1) Generate \( K \) datasets of protected templates each of them using a different key. It is recommended that \( K > 5 \).
2) Compute the Mated samples and Non-Mated samples score distributions for the selected linkage function, across the \( K \) databases generated in step 1.
3) If \( p(H_m) \) and \( p(H_{nm}) \) are available, use them to compute \( \omega \). Otherwise, set \( \omega = 1 \).
4) Compute \( D_M(s) \) and \( D_{GM}^M \).
5) Report \( D_M(s) \) plots, together with the Mated samples and Non-Mated samples distributions, and the corresponding global linkability values \( D_{GM}^M \) (see an example in Fig. 1).
6) Analyse the plots and \( D_{GM}^M \) values

III. CONCLUSIONS

We have proposed two new quantitative measures (\( D_M(s) \) and \( D_{GM}^M \)) for the unlinkability analysis of biometric templates, which can be applied to any BTP scheme. They provide the ability to carry out both a detailed score-wise analysis of the linkability of the templates and a benchmark of the linkability of different systems. Furthermore, the necessary steps towards a complete unlinkability evaluation have been proposed in order to develop a full security benchmark for biometric template protection schemes. We therefore believe that the proposed framework will contribute to the advancement of biometric technologies in the future.
REFERENCES


Bob

Different threats increase the risk that a research paper may contain a finding that is incorrect [1]. We read tones of research papers presenting results which in most cases are not easily reproducible. Indeed, given the increasing number of machine learning software alternatives, researchers may now design, implement and evaluate faster their proposals. However, the complexity of new proposals is also growing, making them harder to reproduce for comparison purposes. This motivation has lead the Biometrics Security and Privacy Group, and the Research and Development Engineers at Idiap to provide, through GitLab their free toolbox known as Bob [2,3]. The toolbox is therefore born with the aim at easing research reproducibility within the context of signal processing and machine learning. They both are certainly essential elements in biometric systems. Making research reproducible is challenging. Experiments are carried out using particular operating system and libraries releases, specific options, etc. Certainly a reduced number of research papers may provide not just results, but even code and data; however, it is certainly hard to maintain code stable, and therefore reproducible over time. According to Vandewalle [4], the levels of reproducibility in signal processing are:

1. Irreproducible
2. Cannot seem to reproduce
3. Reproducible, with extreme effort (> 1 month)
4. Reproducible, with considerable effort (> 1 week)
5. Easily reproducible (~15 min.), but requires proprietary software (e.g. Matlab)
6. Easily reproducible (~15 min.), only free software

The use of a standardized framework, sharing tools and environments, eases reproducibility, providing feedback within the community.

Bob authors consider research reproducible if it is: repeatable, shareable, extensible and stable. The toolbox provides different database interfaces, pre-processors, feature extractors, and recognition algorithms. Pre-compiled binary installations for Linux and MacOS 64-bit operating systems are available in the toolbox site. A sample use case focused specifically on biometrics was presented at ICML17 [3] evaluating a set of face recognition tool chains (comprising: data enhancement, feature extraction and recognition), integrated with database access and evaluation tools. Conda is used as package manager to install all specific required software version on the selected operating system, providing stability.

A more detailed description may be found related to the biometric framework of Bob, thanks to the tutorial at the International Joint Conference 2017 on Biometrics, describing the way to design and execute from basic face recognition experiments, to more complex ones, and even extending the framework to use a pre-trained deep network. The authors claim to present advantages compared to other open source biometric recognition frameworks such as OpenBR, CSU Face Recognition and the BEAT platform. Among the desirable features: 1) C++ and python APIs are provided, 2) a remarkably large library is available, i.e. large number of algorithms present, 3) Bob offers the possibility to extend the framework and use it for software development, 4) accepting image, video and audio in different formats, 5) all this is made possible using a simple interface. It is now the moment to see whether the community will make the toolbox successful.

References


Fingerprint Liveness Detection and Verification:  
Latest Results from FVC-Ongoing and LIVDET2017 Competitions

Fingerprint is often the biometric of choice for applications where high performance, public acceptance and ease of use are required. The fingerprint verification competitions (FVC2000, FVC2002, FVC2004 and FVC2006) organized by the University of Bologna in Italy have later evolved into the FVC-Ongoing competition. FVC-Ongoing aims to track the advances in fingerprint recognition technologies in a web-based automated fashion, measuring performance using well-known performance indicators and metrics on sequestered datasets.

A challenge facing fingerprint verification systems is presentation attacks, commonly referred to as spoof attacks. In this type of attack, an artificial replica of a fingerprint is generated by imprinting the fingerprint image on a material such as silicone. As the image characteristics can be exactly replicated, this type of attack is typically detected by checking for the “liveness” of the finger. Since 2009, the Fingerprint Liveness Detection Competition (LivDet), organized by University of Cagliari, aims to assess the performance of the state-of-the-art algorithms in detecting presentation attacks via artificial fingers.

FVC-Ongoing Fingerprint Verification

The competition is organized in several categories, including fingerprint verification, minutiae-based matching, orientation field extraction, fingerprint indexing and secure template based matching. While the minutiae-based fingerprint verification task had the highest number of participants (2350) since the inception of the competition in 2009, other tasks attracts fewer participants (e.g. fingerprint indexing had 176 and secure template verification had 57 participants respectively), showing where the competition lies.

The evaluation is comprehensive and done according to several metrics:

- **FMR1000**: False Non-Match Rate (FNMR) at a False Match Rate (FMR) <=0.1% (i.e. the lowest FNMR for FMR less than 1 in 1000).
- **FMR10000**: False Non-Match Rate at a FMR<=0.01%.
- **ZeroFMR**: the lowest FNMR at a FMR of 0%.
- **ZeroFNR**: the lowest FMR at a FNMR of 0%.

To date, Hisign has obtained the lowest False Non-Match Rate of 0.007% at a False Match Rate of 0.01% (FMR1000), on the standard database (FVC-STD-1.0). The Equal Error Rate (EER) of that system was 0.022%, while the False-Non-Match rate at zero False Match rate was 0.126%. Neurotechnology has the second lowest False Non-Match Rate of 0.032% at False Match Rate of 0.01%, with an EER of 0.042% and Tiger IT Bangladesh comes third currently.

These results are very impressive with the standard database, but when one considers the more difficult database (FVC-HARD-1.0), Hisign obtains a False Non-Match Rate of 0.797% at FMR1000, with a corresponding EER of 0.53%. This corresponds to roughly 100-fold increase in the FNMR and a 20-fold increase in EER. Sonda Technologies follows these results with a 1.035% FMR1000.

FVC-Ongoing also runs palmprint verification, face image ISO compliance verification and face morphing challenges. Read more at: https://tinyurl.com/y98fbbzb
Fingerprint verification systems are vulnerable to presentation attacks, namely, attacks made from artificial reproductions of fingerprints. These require materials such as silicon, gelatine or latex. Such “fake fingers” are also called “artifacts” according to the recent ISO terminology. Fingerprint presentation attacks detection systems are aimed to implement the ability to distinguish between live and fake fingerprint by hardware or software-based techniques. In particular, these are inspired from the pattern recognition theory. Since it is almost impossible to predict the materials and methods adopted to attack the system, designing a good fingerprint presentation attacks detector is not trivial.

The organization of the International Fingerprint Liveness Detection Competition (LivDet) since 2009, greatly contributed to advance the knowledge about materials and methods to design effective fingerprint liveness detectors. This was done thanks to the efforts of the PRA Lab’s Biometric Unit of the University of Cagliari (Italy) and the Biomedical Signal Analysis Lab of Clarkson University (USA). LivDet is traditionally subdivided in the Algorithms and Systems parts. In 2017, the first part only took place under the management of the University of Cagliari (http://livdet.diee.unica.it), whilst the second part is currently under the management of the Clarkson University (http://fingerprint2017.livdet.org).

The goal of the LivDet competitions is to assess the performance of fingerprint presentation attacks detection algorithms by using a common experimental protocol and data sets. The competitions are open to academic and industrial institutions which want to independently test their own solutions in terms of algorithms or whole hardware systems. Each edition is characterized by a different set of challenges against which competitors must face with. The results of the latest competition, held in 2017, related to the Algorithms part, were presented at the International Conference on Biometrics (ICB 2018) and already publicly available at the LivDet web site (http://livdet.diee.unica.it).

Seventeen competitors participated in the 2017 Algorithms edition. Main focus of this edition was on:

- Evaluating the effectiveness of the artifact at different level of the attacker’s experience.
- Never-seen-before materials in the test set.
- Exploring the effect of different user population on the system’s performance.

The data sets were captured by three electronic fingerprint sensors were adopted to acquire more than 12,000 images: Green Bit DactyScan84C, Digital Persona U.are.U 5160, and Orcanthus Certis2 Image.

The final winner of the competition, Hangzhou Jinglianwen Technology Co.Ltd, attained the average correct classification rate of 95.25% over the three data sets by a CNN-based approach. Skilled people may also impact on the attack’s effectiveness: this was pointed out by a drop of the classification rate to 91.35%, on average. Finally, the integration of verification and presentation attacks detection systems may be helped by the knowledge of live and fake samples of the user population. To sum up, the correct classification rate of solutions proposed in this competition significantly improved with respect to that of previous LivDet editions: from about 75% of the 2011 edition, to 91% of the last edition.
Human recognition using transient auditory evoked potentials: a preliminary study

Do we all listen in the same way? The authors in [1] claim a loud ‘no’. In their work published on “IET Biometrics” on April 19, they use the transient auditory evoked potentials (aka AEPs) in human recognition field. The AEP are neuroelectrical potentials generated by an auditory stimulus which reflects the neural response from the cochlea to the auditory cortex (Figure 1).

Historically, these bio-signals have been widely used in medical applications like emotion detection [2] or mental health assessment [3]. AEPs are divided in two different classes, depending on the type of stimulation: the transient AEP are generated from sharp clicks or tone burst stimuli and can be further classified in ELR, MLR and LLR (Early, Medium and Late latency response, respectively), depending on the latency of the acquired signal. These signals are often used for measuring hearing threshold in newborns and patients in unconscious state [4]. The steady-state AEP are generated by modulated tones, and usually are used for measuring depth level of anaesthesia in patient under surgery [5].

Signals from 10 subjects have been acquired and the data collection involved the following devices:

- Vivosonic Integrity V500, as stimulus generator (Figure 2a);
- ER-3A-ABR, as headphones for presenting the stimulus to the subjects (Figure 2b);
- NicoletTM Wireless 32 EEG amplifier, for recording the brainwaves from 7 active channels (Figure 2c and d).

A pre-processing step is first applied to the raw signal (an example is shown in Figure 3), by filtering out the unwanted bands; the following steps are executed:

1. bandpass filtering [100-3000] Hz;
2. zero-phase filtering;
3. baseline removal;

After this, all the spikes are clipped from the signals and the signals from the 7 active electrodes are synchronized with the recorded stimulus. The time indices of the clicks are then detected and used for segmenting the signal in epochs: the time duration between two clicks is denoted as the epoch and it’s approximately 36.3 ms (436 samples). In order to improve the SNR of the transient AEP, an average between the epochs is performed.
The feature extraction and classification phases have been performed by training a 1D-CNN, whose architecture is the following:

- A 1D-Convolutional Layer, whose input is a matrix, where is the number of AEP observations, denotes the dimension of the signal and denotes the number of channels. The output of the layer is
- A ReLU layer;
- A Max Pooling Layer;
- A LR Layer, which uses a softmax function in multi-class classification mode and a sigmoid function in verification mode.

The obtained results show a Correct Recognition Rate (CRR) of 97.05% and 95.15% for the left and right ear respectively, and up to 99% by fusing the signals from both ear.

Despite the promising results, this topic seems still opened to further researches. Also the applicability to telemedicine applications or in chemical and nuclear facilities, make this topic worthy of further analysis: first of all, by analysing its behaviour if a wider database is used; then, by studying the effects of more sophisticated techniques for the signals’ pre-processing and feature extraction.

References


CALL FOR PAPERS

ICB 2019 : International Conference on Biometrics

Link: http://www.icb2019.org/

When  Jun 4, 2019 - Jun 7, 2019
Where  Crete, GREECE
Submission Deadline  Dec 15, 2018
Notification Due  Feb 28, 2019
Final Version Due  Mar 20, 2019
Categories  biometrics, sensor design

Call For Papers
- Face, Iris, Fingerprint and Ear
- Periocular
- Palm prints
- Multi-Modal and Multi-Spectral Biometrics
- Mobile-based biometrics
- Template protection
- Gait and gesture
- Soft biometrics (including marks, scars and tattoos)
- Template design, selection and update
- Finance-related applications
- Database, protocol and benchmarking
- Large scale ID
- Anti-spoofing
- Law enforcement and forensic applications
- Security applications
- Biometrics in healthcare and societal applications
- Performance modeling and prediction
- Ethical, social and legal issues

Future Generation Computer Systems
The International Journal of eScience
Editor-in-Chief: Peter Sloot

Special Issue on CyberSecurity & Biometrics for a better Cyberworld

Cybersecurity is an essential requirement when living in a digital world. Should one user trust a service on internet? How well secured are my personal data in the digital world? All these questions request new technical and methodological solutions involving many aspects among cryptography, information theory, protocols...

In order to establish a secure link between users and cyber services, biometrics becomes a key technology. However, it has also many drawbacks such as possible false rejection of legitimate users and false acceptance of impostors, privacy concerns and possible attacks (spoofing, replay). In this special issue, we expect high-level research contributions in this area in order to propose useful solutions to secure our Cyberworld.
Call for Papers

The topics include but are not limited the following research areas:

- Security protocols
- Authentication protocols
- Privacy protocols
- Password security
- Security of personal data
- Content protection and digital rights management
- Risk and reputation management
- Identity and trust management
- Information hiding and anonymity
- Privacy, security and trust in social media
- Security of embedded systems
- Behavioral biometrics
- Performance evaluation of biometric systems
- Multi-biometrics
- Quality of biometric data
- Biometric template protection
- Presentation attack detection
- Emerging biometrics

Guest Editor

Prof Christophe ROSENBERGER
ENSECAEN
Christophe.rosenberger@ensicaen.fr

Submission Guideline

All manuscripts and any supplementary material should be submitted through Elsevier Editorial System (EVISE). The authors must select "VSII:Security& Biometrics" when they reach the "Article Type" step in the submission process. The EES website is located at: https://www.evise.com/profile/#/FGCS/login

Submission due date: Nov 30, 2018

Call for Papers: Pattern Recognition
Special Issue on Domain Adaptation for Visual Understanding - Special Issue in Pattern Recognition
Guest Editors: Richa Singh, Mayank Vatsa, Vishal M. Patel, Nalini Ratha
Due Date: Oct 31, 2018

Visual understanding is a fundamental cognitive ability in humans which is essential for identifying objects/people and interacting in social space. This cognitive skill makes interaction with the environment extremely effortless and provides an evolutionary advantage to humans as a species. In our daily routines, we, humans, not only learn and apply knowledge for visual recognition, we also have intrinsic abilities of transferring knowledge between related visual tasks, i.e., if the new visual task is closely related to the previous learning, we can quickly transfer this knowledge to perform the new visual task. In developing machine learning based automated visual recognition algorithms, it is desired to utilize these capabilities to make the algorithms adaptable. Generally traditional algorithms, given some prior knowledge in a related visual recognition task, do not adapt to a new task and have to learn the new task from the beginning. These algorithms do not consider that the two visual tasks may be related and the knowledge gained in one may be used to learn the new task efficiently in lesser time. Domain adaptation for visual understanding is the area of research, which attempts to mimic this human behavior by transferring the knowledge learned in one or more source domains and use it for learning the related visual processing task in target domain. Recent advances in domain adaptation, particularly in co-training, transfer learning, and online learning have benefited the computer vision research significantly. For example, learning from high-resolution source domain image
and transferring the knowledge to learning low-resolution target domain information has helped in building improved cross-resolution face recognition algorithms. This special issue will focus on the recent advances on domain adaptation for visual recognition.

**Complete call for papers:**
[https://www.journals.elsevier.com/pattern-recognition/call-for-papers/domain-adaptation-for-visual-understanding](https://www.journals.elsevier.com/pattern-recognition/call-for-papers/domain-adaptation-for-visual-understanding)

**Call for Papers, Workshop, Tutorials, Demonstrations:** 2019 IEEE Conference on Automatic Face and Gesture Recognition

The 14th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2019) will be held in Lille, France, 14 -18 May 2019. The IEEE conference series on Automatic Face and Gesture Recognition is the premier international forum for research in image and video-based face, gesture, and body movement recognition. Its broad scope includes: advances in fundamental computer vision, pattern recognition and computer graphics; machine learning techniques relevant to face, gesture, and body motion; new algorithms and applications.

**Details are available at:** [http://fg2019.org/about/](http://fg2019.org/about/)