# 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,
({marta.gomez-barrero,christian.rathgeb,christoph.busch}@h-da.de)
†European Commission - DG-Joint Research Centre, E.3, 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 [4].

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 [3]. However, little attention has been paid to the objective evaluation of the template' 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 linkability 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 linkability 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 linkability based on score distributions obtained from the linkage function, independently of what the linkage 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 linkability 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 linkability**: 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 $\mathrm{D}_{\leftrightarrow}(s)$: System Score-Wise Linkability

$\mathrm{D}_{\leftrightarrow}(s) \in [0,1]$ evaluates the linkability of a system for each *specific linkage score* $s = LS(\mathbf{T}_1, \mathbf{T}_2)$. 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 $\mathrm{D}_{\leftrightarrow}(s_1) = 1$, it means that, *in case* the linkage function produced $s_1$, we would be able to link both templates $\mathbf{T}_1$ and $\mathbf{T}_2$ to the same instance with almost all certainty. On the other hand, $\mathrm{D}_{\leftrightarrow}(s_0) = 0$ should be interpreted as full unlinkability for that particular score $s_0$. 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 $\mathrm{D}_{\leftrightarrow}(s)$ between 0 and 1 report an increasing degree of linkability.

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,

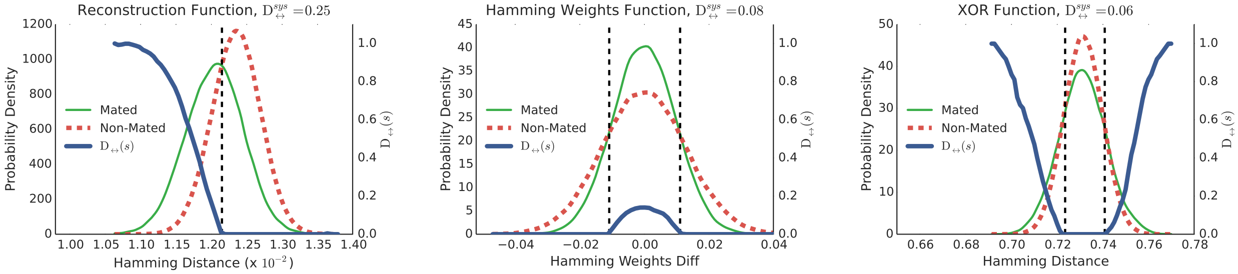

Fig. 1: Unlinkability analysis of a facial BTP scheme under three linkage functions.

such linkability can be accounted for in terms of the following difference of conditional probabilities:

$$\mathrm{D}_{\leftrightarrow}(s) = p(H_m|s) - p(H_{nm}|s)$$

However, these two conditional probabilities are unknown. Hence, we start the computation from the likelihood ratio $LR(s) = p(s|H_m)/p(s|H_{nm})$ 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 $\mathrm{D}_{\leftrightarrow}(s)$ as a two-part function of $s$ as follows:

$$\mathrm{D}_{\leftrightarrow}(s) = \begin{cases} 0 & \text{if } LR(s)\cdot\omega \leq 1 \\ 2\frac{LR(s)\cdot\omega}{1+LR(s)\cdot\omega} - 1 & \text{if } LR(s)\cdot\omega > 1 \end{cases}$$

where $\mathrm{D}_{\leftrightarrow}(s) = 0$ 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 $\mathrm{D}_{\leftrightarrow}^{sys}$: 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 $\mathrm{D}_{\leftrightarrow}^{sys} \in [0,1]$, which gives an estimation of the global linkability of a system, *independently* of the score. This way, if a system has $\mathrm{D}_{\leftrightarrow}^{sys} = 1$ (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, $\mathrm{D}_{\leftrightarrow}^{sys} = 0$ 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 $\mathrm{D}_{\leftrightarrow}^{sys}$ between 0 and 1 report an increasing degree of linkability.

Therefore, we are interested on 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 $\mathrm{D}_{\leftrightarrow}^{sys}$ as

$$\begin{aligned}\mathrm{D}_{\leftrightarrow}^{sys} &= \int_{\substack{p(H_m|s) > \\ p(H_{nm}|s)}} p(s|H_m)\cdot\left(p(H_m|s) - p(H_{nm}|s)\right)\mathrm{d}s \\ &= \int p(s|H_m)\cdot\mathrm{D}_{\leftrightarrow}(s)\,\mathrm{d}s\end{aligned}$$

This way, the final value of $\mathrm{D}_{\leftrightarrow}^{sys}$ 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 $K$ databases 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 $\mathrm{D}_{\leftrightarrow}(s)$ and $\mathrm{D}_{\leftrightarrow}^{sys}$.
5) Report $\mathrm{D}_{\leftrightarrow}(s)$ plots, together with the *Mated samples* and *Non-Mated samples* distributions, and the corresponding global linkability values $\mathrm{D}_{\leftrightarrow}^{sys}$ (see an example in Fig. 1).
6) Analyse the plots and $\mathrm{D}_{\leftrightarrow}^{sys}$ values

## III. Conclusions

We have proposed two new quantitative measures ($D_{\leftrightarrow}(s)$ and $D_{\leftrightarrow}^{sys}$) 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

[1] European Council, "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," 04 2016.

[2] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*, ISO, 2011.

[3] S. Rane, "Standardization of biometric template protection," *IEEE Multimedia*, vol. 21, no. 4, pp. 94–99, 2014.

[4] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, 2011.

[5] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proc. IEEE Signal Processing*, 2009, pp. 188–203.

[6] I. Buhan, J. Breebaart, J. Guajardo *et al.*, "A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem," in *Proc. Int. Conf. on Data Privacy Management and Autonomous Spontaneous Security, DPM/SETOP*, 2009, pp. 78–92.

[7] I. Buhan, J. Merchan, and E. Kelkboom, "Efficient strategies for playing the indistinguishability game for fuzzy sketches," in *Proc. Int. Workshop on Information Forensics and Security, WIFS*, 2010.

[8] A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," in *Proc. Electronic Imaging*, 2008, pp. 68 190O–68 190O.

[9] E. J. Kelkboom, J. Breebaart, T. A. Kevenaar, I. Buhan, and R. N. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 1, pp. 107–121, 2011.

[10] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in *Proc. SPIE 7541*. International Society for Optics and Photonics, 2010, p. 75410O.

[11] E. Piciucco, E. Maiorana *et al.*, "Cancelable biometrics for finger vein recognition," in *Proc. SPLINE*. IEEE, 2016, pp. 1–5.

[12] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for MCC fingerprint templates," in *Proc. BIOSIG*, 2014.

[13] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis of bloom filter-based iris biometric template protection," in *Proc. Int. Conf. on Biometrics, ICB*, 2015, pp. 527–534.

[14] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, 2014.

[15] E. A. Rua, E. Maiorana, J. L. A. Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 269–282, 2012.

[16] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC FDIS 30136, Performance Testing of Biometric Template Protection Schemes*, International Organization for Standardization, 2017.