# Achieving Cancellability in End-to-End Deep Biometrics with the Secure Triplet Loss

*João Ribeiro Pinto, Miguel V. Correia, Jaime S. Cardoso*

INESCTEC

VCMI VISUAL COMPUTING & MACHINE INTELLIGENCE RESEARCH GROUP

## HIGHLIGHTS:

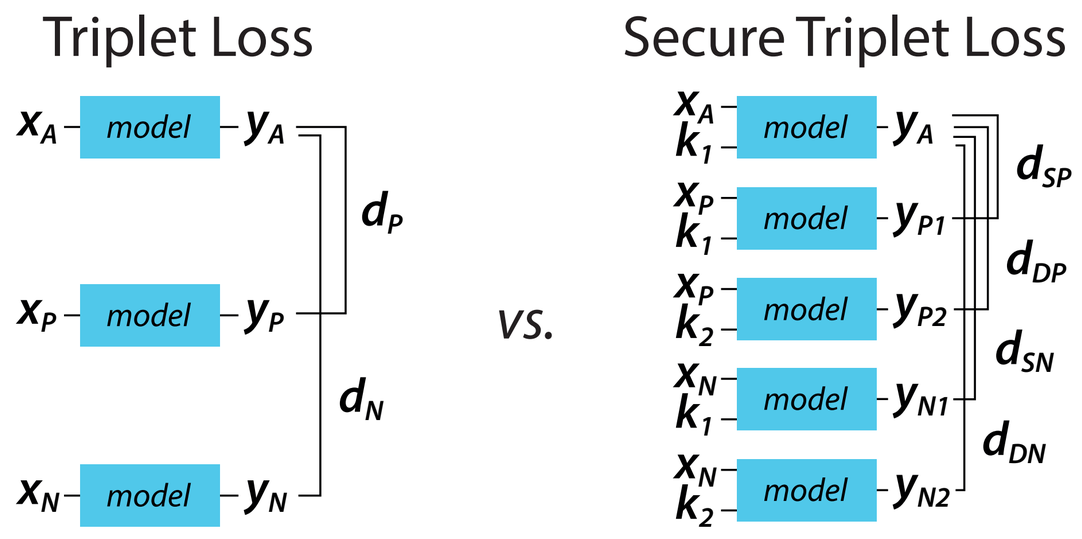
> *First method for cancellability with end-to-end deep models*
> *Based on triplet loss using cancellable keys*
> *Avoids typical encryption and other separate processing*
> *Tested for ECG biometric identity verification*
> *Achieves cancellability and improved performance*

## SUMMARY:

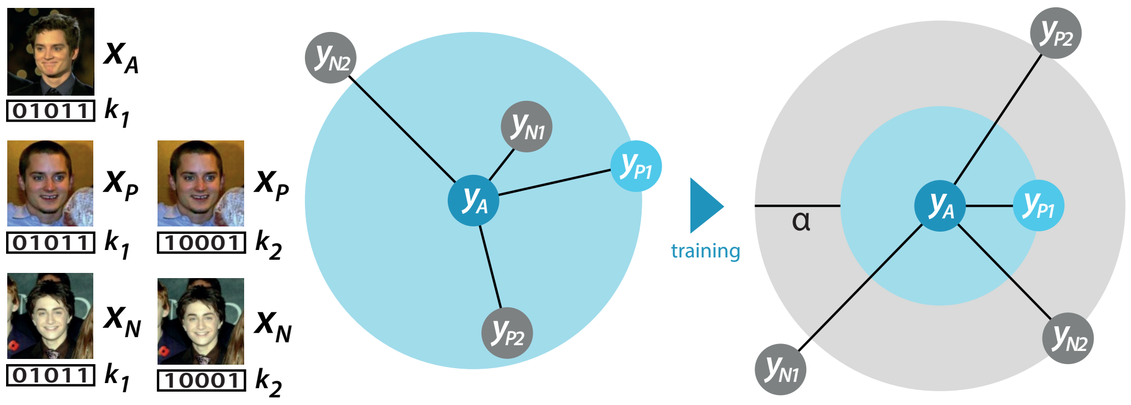
> *Unlike passwords, biometric traits are hard to change*
> *Data in biometric systems needs to be easily cancellable*
> *Typically achieved using bio-hashing or encryption*
> *Template security commonly leads to worse performance*
> *Current methods are inadequate for end-to-end models*

> *We adapt the triplet loss to receive samples and keys*
> *Triplet loss will only cluster samples with same id. and key*
> *Samples bound with cancelled keys are easily invalidated*
> *Cancellability is ensured and performance improves*
> *Template linkability drawback needs to be addressed*

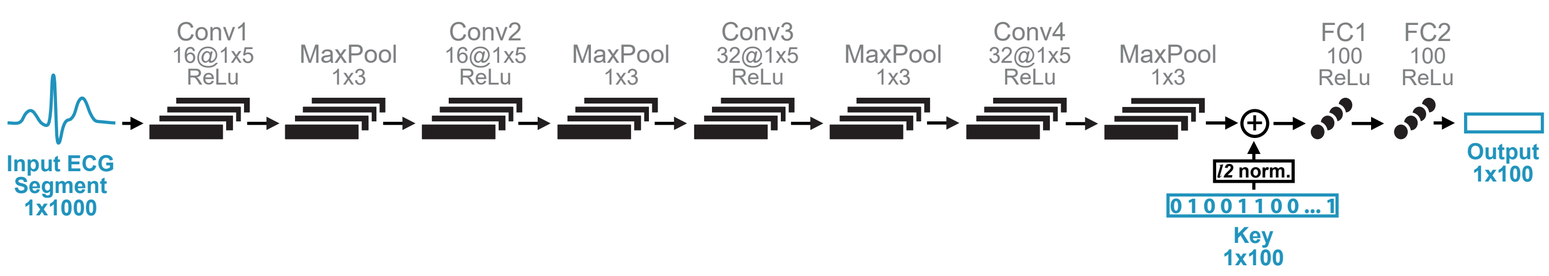
## PROPOSED METHODOLOGY:




## BEHAVIOUR DURING TRAINING:



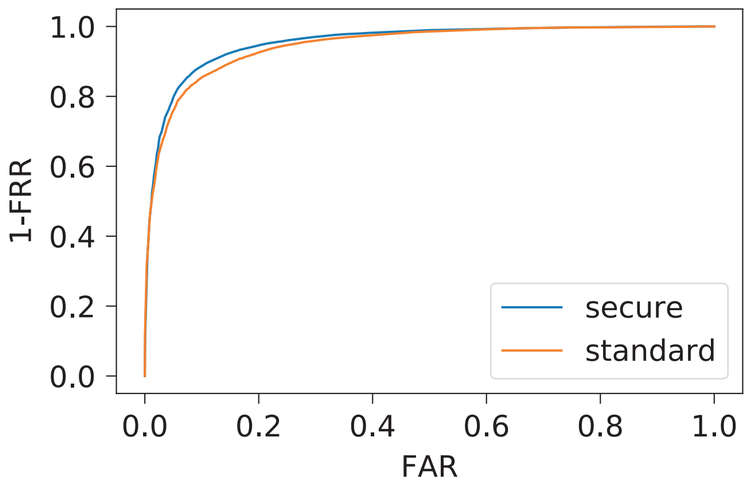

*$x_A$ - anchor; $x_P$ - positive, $x_N$ - negative, $k_m$ - cancellable keys*



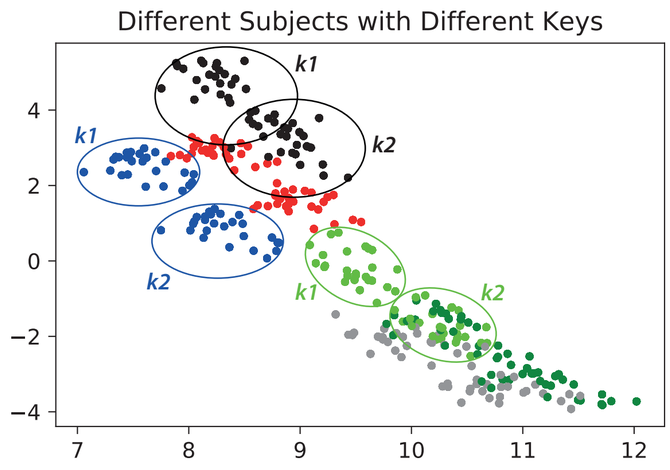

## EXPERIMENTAL SETTINGS:

> *Off-the-person ECG data from the UofTDB*
> *Competitive model for ECG id. verification*
> *Triplets randomly generated according to id.*
> *Random binary array keys, l2-normalised*

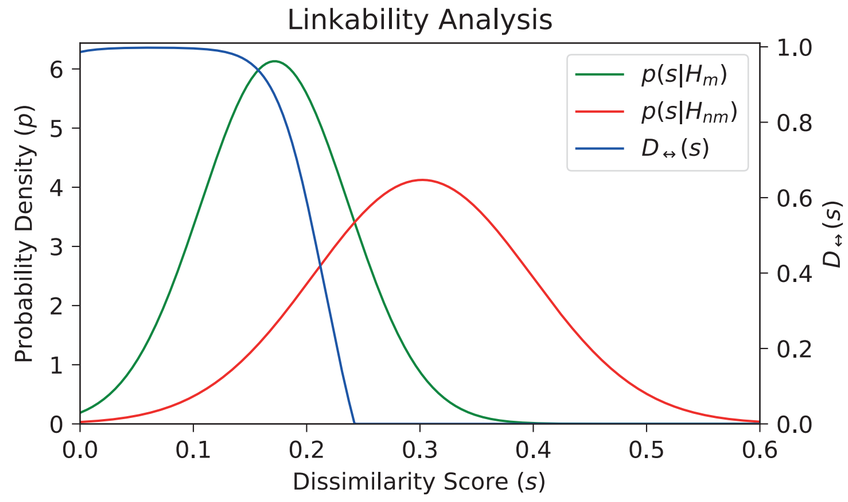
## RESULTS:



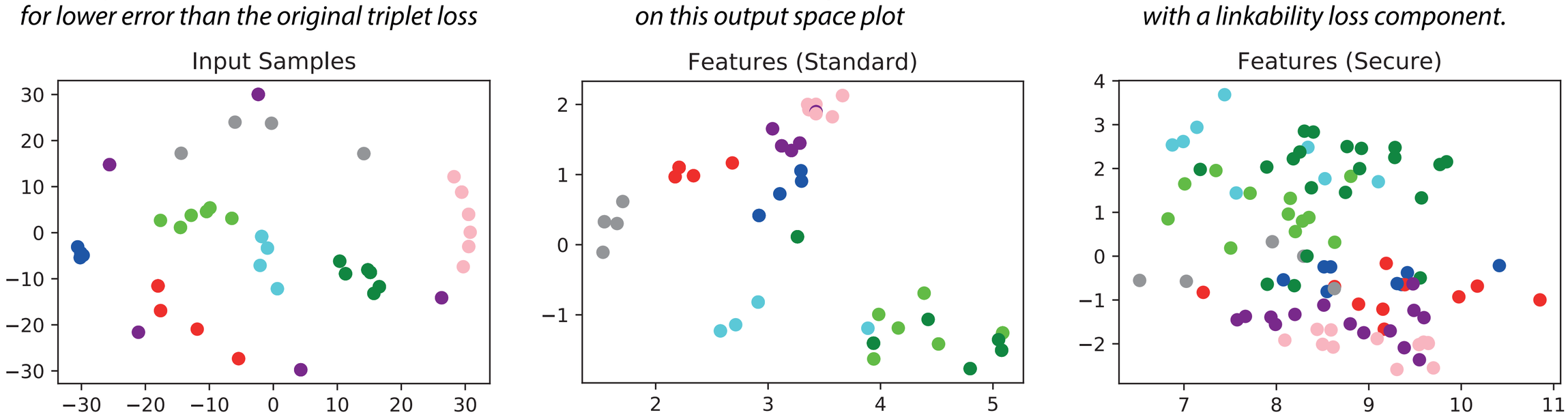

*The proposed cancellability method not only avoided performance decay: it even allowed for lower error than the original triplet loss*




*The effect of changing a key on the templates of a subject is clear on this output space plot*




*However, the method presents high template linkability. This drawback could be addressed with a linkability loss component.*




*Unlike the triplet loss, the secure triplet loss doesn't always bring samples of the same class together - only when the keys match, otherwise the samples will be spread over the output space in order to ensure cancellability*

**need more info?**
**> bit.ly/SecureTL**
**> joao.t.pinto@inesctec.pt**

This work was financed by the ERDF -- European Regional Development Fund through the Operational Programme for Competitiveness and Internationalization - COMPETE 2020 Programme and by National Funds through the Portuguese funding agency, FCT -- Fundação para a Ciência e a Tecnologia within project ``POCI-01-0145-FEDER-030707", and within the PhD grant ``SFRH/BD/137720/2018". The authors wish to acknowledge the creators of the UofTDB database (University of Toronto, Canada).