PERFORMANCE AND SECURITY EVALUATION OF BEHAVIORAL BIOMETRIC SYSTEMS

Ph.D. thesis defense

Yris Brice WANDJI PIUGIE

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE
Fime SAS, 14000 Caen, FRANCE

Supervision:

- Christophe ROSENBERGER
- Christophe CHARRIER
- Joël DI MANNO

GREYC Electronics and Computer Science Laboratory

UNICAEN

ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE

cnrs

fime

anrt ASSOCIATION NATIONALE RECHERCHE TECHNOLOGIE

Introduction

Context

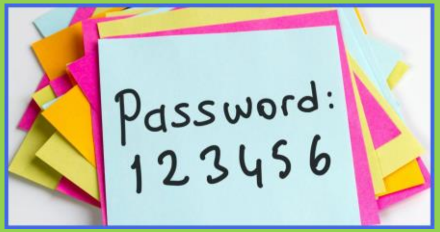
User authentication as cybersecurity countermeasures

In 2021, at least $20 billion was paid out to ransomware hackers

Introduction

User authentication

Something you have…



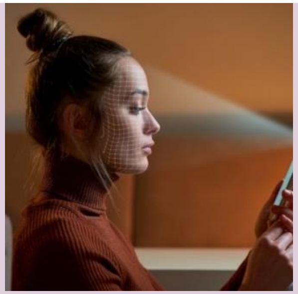
Something you know…

What you are…

Three main solutions for user authentication

Introduction

Physiological


Facial


Iris | retina


Fingerprint


Palm | vein

Behavioral


Voice


Human Activities

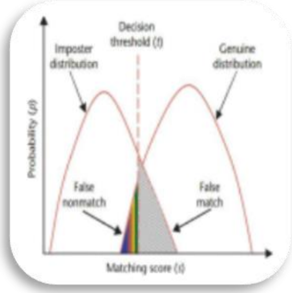

Gesture


Keystroke

Introduction

Biometric certification/evaluation

- Why do we need certification?
  - Security
  - User experience



Performance measurement

Evaluation methodology

- Technology evaluation
- Scenario-based evaluation
- Operational evaluation

Presentation Attack Detection evaluation

Introduction

Major certification actors

Standards

- ISO 39794-17
- ISO 19795
- ISO 30107

Authority

Develop interoperable authentication standards based on public key cryptography to solve the **password problem**

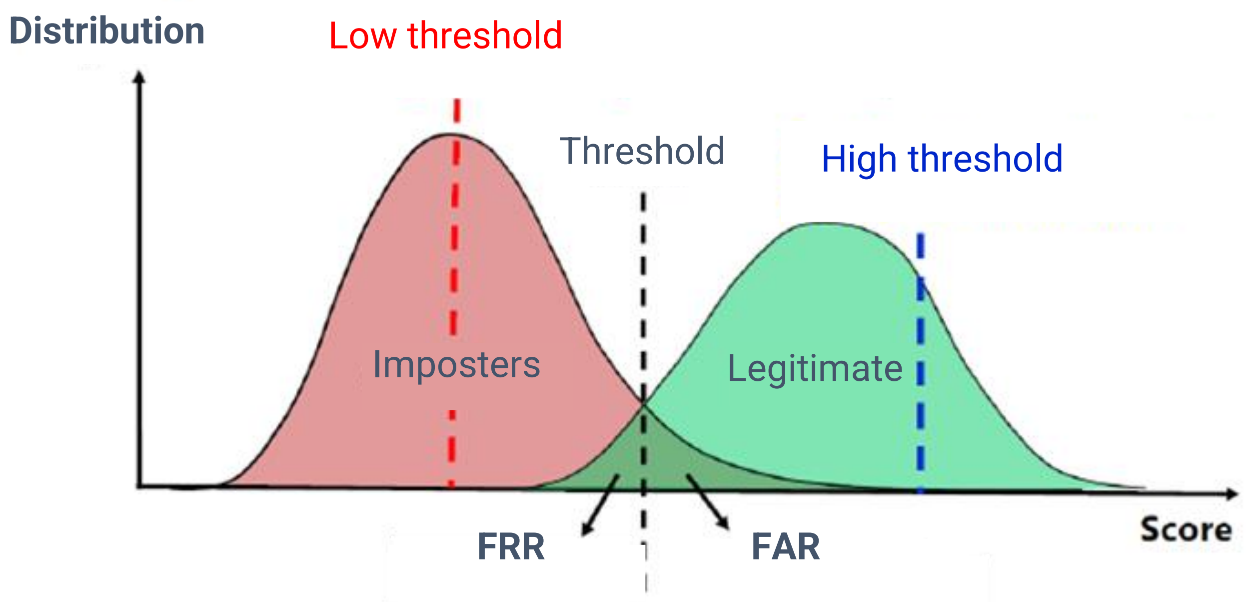
Laboratory

Testing lab

Metrics used

Biometric data : simulating impostor and legimate attempts

- **FAR** (False Acceptance Rate): percentage of impostors wrongly match by the system.
- **FRR** (False Rejection Rate): percentage of users wrongly rejected.
- **EER** (Equal Error Rate): error rate corresponding to a setting of the biometric system's **decision threshold** so that the **FAR** value is equal to **FRR**.



Introduction

Performance measurements (example)

FIDO 3.0 requirements by levels

	BioLevel 1	BioLevel 1+	BioLevel 2	BioLevel 2+
Number of test subjects	25	245	25	245
FAR	1%	1:10k	1%	1:10k
FRR	7%	5%	7%	5%

Note:

- Requirements on FAR and FRR are given at 80% confidence
- For BioLevel 1 and BioLevel 2, Documented self attestation FAR and FRR are mandatory respectively at 1:10k and 5%

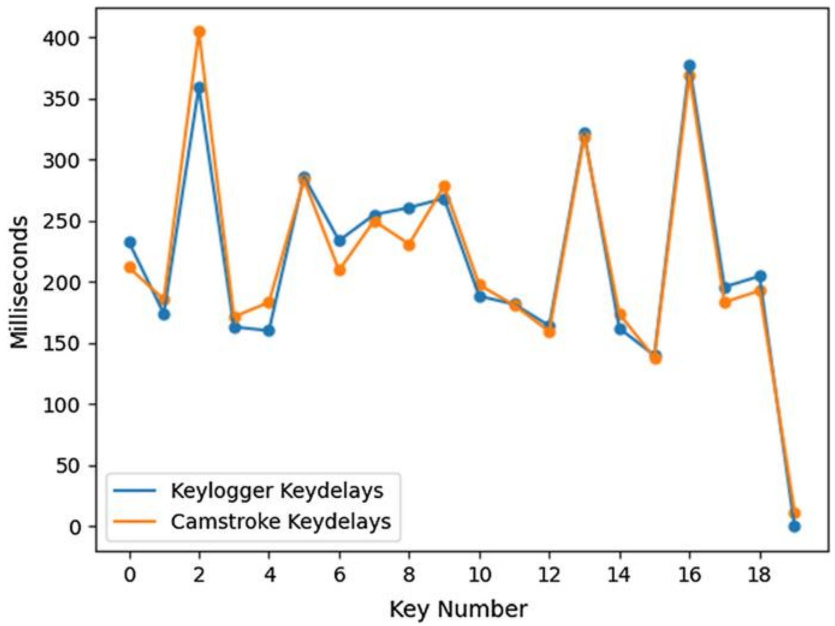
Schuckers, S., Cannon, G., Tekampe, N., Tabassi, E., Karlsson, M., and Newton, E. (2023). Fido biometrics requirements. Population, 5(2-1):2–3

Introduction

Presentation attack detection (PAD)

- The aim of **PAD test**
  Evaluate the reaction of a biometric security product to various **PAI (Presentation Attack Instrument)** known as **spoofs**.

- Examples of **PAI** in behavioral, **simulating dynamic typing** through **keystroke imitation**



Siahaan, Chrisando Ryan Pardomuan, and Andry Chowanda. "Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen-recorded video." *Journal of Big Data* 9.1 (2022): 1-29.

Introduction

Ph.D. objective

Contribute to the certification of behavioral biometric systems:

- by assessing performance
- by assessing presentation attacks

Specific objectives

1. **Proposing a generic method for analyzing behavioral biometrics**
2. **Generating synthetic behavioral presentation attack datasets**

Contents

Contents

Generic system – Introduction

Motivation

- **Objective**
  Proposed a baseline system to evaluate behavioral biometrics

- **Validation**

Keystroke dynamics

Human activity

Generic system – Related works

Keystroke dynamics based user authentication

Overview of keystroke dynamics for user authentication-related work using neural networks.

Study	Features	Classification	Testing type	Env.	#Users	Samples	EER
Andrean *et al.* [20]	Latency, Trigraph/N-graph	MLP	Static, Dynamic	controlled	51	400	16.14%
Lu *et al.* [21]	Latency, Trigraph/N-graph	CNN+RNN	-	controlled	260	-	05.97%
Çeker *et al.* [22]	-	CNN	Static, Dynamic	controlled	133	-	06.50%
Alpar [23]	Trigraph/N-graph	Gauss-newton based neural network	-	-	13	780	05.10%
Roth *et al.* [24]	Digraph/N-graph	Digraph Static	Static, Dynamic	controlled	50	-	11.00%
Harun *et al.* [25]	Latency	NN, dist. classifier	Static	Controlled	15	150	22.90%
Revett *et al.* [26]	Latency, Trigraph/N-graph	Specht Probabilistic NN	Static	Controlled	50	10000	05.70%

Generic system – Related works

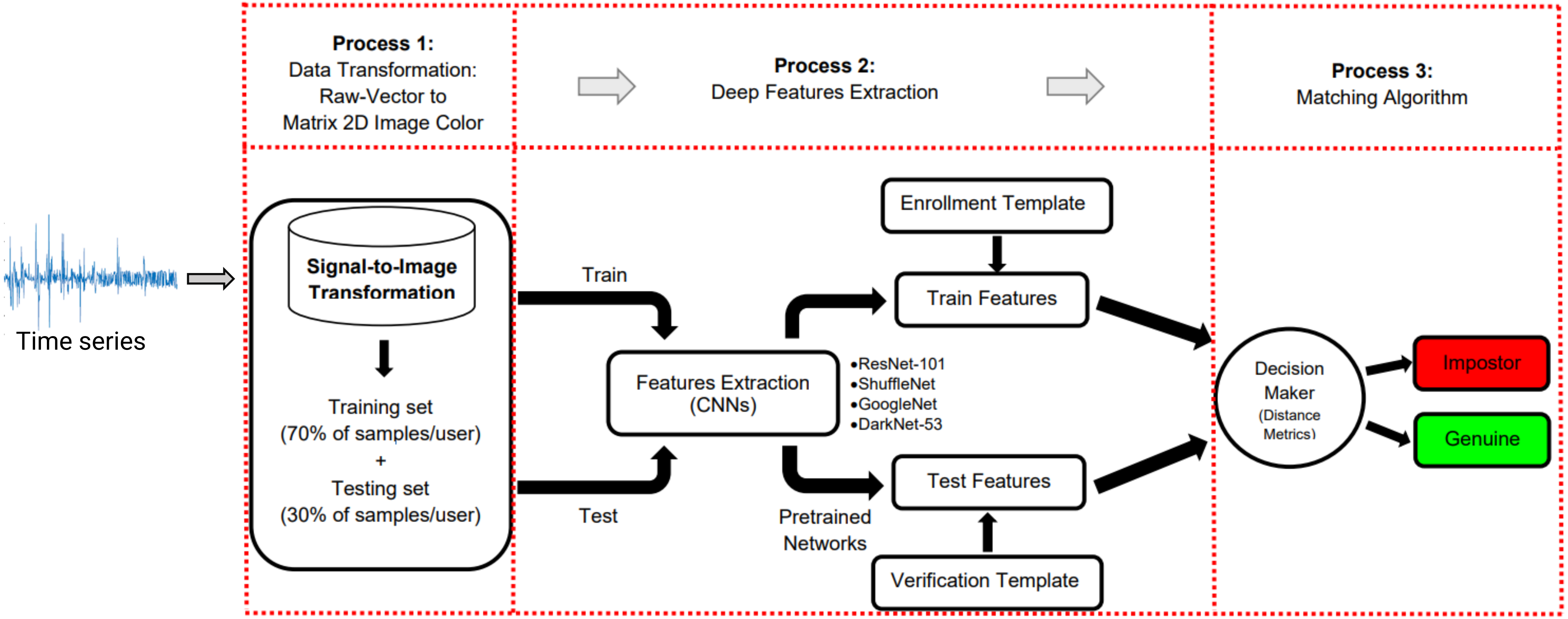
Human activities authentication

Overview of user activity authentication in the state of the art.

Paper	Approach	Method	Activity	Input Source	Accuracy	EER
(Marsico and Mecca, 2017)	Action recognition	DTW	Gait	Smartphone	[83.00% – 93.00%]	[0.09% – 0.10%]
(Patel et al., 2016)	Continuous user authentication	Ten different classifier	Walking, sitting	Mobile devices	-	07.50%
(Zhang, 2019)	Learning human identity from motion patterns	Dense Clockwork RNN	Walking	Smartphone	93.02%	18.17%
(Mantyjarvi et al., 2005)	Identifying users from gait pattern	Correlation coefficients	walking	Smartphone	[72% – 88%]	7%
(Muaaz and Mayrhofer, 2013)	Gait recognition, analysis of approaches	SVM	Walking	Cell phone	-	33.30%
(Zhong et al., 2015)	Pace independent mobile gait biometrics	Nearest neighbor	Walking	Mobile	-	7.22%
(Zareen and Jabin, 2016)	User verification	HMM	25 users, 500 signatures	Samsung Galaxy Note	-	06.20%
(Gafurov et al., 2006)	User verification	Histogram similarity and Cycle length	Gait	Mobile devices	-	[05.00% – 09.00%]
(Parkinson et al., 2021)	User verification	Manhattan distance	Hand movement	Keyboard	[89.00% – 94.00%]	[06.00% – 11.00%]

Generic system – Proposed method

Design of the generic behavioral biometric systems



Architecture of our proposed keystroke dynamics based authentication system

Generic system – Process 1

Data transformation

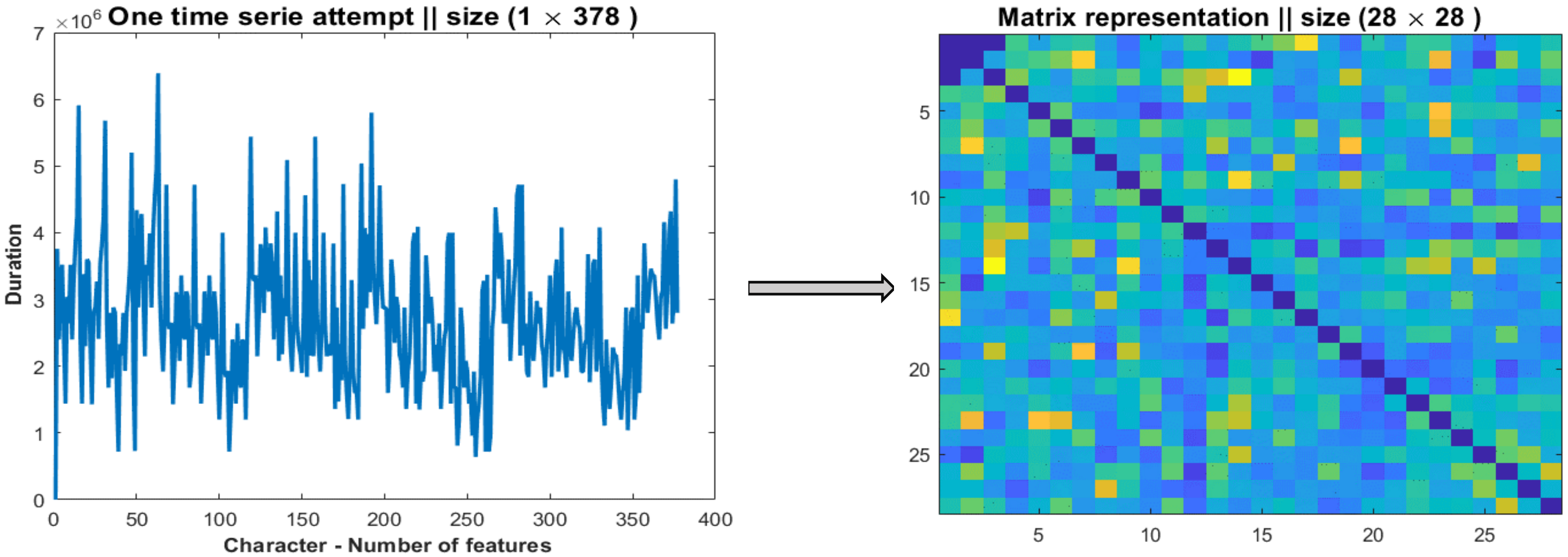
- The time series v composed of 378 values is represented by a matrix **M** of size 28x28.

$$m = \frac{n(n-1)}{2}$$

where
m : the length of features
n : the size of the matrix

$$\mathbf{M}(i,j) = v\left[\binom{n}{2} - \binom{n-i}{2} + (j-i-1)\right]$$

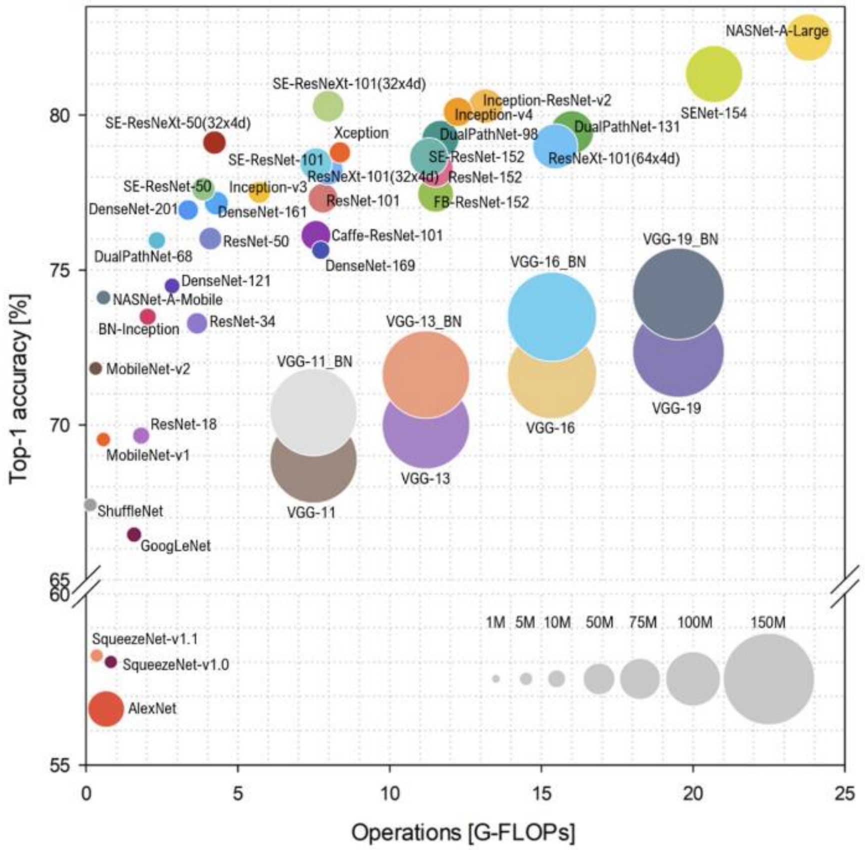
- It represents the number of distinct pairs that can be formed from n elements.



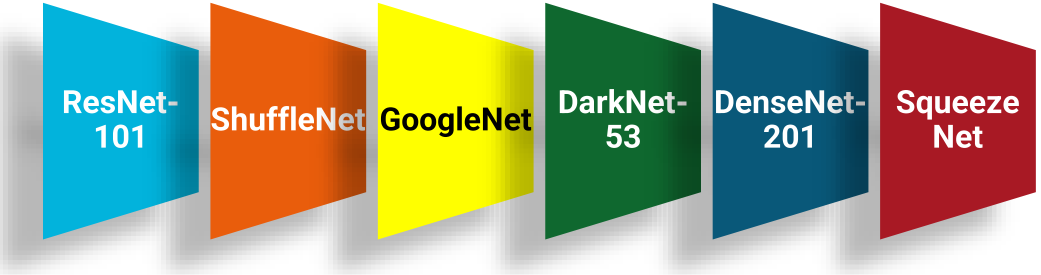
378 values represented by a matrix of size 28x28.

Generic system – Process 2

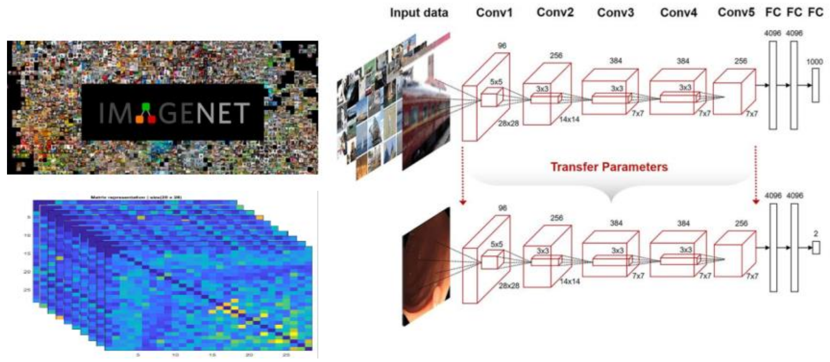
Deep features extractions



Deep learning architectures



TRANSFER LEARNING



Generic system – Process 3

Matching algorithm : distance metrics between reference (xs) vs sample (xt)

Minkowski distance

$$d = \sum_{j=1}^{n} |x_{sj} - x'_{tj}|$$

Euclidean distance

$$d^2 = (x_s - x_t)(x_s - x_t)'$$

Cosine distance

$$d = 1 - \frac{x_s x'_t}{\sqrt{(x_s x'_s)(x_t x'_t)}}$$

Generic system – Protocol

Keystroke dynamics – GREYC-NISLAB database

GREYC keystroke software

Passphrases

Password	Description	Size	Features
P1	leonardo dicaprio	17-char	64
P2	the rolling stones	18-char	68
P3	michael schumacher	18-char	68
P4	red hot chilli peppers	22-char	84
P5	united states of america	24-char	92
P_T	fusion of features (P1+P2+P3+P4+P5)	99-char	376

2200 samples/time series (20 attempts per user)

User	70 (France); 40 (Norway)
Gender	78 males (47 from France, 31 from Norway); 32 females (23 from France, 9 from Norway)
Age Category (between 15 and 65 years old)	$<$ 30 years old (37 men, 14 women); $\geq$ 30 years old (41 men, 18 women)
Handedness	98 right-handed (70 men, 28 women); 12 left-handed (8 men, 4 women)

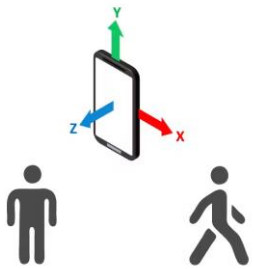
Syed Idrus, S. Z., Cherrier, E., Rosenberger, C., and Bours, P. (2013). Soft biometrics database: A benchmark for keystroke dynamics biometric sys- tems. In 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG), pages 1–8.

Generic system – Protocol

Human activities – database

30 users wearing a **Samsung Galaxy S II** on waist using embedded:

- **Accelerometer**
- **Gyroscope**



Data captured on:

- **3-axial angular velocity**
- **3-axial linear acceleration**

Activities, including 10,299 samples for each activity along with their respective descriptions in the UCI-HAR database.

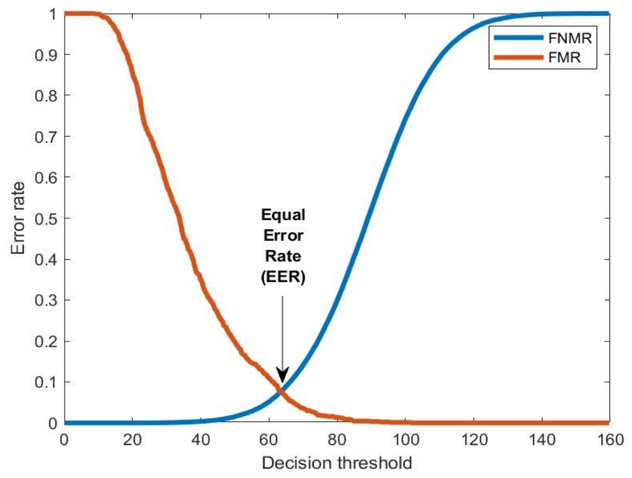
Activity	Abbreviation	No. of Samples	Each Human Activity ratio	Description
Laying	lyx	1722	16.72%	Subject sleeps or lies down on a bed
Sitting	six	1544	14.99%	Subject sits on a chair either working or resting
Standing	stx	1406	13.65%	Subject stands and talks to someone
Walking	wlx	1777	17.25%	Subject goes down multiple flights
Walking Downstair	wdn	1906	18.51%	Subject goes down multiple flights
Walking Upstairs	wup	1944	18.88%	Subject goes up multiple flights

Anguita, D., Ghio, A., Oneto, L., Parra, X., and Reyes-Ortiz, J. L. (2013). A public domain dataset for human activity recognition using smartphones. In Esann, volume 3, page 3.

Generic system – Protocol

Preprocessing

- **Enrollment template**: **70%** of the sample attempts per user in the dataset (training set).
- **Verification samples: 30%** of the samples attempts per user in the dataset (testing set).
- Relationship between FMR, FNMR and **EER**

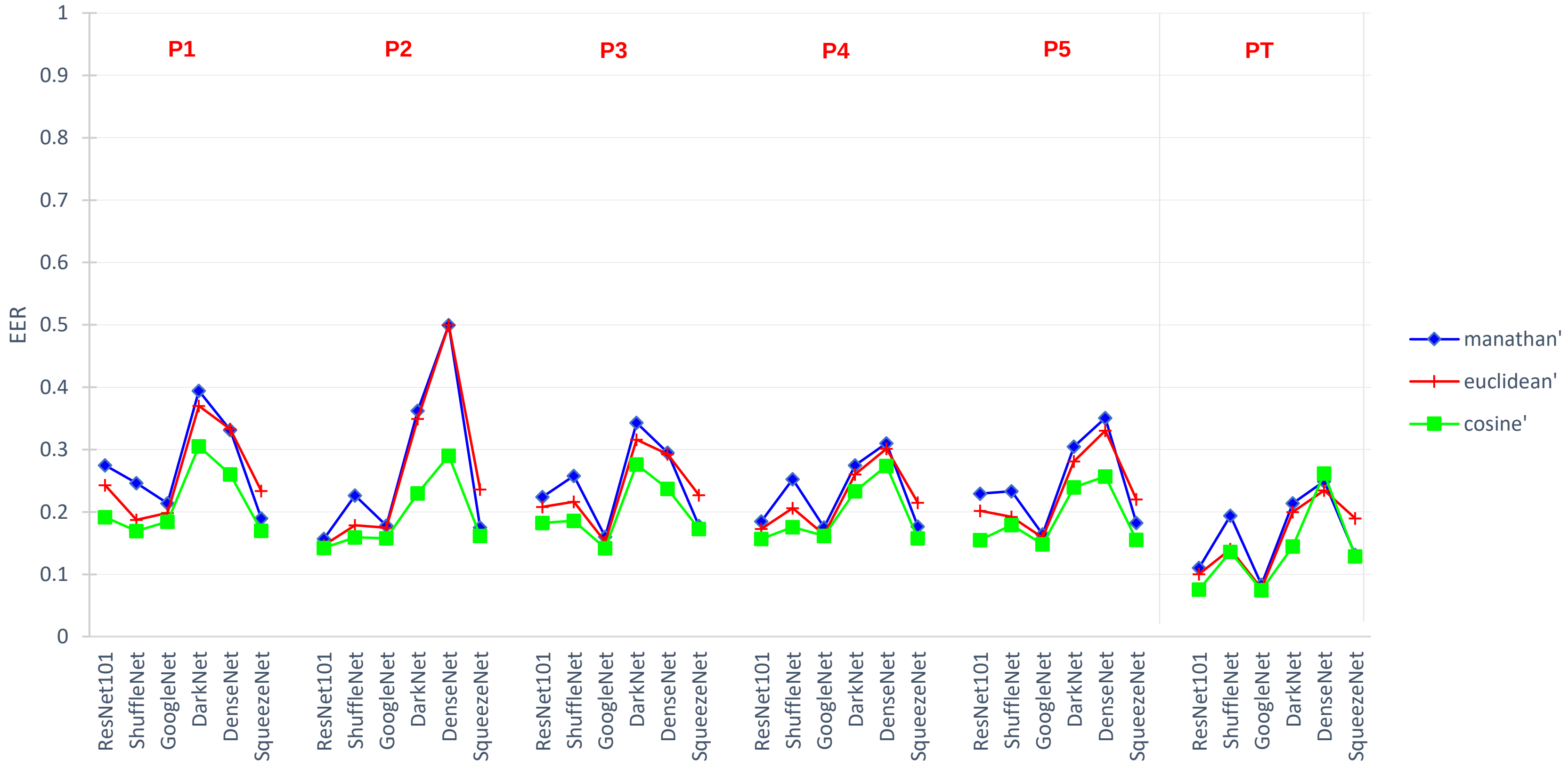


- Architectures and **optimizations hyper-parameters** for the deep learning approaches

Models	#Layers	#Depth	Image Input Size	Activate	Normalize	Algorithm	Loss	#Epochs	#Batch	#Learning rate
ResNet-101	347	101	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
ShuffleNet	172	50	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
GoogleNet	144	22	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
DarkNet-53	184	53	256-by-256	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
DenseNet-201	708	201	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
SqueezeNet	68	18	227-by-227	ReLU	Batch	SGDM	cross-entropy	500	10	0.001

Generic system – Performance evaluation on each sub-dataset

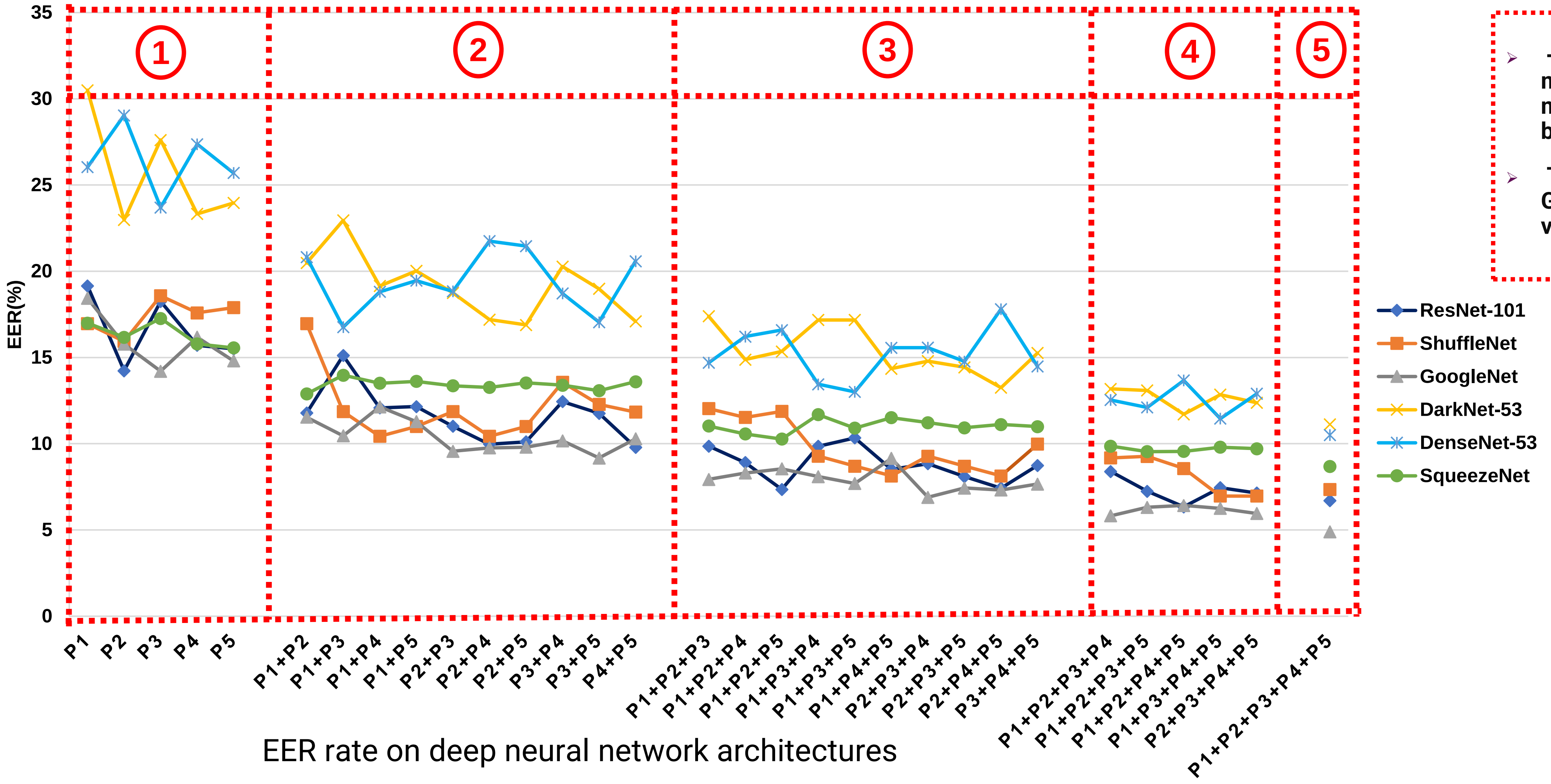
5 types passphrase correspond to PT



EER (x100) rate on deep architectures for P1, P2, P3, P4, P5 and PT sub-databases

- P_T : The more we have information about the user, the better are the results (04.89%).
- ResNet and GoogleNet offer best result
- Used of the Cosine distance metric for the rest of performance evaluation

Generic system – What is the performance when the user enters multiple passphrases?



EER rate on deep neural network architectures

- + 5 passphrases => the more efficient the matching systems becomes
- The best model is GoogleNet with an EER values of 04.89%

Generic system – Fusion of features vs fusion of scores

Keystroke dynamics in a context of multi-instances

Fusion of deep features versus **Fusion of scores levels.**

Models (EER_{cosine})	**Fusion of features**	**Fusion of scores**
ResNet-101	07.55%	06.70%
ShuffleNet	13.59%	07.34%
GoogleNet	**07.45%**	**04.89%**
DarkNet-53	14.96%	11.11%
DenseNet-201	26.18%	10.50%
SqueezeNet	12.87%	08.68%

Generic system – Comparison with recent works

Reported work on keystroke dynamics

Comparison with other published works in keystroke dynamics.

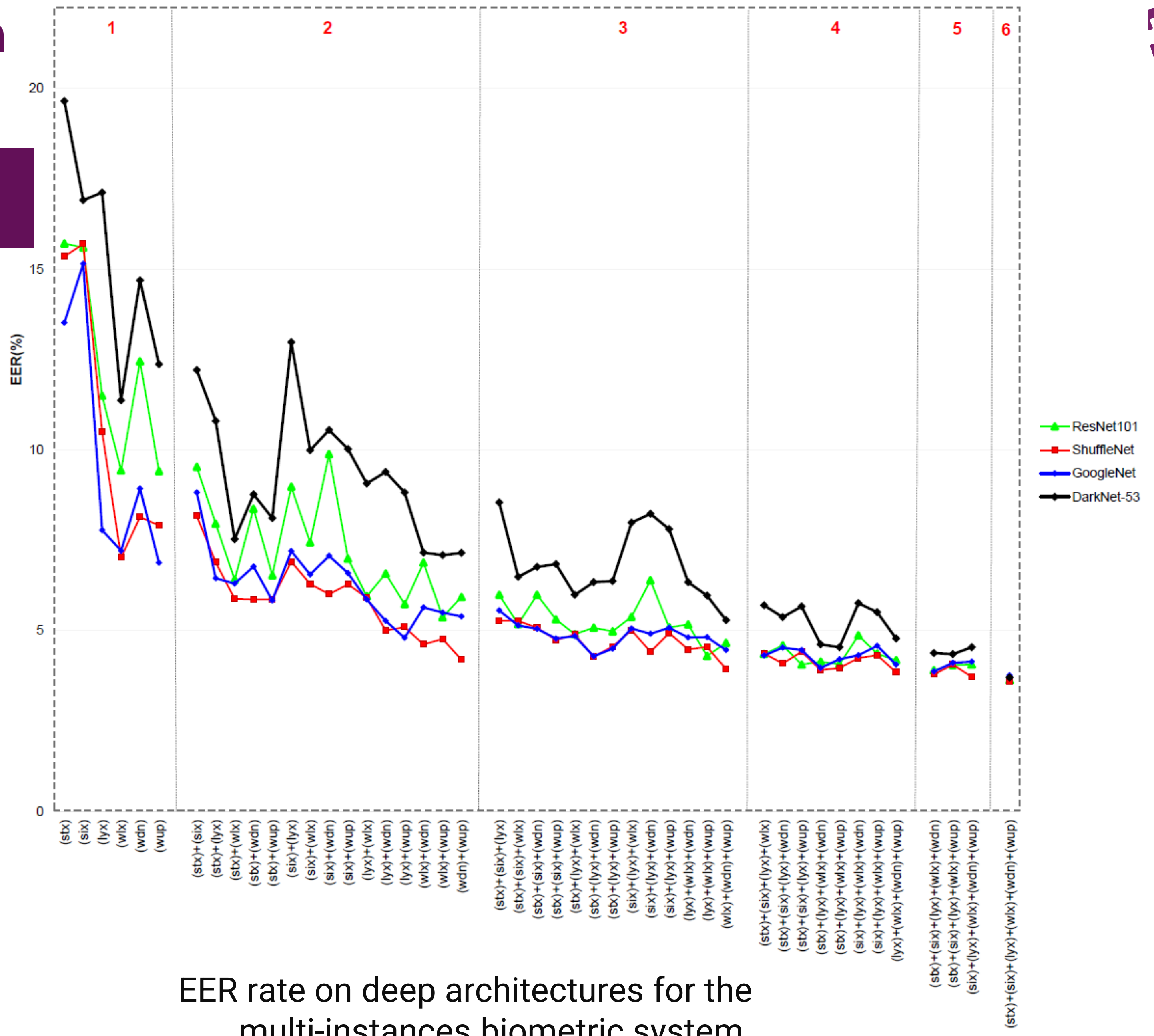
Database	Author/S (ref)	Years	Classifiers	EER
GREYC-NISLAB	**This work**	**2021**	**GoogleNet**	**4.89%**
GREYC-NISLAB	Idrus *et al.* [Idrus et al., 2015]	2015	SVM	[08.45% – 10.63%]
Clarkson II	Li *et al.* [Li et al., 2021]	2021	CNN & CNN-GRU	[07.55% – 07.74%]
Synthetic	Ayotte *et al.* [Ayotte et al., 2021a]	2021	SVM & MLP	[04.90% – 05.46%]
GREYC 2009 vs WEB GREYC	Mhenni *et al.* .[Mhenni et al., 2018]	2018	kNN	[06.61% – 07.08%]
GREYC Keystroke	Zhong *et al.* [Zhong and Deng, 2015]	2015	SVM	[08.45% – 10.65%]

- Good results compared with the state of the art in terms of **EER score**.

Generic system – Human activity authentication

GREYC
Electronics and Computer Science Laboratory

Fusion of score



EER rate on deep architectures for the multi-instances biometric system.

- \+ activities => the more efficient the matching system becomes
- The best model is ShuffleNet with an EER value of 3.58%

fime

Generic system – Fusion of features vs fusion of scores

User authentication based human activity

Fusion of deep features versus **Fusion of scores level** on UCI-HAR dataset

Models (EER_{cosine})	Fusion of features	Fusion of scores
ResNet-101	12.48%	3.63%
ShuffleNet	**11.57%**	**3.58%**
GoogleNet	13.52%	3.76%
DarkNet-53	11.72%	3.70%

Generic system – Comparison with recent works

Comparison with other published works (target = user)

Dataset	Author/S (ref)	Years	Classifiers	EER
UCI-HAR (target = users)	**[Wandji Piugie et al., 2023]**	**2023**	**ShuffleNet**	**03.57%**
UCI-HAR (target = users)	Mekruksavanich *et al.* [Mekruksavanich and Jitpattanakul, 2021]	2021	DeepConvLSTM	5.10%
Touch gestures data	Patel *et al.* [Patel et al., 2016]	2016	Ten classifiers	07.50%
WISDM	Zhang *et al.* [Zhang, 2019]	2019	Dense Clockwork RNN	18.17%
Gait signal data	Mantyjarvi *et al.* [Mantyjarvi et al., 2005]	2005	Correlation coefficients	07%
Biometric gait data	Muaazz *et al.* [Muaaz and Mayrhofer, 2013]	2013	SVM	33.30%
Mobile gait data	Zhong *et al.* [Zhong et al., 2015]	2015	Nearest neighbor	07.22%

- Good results compared with the state of the art in terms of **EER score**.

Generic system – Summary

- Proposal of a generic system for analyzing behavioral biometric data.
- Use of time series-to-image transformation.
- Good results compared to the state of the art on the two tested modalities.

International journal

- **Yris Brice Wandji Piugie**, Christophe Charrier, Joël Di Manno, Christophe Rosenberger, "**Deep Features Fusion for User Authentication Based on Human Activity**," in IET Biometrics Journal, vol. 12, no. 4, pp. 222-234, July 2023. (**ranked Q2**)

International conference

- **Yris Brice Wandji Piugie**, Joël Di Manno, Christophe Rosenberger, Christophe Charrier, "**Keystroke Dynamics based User Authentication using Deep Learning Neural Networks**," International Conference on Cyberworlds (CW), Kanazawa, Japan, 2022, p. 220-227. (**ranked CORE B**)
- **Best Full paper award at the International Conference Cyberworlds 2022 in Kanazawa, Japan**
- **Yris Brice Wandji Piugie**, Joël Di Manno, Christophe Rosenberger, Christophe Charrier, "**How Artificial Intelligence can be used for Behavioral Identification?**", International Conference on Cyberworlds (CW). IEEE, Caen, France, 2021, pp. 246-253. (**ranked CORE B**).

Contents

Contents

Synthetic PAI – Introduction

Context

- Despite promising results and a wide range of applications of biometric systems
- Biometric systems remain vulnerable to malicious attacks, particularly presentation attacks

Specific objectives

1. **Build a behavioral instrument attacks (PAI)**
2. **Presentation attack test with the generated PAI**

Synthetic PAI – Related works

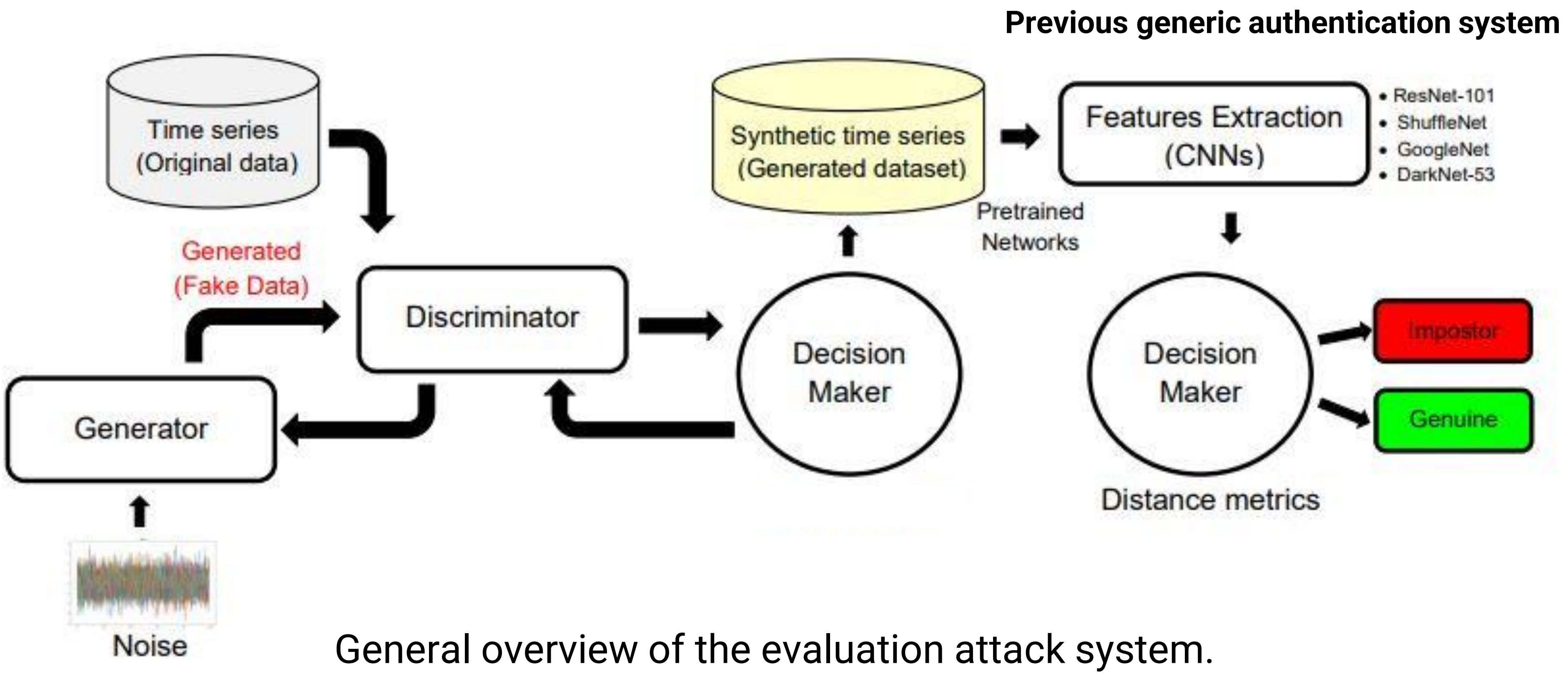
Review of GAN networks for time series applications

Collection of GAN architectures, their applications, datasets used in their experiments, and evaluation criteria for assessing the quality of each respective GAN.

Application	GAN Architecture(s)	Dataset(s)	Evaluation Metrics
Anomaly detection	LSTM-LSTM [25]; LSTM-(LSTM&CNN) [26]; LSTM-LSTM (MAD-GAN) [27]	SET50, NYC taxi data, ECG, SWaT, WADI	Manipulated data used as a test set, ROC curve, precision, recall, F1, accuracy
Audio generation	C-RNN-NN [13]; TGAN(variant) [28]; RNN-FCN [29]; DCGAN(variant) [30]; CNN-CNN [31]	Nottingham dataset, midi music files, MIR-1K, The-Session, speech	Human perception, polyphony, scale consistency, tone span, repetitions, NSDR, SIR, SAR, FD, t-SNE, distribution of notes
Financial time series generation/prediction	TimeGAN [9]; SigCWGAN [32]; DAT-GAN [33]; QuantGAN [34]	S&P 500 index(SPX), Dow Jones index (DJI), ETFs	Marginal distributions, dependencies, TSTR, Wasserstein distance, EM distance, DY metric, ACF score, leverage effect score, discriminative score, predictive score
Time series estimation/prediction	LSTM-NN [35]; LSTM-CNN [36]; LSTM-MLP [36]	Meteorological data, Truven MarketScan dataset	RMSE, MAE, NS, WI, LMI
Time series imputation/repairing	MTS-GAN [37]; CNN-CNN [38]; DCGAN(variant) [39]; AE-GRUI [40]; RGAN [41]; FCN-FCN [42]; GRUI-GRUI [43]	TEP, point machine, wind turbine data, PeMS, PhysioNet Challenge 2012, KDD CUP 2018, parking lot data	Visually, MMD, MAE, MSE, RMSE, MRE, spatial similarity, AUC score
Other time series generation	VAE-CNN [44]	Fixed length time series "vehicle and engine speed"	DTW, SSIM
Medical/Physiological generation	LSTM-LSTM [14], [45]–[49]; LSTM-CNN [50], [51]; BiLSTM-CNN [52]; BiGridLSTM-CNN [53]; CNN-CNN [54], [55]; AE-CNN [56]; FCNN [57]	EEG, ECG, EHRs, PPG, EMG, speech, NAF, MNIST, synthetic sets	TSTR, MMD, reconstruction error, DTW, PCC, IS, FID, ED, S-WD, RMSE, MAE, FD, PRD, averaging samples, WA, UAR, MV-DTW

Synthetic PAI – Proposed architecture

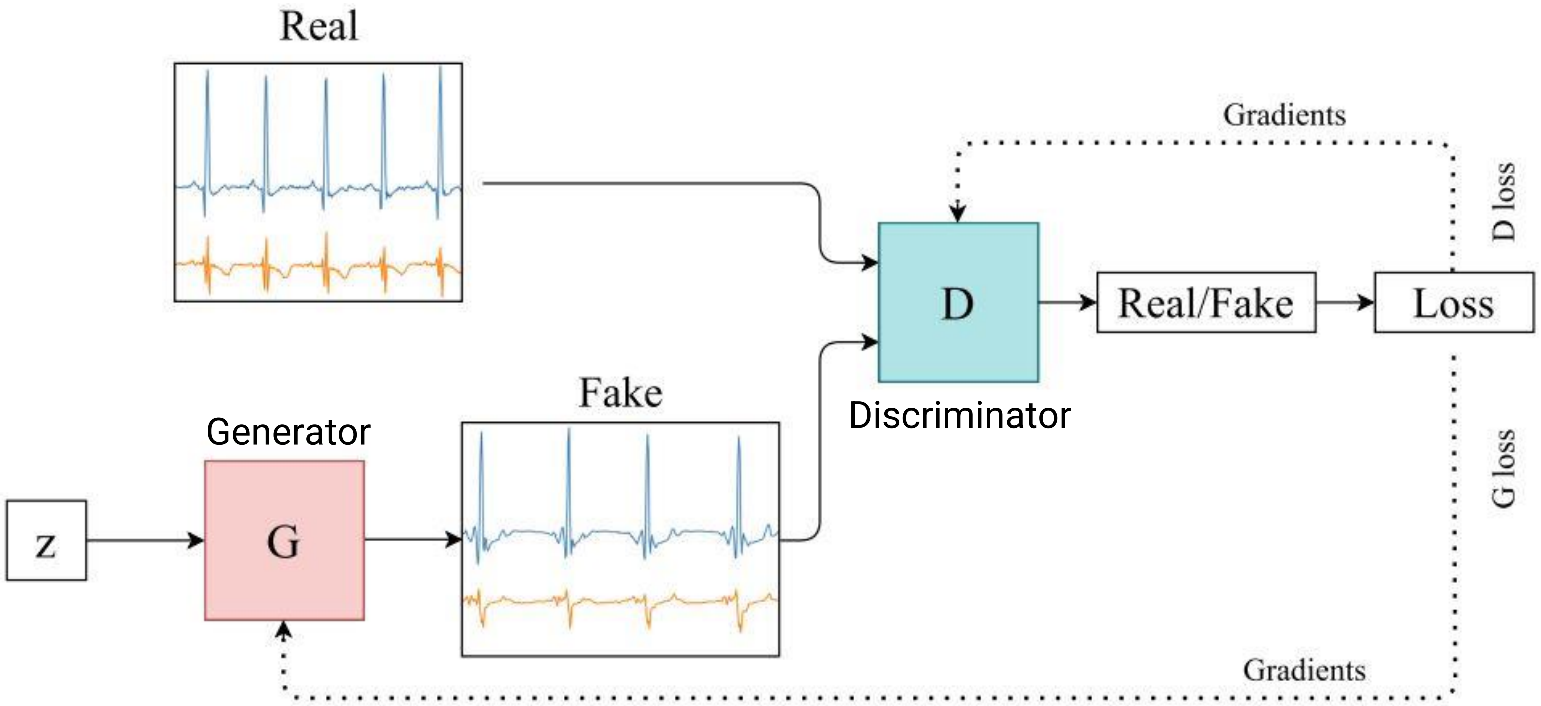
Evaluation attack system



General overview of the evaluation attack system.

Synthetic PAI – Generative Adversarial Networks

GAN principle



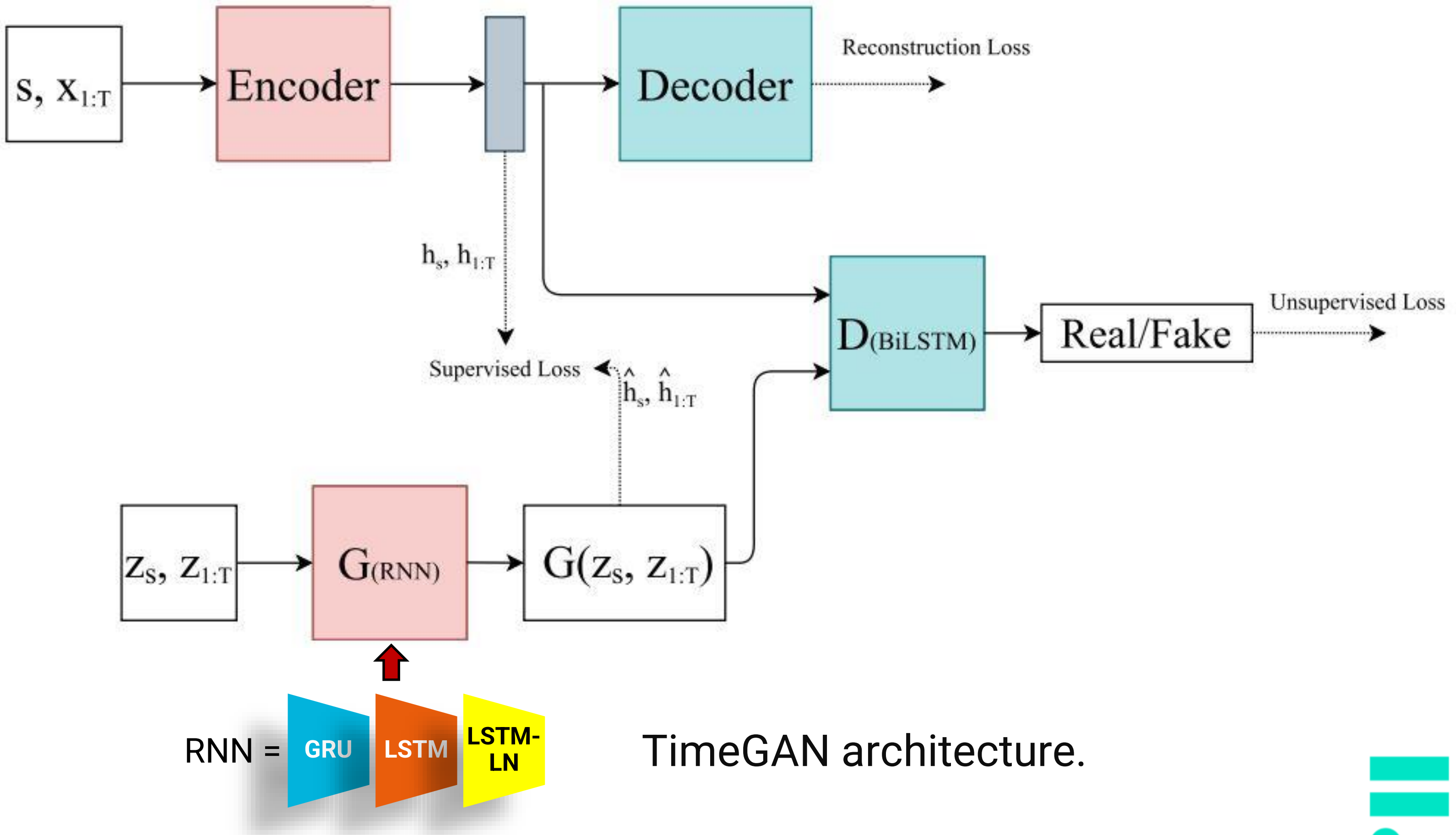
Generative adversarial network.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2014). Generative adversarial nets. Advances in neural information processing systems, 27

Synthetic PAI – TimeGAN architecture

Methodology for generating synthetic signals

- s : static feature
- x : temporal feature
- h : real latent codes
- ĥ : synthetic latent codes



TimeGAN architecture.

Brophy, E., Wang, Z., She, Q., and Ward, T. (2023). Generative adversarial networks in time series: A systematic literature review. ACM Computing Surveys, 55(10):1–31.

Synthetic PAI – Protocol

TimeGAN network Parameter

Module

- GRU : Gated Recurrent Unit
- LSTM : Long Short Term Memory
- LSTM-LN : Long Short Term Memory Layer Normalization

TimeGAN network parameters applied on **GREYC-NISLAB** and **UCI-HAR** databases

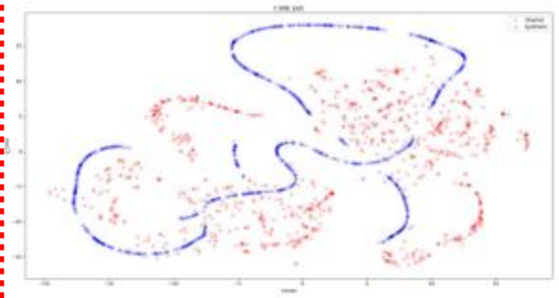
Parameter	Option
Module	'GRU', 'LSTM', 'LSTM LN'
Hidden dimensions	24
Number of layers	5
Iterations	10000
Batch size	128

Synthetic PAI – Method results

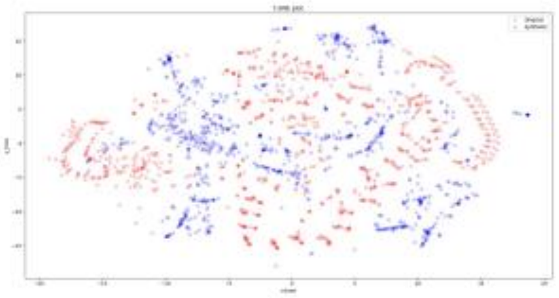
Visual inspection : t-SNE

t-SNE (t-Distributed Stochastic Neighbor Embedding)

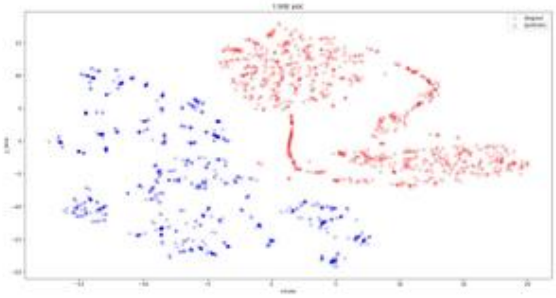
- Dimensionality reduction
- Data Visualization
- Preserving Local Similarities



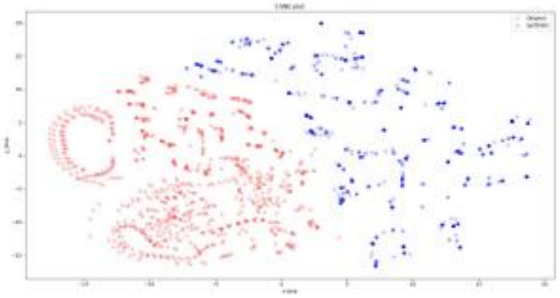
(A) UCI-HAR with GRU module



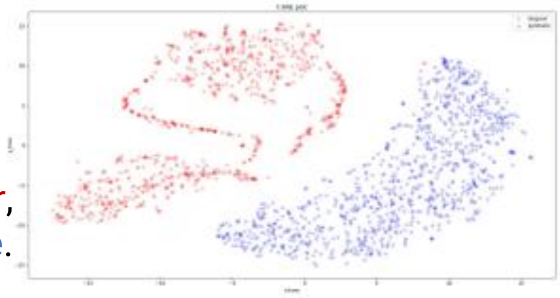
(B) GREYC-NISLAB with GRU module



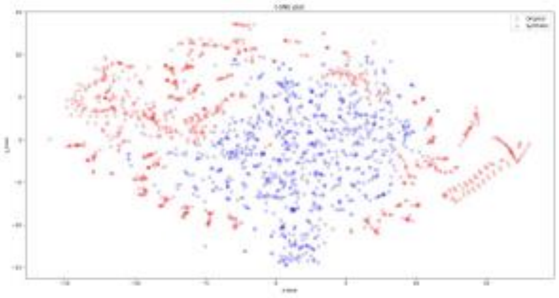
(C) UCI-HAR with LSTM module



(D) GREYC-NISLAB with LSTM module



(E) UCI-HAR with LSTM LN module



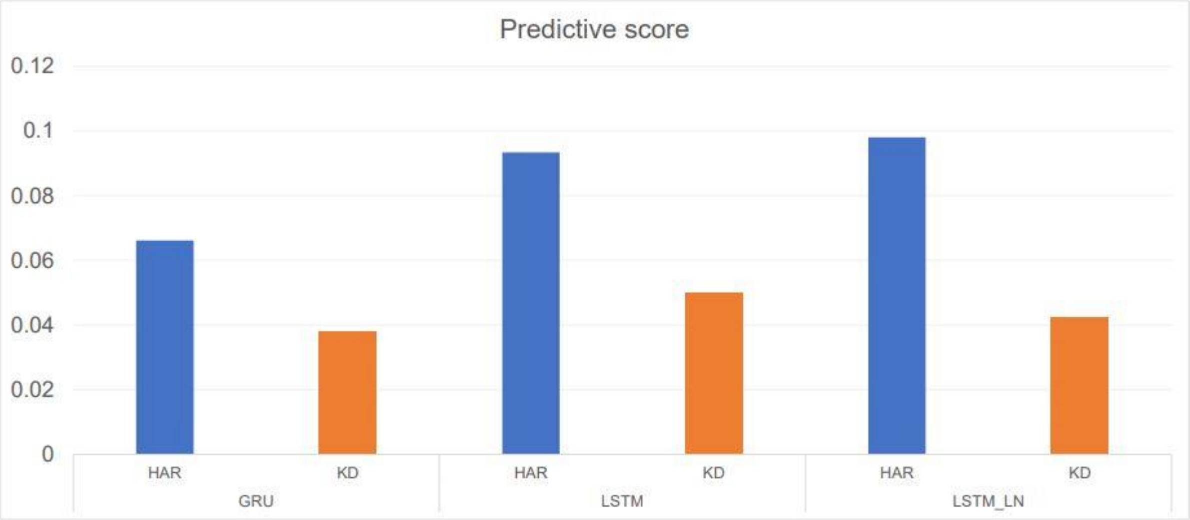
(F) GREYC-NISLAB with LSTM LN module

The real dataset is in red color,
and the synthetic dataset is in blue.

Synthetic PAI – Method results

Objective metric : predictive score

- Pearson's Correlation Coefficient $$\mathrm{PCC} = \frac{\sum_{i=1}^{N}(x_i - \tilde{x})(y_i - \tilde{y})}{\sqrt{(\sum_{i=1}^{N}((x_i - \tilde{x})^2 \sum_{i=1}^{N}((y_i - \tilde{y})^2}}$$
- Percent Root mean square Difference $$\mathrm{PRD} = \sqrt{\frac{\sum_{i=1}^{N}((x_i - y_i)^2}{\sum_{i=1}^{N}((x_i)^2}}$$
- Root Mean Square Error $$\mathrm{RMSE} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}((x_i - y_i)^2}$$
- Mean Relative Absolute Error $$\mathrm{MRAE} == \frac{1}{N}\sum_{i=1}^{N}\left|\frac{x_i - y_i}{x_i - f_i}\right|$$

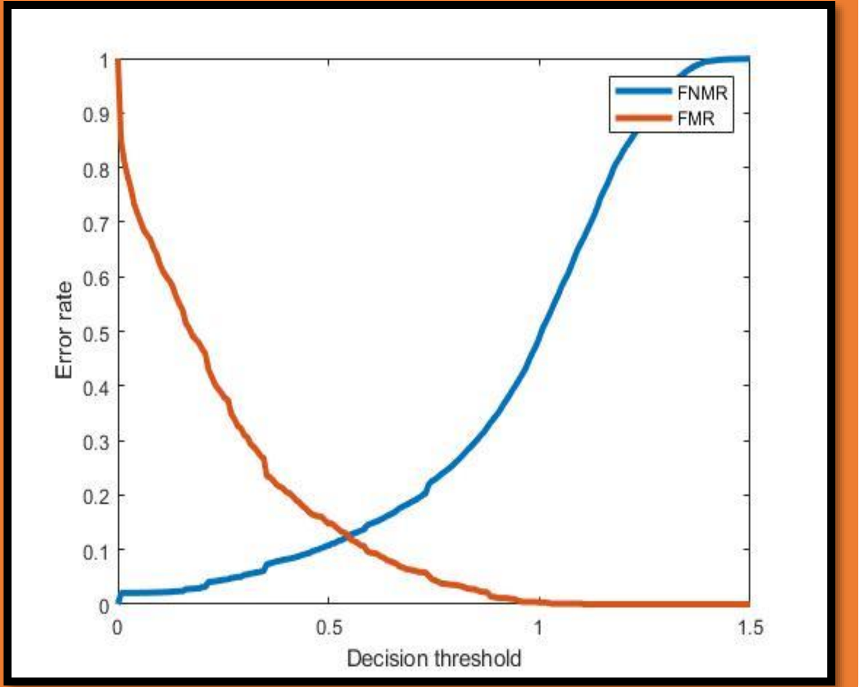


TimeGAN with predictive score (MRAE).

Synthetic PAI – Performance evaluation

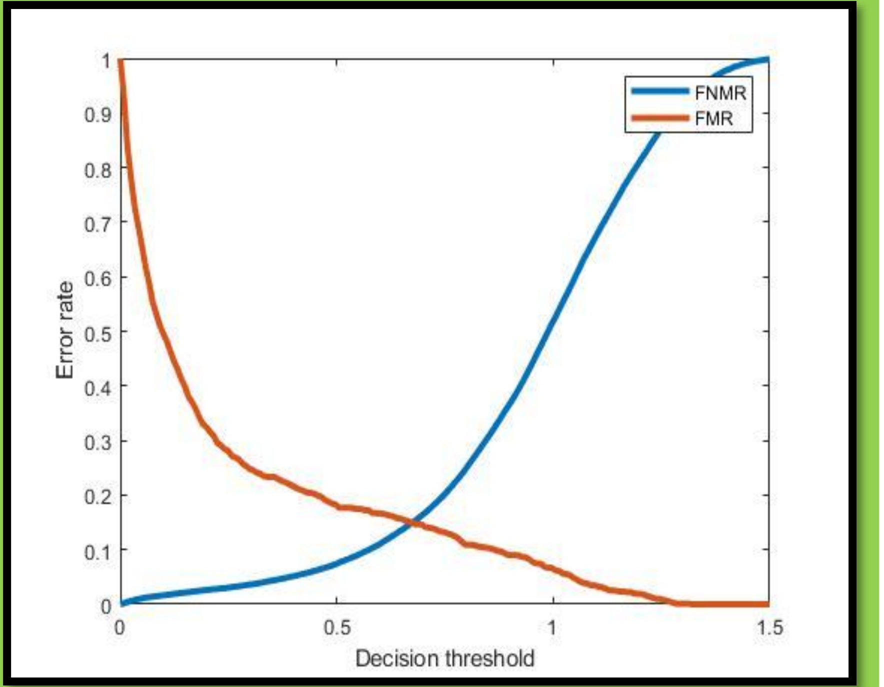
Synthetic data evaluation

GREYC-NISLAB on GoogleNet



EER = 12.48%

UCI-HAR on ShuffleNet



EER = 14.92%

Synthetic PAI – Performance evaluation

Comparison of synthetic versus real data

Performance metrics comparison

Dataset	Classifier name	Type of data	EER
UCI-HAR	ShuffeNet	Real	03.57%
		Synthetic	14.92%
GREYC-NISLAB	GoogleNet	Real	04.89%
		Synthetic	12.48%

- Consistent in term of EER values
- Synthetic behavioral biometric data obtain higher EER values

Synthetic PAI – Summary

Results obtained

- Proposal of generic synthetic behavioral data.
- Consistent results in terms of visual inspection with t-SNE.
- Preserving temporal dynamics, meaning that new sequences respect the original relationships between variables over time.
- Data generation to generate databases for performance or presentation attacks.
- Explain the lower performance on synthetic data.

Contents

Conclusions and perspectives

Proposal of a generic method based on Deep for analyzing behavioral biometrics, with applications such as KD and HA.

Work on user identification: demonstrating our capability to profile users using classical machine learning techniques.

Definition of an innovative method for processing raw biometric data considered as time series.

Promising results on behavioral biometric data generation, which can be used to generate databases for performance or presentation attacks.

Conclusions and perspectives

Future research

- Add psychological features (user's emotion) and evaluate the impact.
- Explore biaises in behavioral modalities related to gender, age, hand, and ethnicity.
- Develop quality measurement for behavioral biometric data.
- Generate large behavioral biometric datasets.
- Test behavioral PAIs level C from FIDO requirement.
- Apply the proposed generic method to the analysis of other behavioral biometric modalities.
- Study the impact of the noise on TimeGAN generation.
- Adapted the loss function (1-loss(F(V(G,D)) on TimeGAN.
- Consider the user profile in the synthetic behavioral generation.

Publications

International journal

- **Yris Brice Wandji Piugie**, Christophe Charrier, Joël Di Manno, Christophe Rosenberger, "**Deep Features Fusion for User Authentication Based on Human Activity**," in IET Biometrics Journal, vol. 12, no. 4, pp. 222-234, July 2023. (**ranked Q2**)

International conferences, Honors & Awards

- **Yris Brice Wandji Piugie**, Joël Di Manno, Christophe Rosenberger, Christophe Charrier, "**Keystroke Dynamics based User Authentication using Deep Learning Neural Networks**," International Conference on Cyberworlds (CW), Kanazawa, Japan, 2022, p. 220-227.(**ranked CORE B**)
- **Best Full paper award at the International Conference Cyberworlds 2022 in Kanazawa, Japan**
- **Yris Brice Wandji Piugie**, Joël Di Manno, Christophe Rosenberger, Christophe Charrier, "**How Artificial Intelligence can be used for Behavioral Identification?**", International Conference on Cyberworlds (CW). IEEE, Caen, France, 2021, pp. 246-253. (**ranked CORE B**).
- Cyrius Nugier, Diane Leblanc-Albarel, Agathe Blaise, Simon Masson, Paul Huynh and **Yris Brice Wandji Piugie**, "**An Upcycling Tokenization Method for Credit Card Numbers**," SECRYPT 2021-18th International Conference on Security and Cryptography, Paris, France, 2021, pp. 1-12. (**rank CORE B**).

Poster

- Yris Brice Wandji Piugie, Joël Di Manno, Christophe Rosenberger, and Christophe Charrier. 2022. **Keystroke dynamics-based user authentication using deep learning neural networks** (DFKI-INRIA summer school, Saarbruken-Germany).
- Yris Brice Wandji Piugie, Joël Di Manno, Christophe Rosenberger, and Christophe Charrier. 2021. **How artificial intelligence can be used for behavioral identification?** in 2021 International Conference on Cyberworlds (CW), Caen-France

End

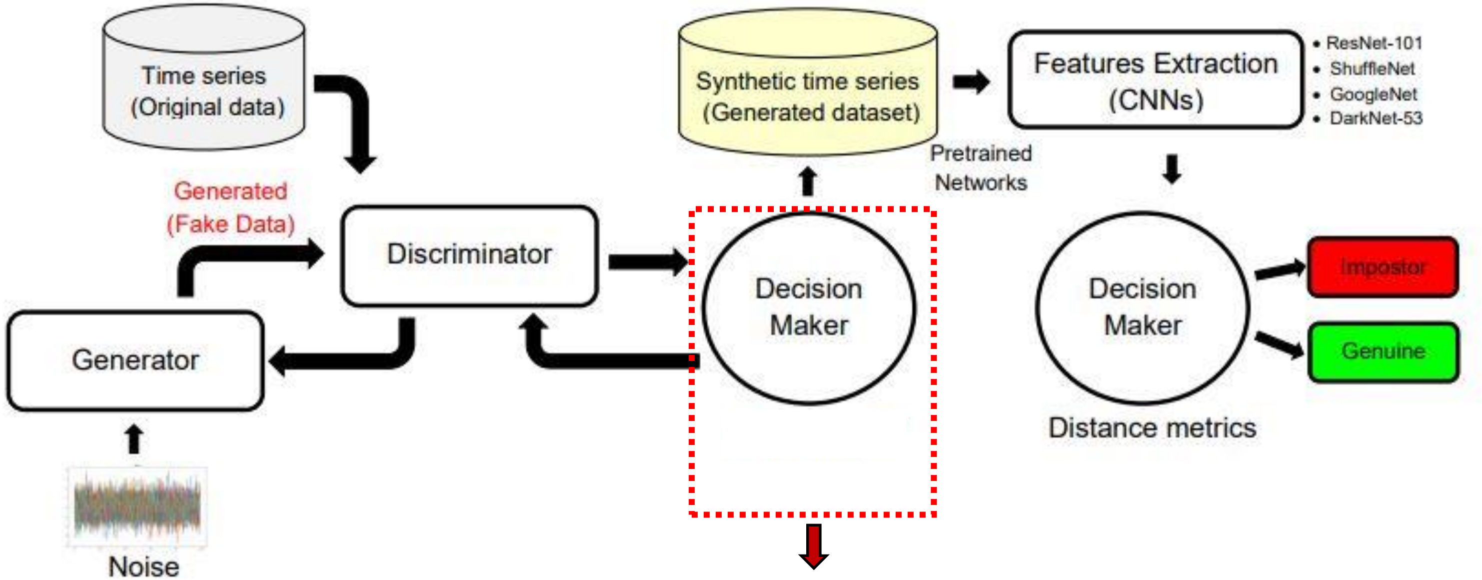
- Thank you

- Questions ?

yris-brice.wandji-piugie@unicaen.fr
https://wandjip191.users.greyc.fr/

Review answer

Study the impact of the noise

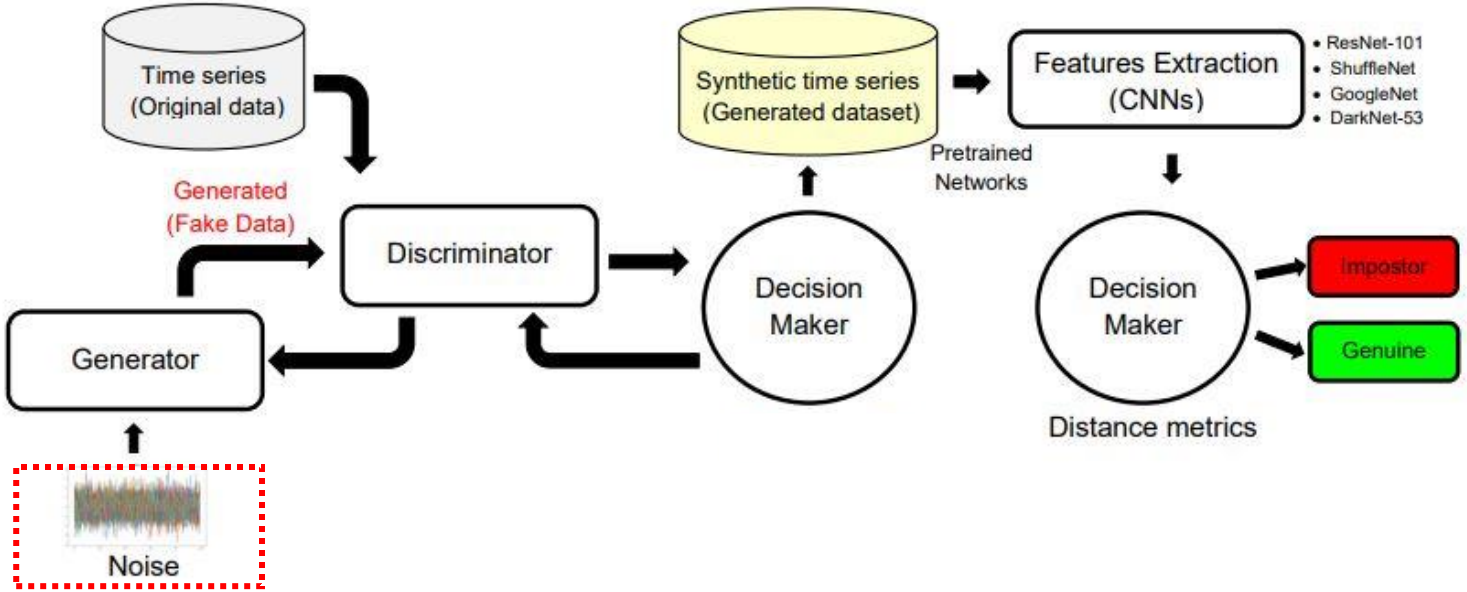


This is done through:

- **Visual inspection**
- **Precision score**
- **Loss function**

Review answer

Study the impact of the noise



sigma = [0.2; 0.5; 0.7; 0,9]

Review answer

PAIs level C from FIDO 3.0 requirement

Level C	**Time:** > 7 days **Expertise:** Expert(s) **Equipment:** Specialized, bespoke	3D printed spoofs	silicon masks, theatrical masks	contact lens/prosthetic eye with a specific pattern	voice synthesizer
	Source of Biometric Characteristic: Difficult	3D fingerprint information from subject	high quality photo, 3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

Level C

Level C includes the most difficult attacks.

1. **Elapsed time:** <=one month, >one month
2. **Expertise:** Expert, multiple experts
3. **Equipment:** Specialized, bespoke
4. **Access to biometric characteristics:** Difficult

If at least one of these characteristics reaches the levels listed above, the attack is categorized as Level C.

More sophisticated voice synthesizer which can playback any words, trained from long, high quality recordings or a database of recordings	C
Impersonation, where an attacker is able to mimic a person's voice	C