Ensemble of Adaptive Algorithms for Keystroke Dynamics

Paulo Henrique Pisani [1]

Ana Carolina Lorena [2]

André C. P. L. F. de Carvalho [1]

[1] Universidade de São Paulo (USP)
[2] Universidade Federal de São Paulo (UNIFESP)

Brazilian Conference on Intelligence Systems (BRACIS) – november/2015

1.
Introduction

2.
Ensembles in Adaptive Biometric Systems

3.
Experimental Results and Conclusion

1. Introduction

2. Ensembles in Adaptive Biometric Systems

3. Experimental Results and Conclusion

Biometrics is considered a suitable option to improve current authentication systems.

Biometric features must meet some requirements [Jain et al., 2004]:

Universality	everyone has the feature.
Collectability	it is possible to quantify the feature quantitatively.
Distinctiveness	the feature allows to distinguish one person from another.
Permanence	feature should be invariant over time.

Biometrics is considered a suitable option to improve current authentication systems.

Biometric features must meet some requirements [Jain et al., 2004]:

Universality	• everyone has the feature.
Collectability	• it is possible to quantify the feature quantitatively
Distinctiveness	
Permanence	• feature should be invariant over time.

However, several studies have shown that it is not the case in practice: ***template ageing*** [Fenker et al., 2013].

Context

Adaptive Biometric Systems deal with *template ageing* by automatically adapting the user model over time.

Several **adaptive one-class algorithms** have been used for this purpose. However, the performance is not usually consistent over different datasets;

Context

Adaptive Biometric Systems deal with *template ageing*

Studies have shown that the combination of individual techniques in **ensembles** may lead to **more accurate and stable decision models**.

Several **adaptive one-class algorithms** have been used for this purpose. However, the

This paper investigates the use of simple **ensemble approaches** for adaptive biometric systems:

- *Proposal of a model to apply an ensemble of adaptive algorithms for biometrics;*
- *Study of the behaviour of the ensemble with adaptive algorithms in a data stream context.*

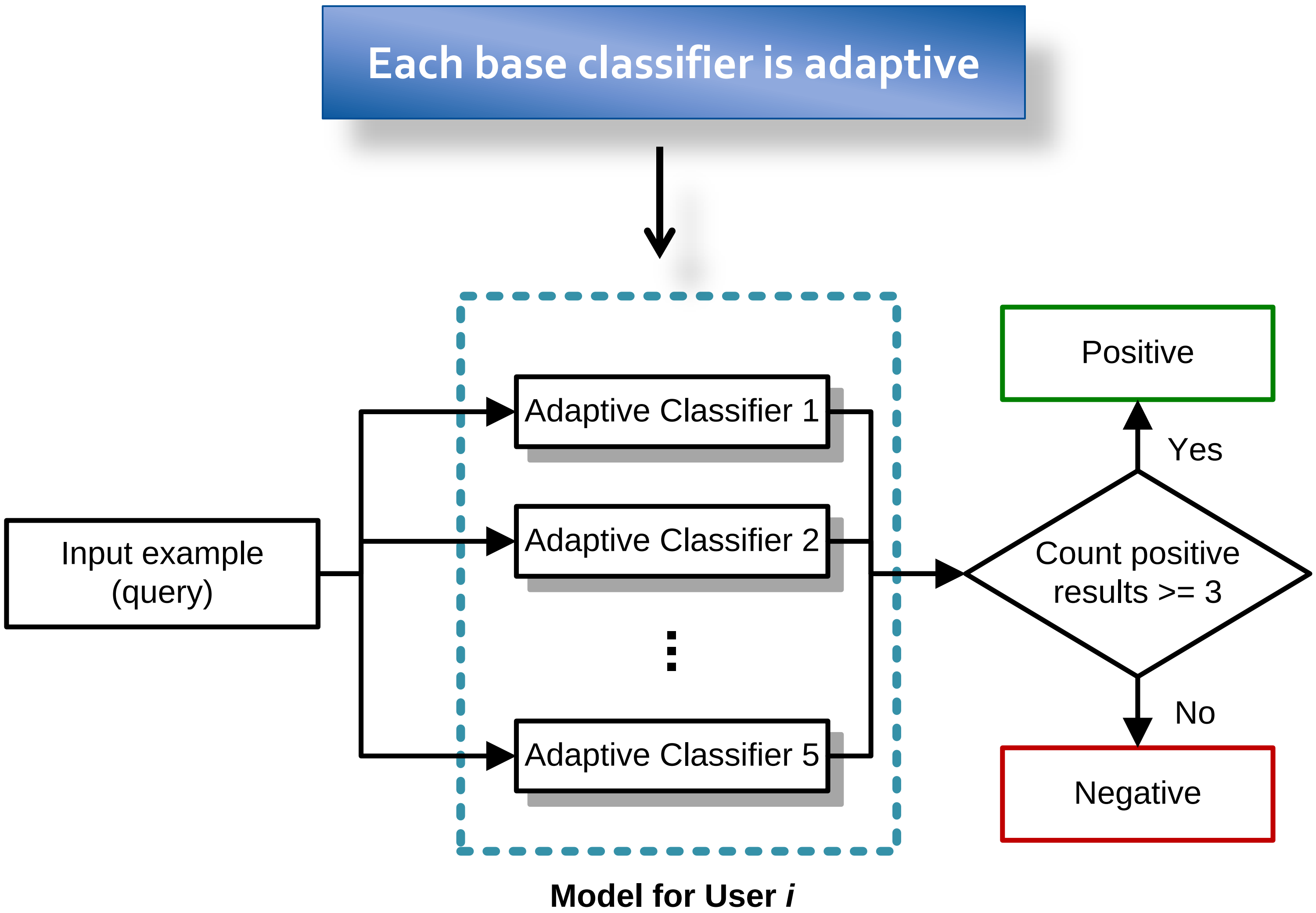
Context

1.
Introduction

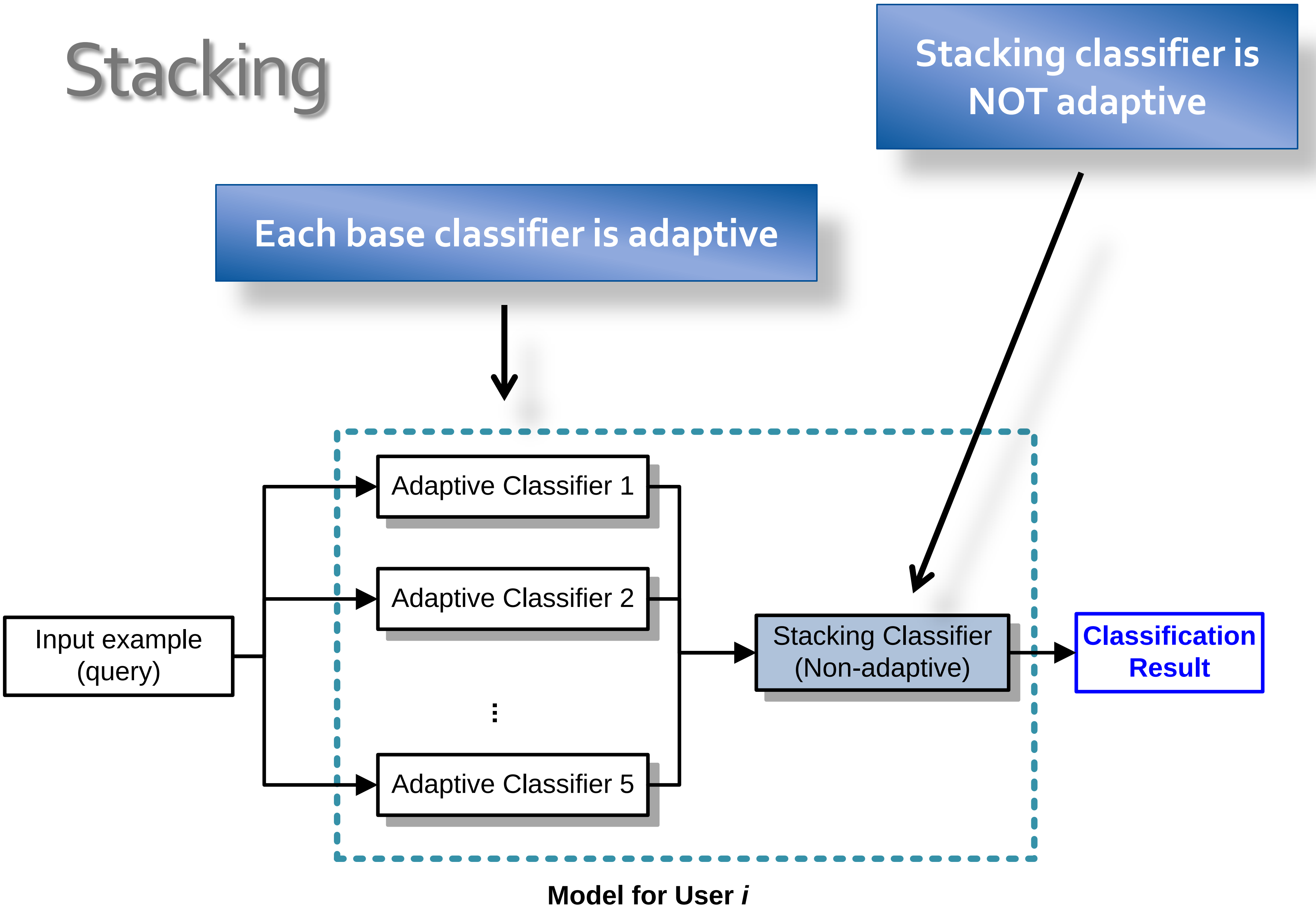
2.
Ensembles in Adaptive Biometric Systems

3.
Experimental Results and Conclusion

Majority Voting

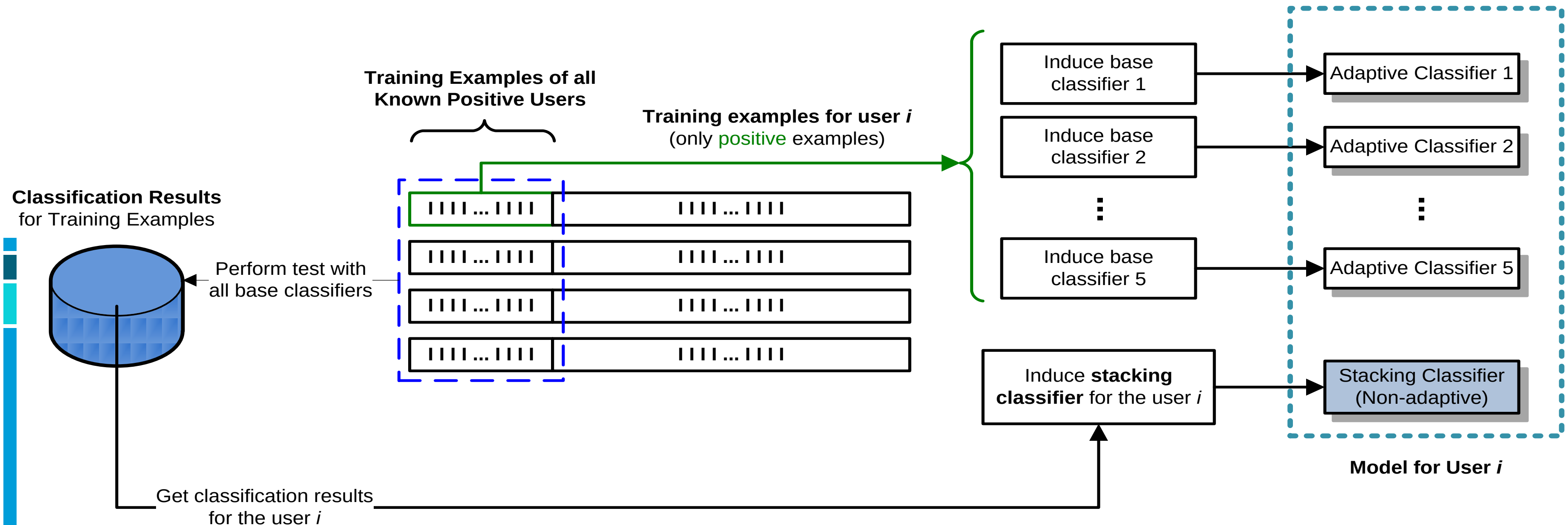


Stacking


Stacking classifier is NOT adaptive
Each base classifier is adaptive
Adaptive Classifier 1
Adaptive Classifier 2
⋮
Adaptive Classifier 5
Input example (query)
Stacking Classifier (Non-adaptive)
Classification Result
Model for User *i*

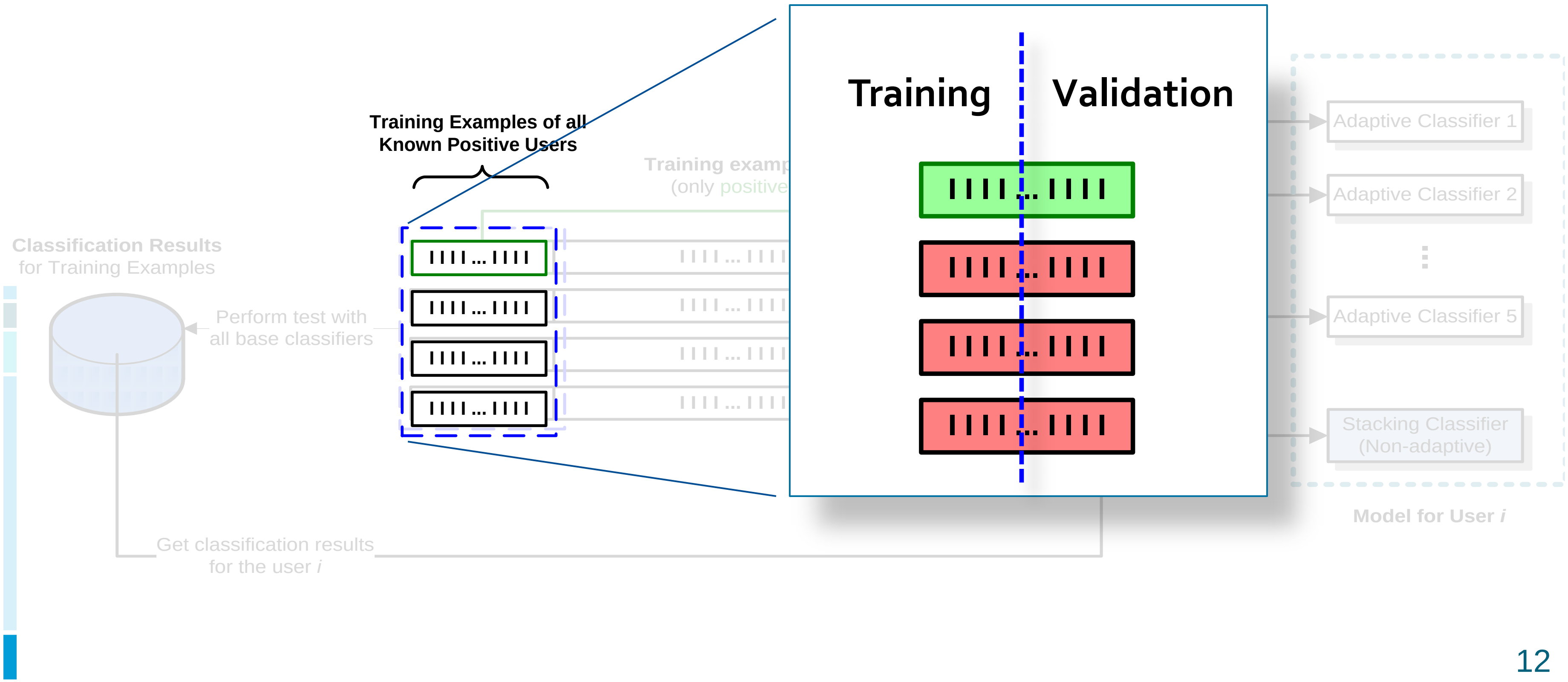
Stacking Training

- Stacking classifier requires both positive and negative examples
- Biometric system has access to data from all enrolled users



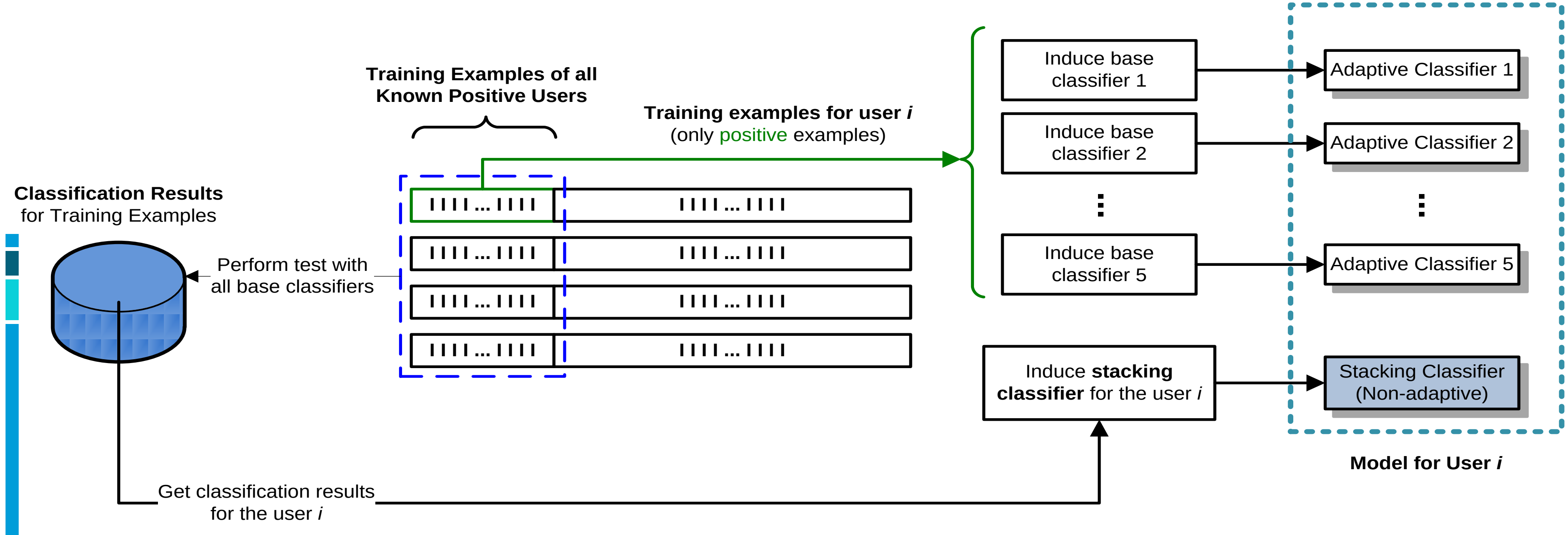
Stacking Training

- Stacking classifier requires both positive and negative examples;
- Biometric system has access to data from all enrolled users;



Stacking Training

- Stacking classifier requires both positive and negative examples;
- Biometric system has access to data from all enrolled users;



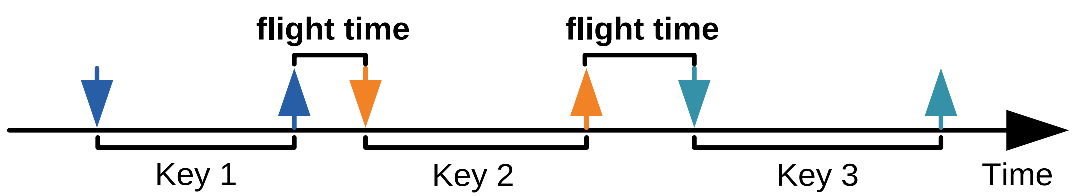
1\.
Introduction

2\.
Ensembles in Adaptive Biometric Systems

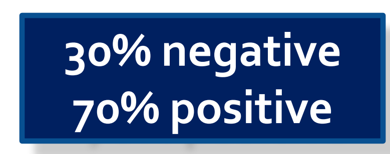
3\.
Experimental Results and Conclusion

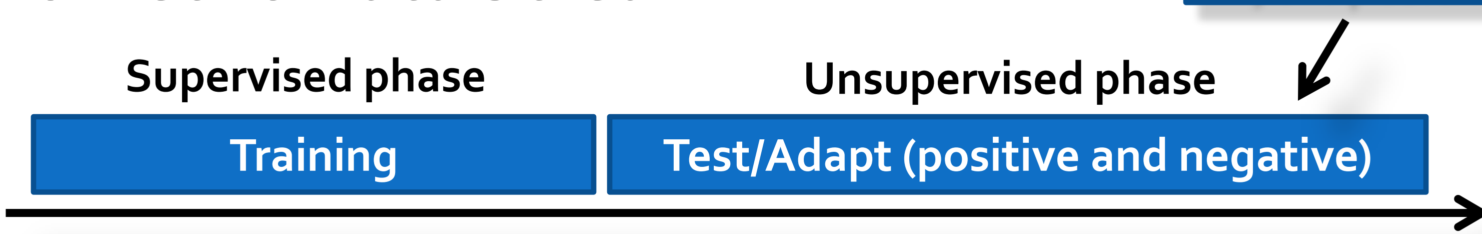
Experimental Setup

- Datasets:
  - GREYC: 100 users (2 months)
  - CMU: 51 users (8 sessions)
  - GREYC-Web: 35 users (> 1 year)
- Extracted features:



- Biometric Data Stream:





Experimental Setup

- **Base** Classification Algorithms (adaptive):
  - **M2005** (I. Double Parallel)
  - **Self-Detector** (Sliding, Usage Control R, Usage Control S, Usage Control 2)
- **Stacking** Classification Algorithms (static):
  - Multilayer Perceptron
  - Decision Tree (J48)
  - Random Forest
  - Naïve Bayes

Experimental Results

	GREYC Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.090 (0.010)	0.165 (0.005)	0.872 (0.006)
	Self-Detector (Sliding)	0.092 (0.011)	0.129 (0.004)	$\boxed{\textbf{0.890}\ (0.006)}$
	Self-Detector (Usage Control R)	0.092 (0.010)	0.140 (0.005)	0.884 (0.006)
	Self-Detector (Usage Control S)	0.089 (0.010)	0.149 (0.005)	0.881 (0.006)
	Self-Detector (Usage Control 2)	**0.069** (0.009)	0.168 (0.006)	0.882 (0.006)
	M2005	0.221 (0.019)	0.130 (0.003)	0.824 (0.009)
	M2005 (I. Double Parallel)	0.210 (0.018)	**0.092** (0.004)	0.849 (0.008)
E	*Ensemble (Voting)*	**0.087** (0.010)	0.126 (0.005)	$\boxed{0.893\ (0.006)}$
	Ensemble (MLP)	0.181 (0.016)	0.054 (0.004)	0.882 (0.008)
	Ensemble (Random Forest)	0.185 (0.016)	**0.053** (0.004)	0.881 (0.008)
	Ensemble (Naive Bayes)	0.116 (0.012)	0.094 (0.005)	**0.895** (0.007)
	Ensemble (Decision Tree)	0.184 (0.013)	0.066 (0.005)	0.875 (0.006)

	CMU Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.287 (0.023)	0.410 (0.016)	0.651 (0.009)
	Self-Detector (Sliding)	0.291 (0.031)	**0.211** (0.013)	0.749 (0.016)
	Self-Detector (Usage Control R)	0.311 (0.030)	0.220 (0.013)	0.735 (0.015)
	Self-Detector (Usage Control S)	0.213 (0.014)	0.275 (0.012)	0.756 (0.008)
	Self-Detector (Usage Control 2)	0.143 (0.012)	0.323 (0.014)	0.767 (0.009)
	M2005	0.273 (0.028)	0.451 (0.019)	0.638 (0.013)
	M2005 (I. Double Parallel)	**0.122** (0.011)	0.306 (0.008)	$\boxed{\textbf{0.786}\ (0.006)}$
E	*Ensemble (Voting)*	**0.208** (0.017)	0.239 (0.013)	$\boxed{0.776\ (0.009)}$
	Ensemble (MLP)	0.257 (0.039)	0.182 (0.018)	**0.781** (0.012)
	Ensemble (Random Forest)	0.283 (0.044)	**0.168** (0.020)	0.775 (0.014)
	Ensemble (Naive Bayes)	0.255 (0.025)	0.202 (0.010)	0.772 (0.015)
	Ensemble (Decision Tree)	0.299 (0.043)	0.169 (0.016)	0.766 (0.014)

	GREYC-Web Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.066 (0.008)	0.141 (0.005)	0.896 (0.005)
	Self-Detector (Sliding)	0.074 (0.011)	**0.085** (0.004)	0.920 (0.007)
	Self-Detector (Usage Control R)	0.069 (0.009)	0.086 (0.004)	$\boxed{\textbf{0.922}\ (0.006)}$
	Self-Detector (Usage Control S)	0.053 (0.007)	0.123 (0.005)	0.912 (0.005)
	Self-Detector (Usage Control 2)	**0.035** (0.007)	0.148 (0.010)	0.908 (0.007)
	M2005	0.096 (0.013)	0.245 (0.016)	0.829 (0.008)
	M2005 (I. Double Parallel)	0.095 (0.015)	0.131 (0.011)	0.887 (0.008)
E	*Ensemble (Voting)*	**0.052** (0.007)	0.091 (0.004)	$\boxed{\textbf{0.928}\ (0.005)}$
	Ensemble (MLP)	0.126 (0.015)	**0.052** (0.006)	0.911 (0.008)
	Ensemble (Random Forest)	0.122 (0.026)	**0.052** (0.004)	0.913 (0.012)
	Ensemble (Naive Bayes)	0.087 (0.022)	0.067 (0.007)	0.923 (0.008)
	Ensemble (Decision Tree)	0.121 (0.016)	0.063 (0.005)	0.908 (0.007)

Majority Voting Ensemble:
Consintent high performance

Overall performance

Experimental Results

	GREYC Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.090 (0.010)	0.165 (0.005)	0.872 (0.006)
	Self-Detector (Sliding)	0.092 (0.011)	0.129 (0.004)	**0.890** (0.006)
	Self-Detector (Usage Control R)	0.092 (0.010)	0.140 (0.005)	0.884 (0.006)
	Self-Detector (Usage Control S)	0.089 (0.010)	0.149 (0.005)	0.881 (0.006)
	Self-Detector (Usage Control 2)	**0.069** (0.009)	0.168 (0.006)	0.882 (0.006)
	M2005	0.221 (0.019)	0.130 (0.003)	0.824 (0.009)
	M2005 (I. Double Parallel)	0.210 (0.018)	**0.092** (0.004)	0.849 (0.008)
E	*Ensemble (Voting)*	**0.087** (0.010)	0.126 (0.005)	0.893 (0.006)
	Ensemble (MLP)	0.181 (0.016)	0.054 (0.004)	0.882 (0.008)
	Ensemble (Random Forest)	0.185 (0.016)	**0.053** (0.004)	0.881 (0.008)
	Ensemble (Naive Bayes)	0.116 (0.012)	0.094 (0.005)	**0.895** (0.007)
	Ensemble (Decision Tree)	0.184 (0.013)	0.066 (0.005)	0.875 (0.006)

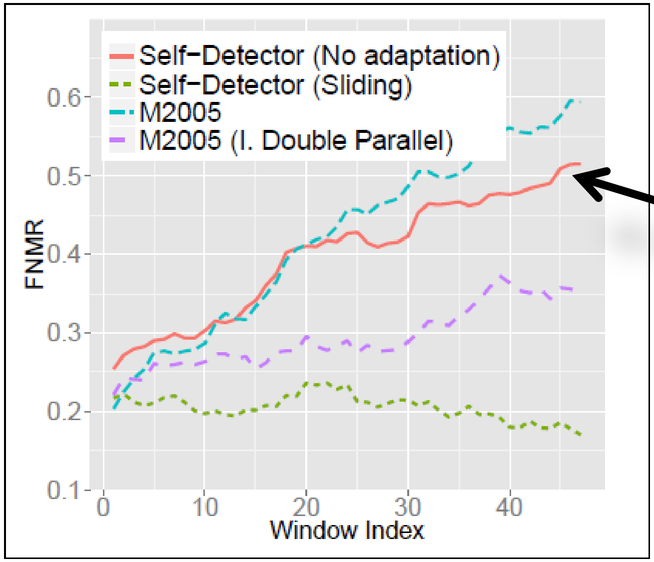
	CMU Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.287 (0.023)	0.410 (0.016)	0.651 (0.009)
	Self-Detector (Sliding)	0.291 (0.031)	**0.211** (0.013)	0.749 (0.016)
	Self-Detector (Usage Control R)	0.311 (0.030)	0.220 (0.013)	0.735 (0.015)
	Self-Detector (Usage Control S)	0.213 (0.014)	0.275 (0.012)	0.756 (0.008)
	Self-Detector (Usage Control 2)	0.143 (0.012)	0.323 (0.014)	0.767 (0.009)
	M2005	0.273 (0.028)	0.451 (0.019)	0.638 (0.013)
	M2005 (I. Double Parallel)	**0.122** (0.011)	0.306 (0.008)	**0.786** (0.006)
E	*Ensemble (Voting)*	**0.208** (0.017)	0.239 (0.013)	0.776 (0.009)
	Ensemble (MLP)	0.257 (0.039)	0.182 (0.018)	**0.781** (0.012)
	Ensemble (Random Forest)	0.283 (0.044)	**0.168** (0.020)	0.775 (0.014)
	Ensemble (Naive Bayes)	0.255 (0.025)	0.202 (0.010)	0.772 (0.015)
	Ensemble (Decision Tree)	0.299 (0.043)	0.169 (0.016)	0.766 (0.014)

	GREYC-Web Dataset			
	Algorithm	**FMR**	**FNMR**	**Acc (balanc.)**
B	*Self-Detector (No adaptation)*	0.066 (0.008)	0.141 (0.005)	0.896 (0.005)
	Self-Detector (Sliding)	0.074 (0.011)	**0.085** (0.004)	0.920 (0.007)
	Self-Detector (Usage Control R)	0.069 (0.009)	0.086 (0.004)	**0.922** (0.006)
	Self-Detector (Usage Control S)	0.053 (0.007)	0.123 (0.005)	0.912 (0.005)
	Self-Detector (Usage Control 2)	**0.035** (0.007)	0.148 (0.010)	0.908 (0.007)
	M2005	0.096 (0.013)	0.245 (0.016)	0.829 (0.008)
	M2005 (I. Double Parallel)	0.095 (0.015)	0.131 (0.011)	0.887 (0.008)
E	*Ensemble (Voting)*	**0.052** (0.007)	0.091 (0.004)	**0.928** (0.005)
	Ensemble (MLP)	0.126 (0.015)	**0.052** (0.006)	0.911 (0.008)
	Ensemble (Random Forest)	0.122 (0.026)	**0.052** (0.004)	0.913 (0.012)
	Ensemble (Naive Bayes)	0.087 (0.022)	0.067 (0.007)	0.923 (0.008)
	Ensemble (Decision Tree)	0.121 (0.016)	0.063 (0.005)	0.908 (0.007)

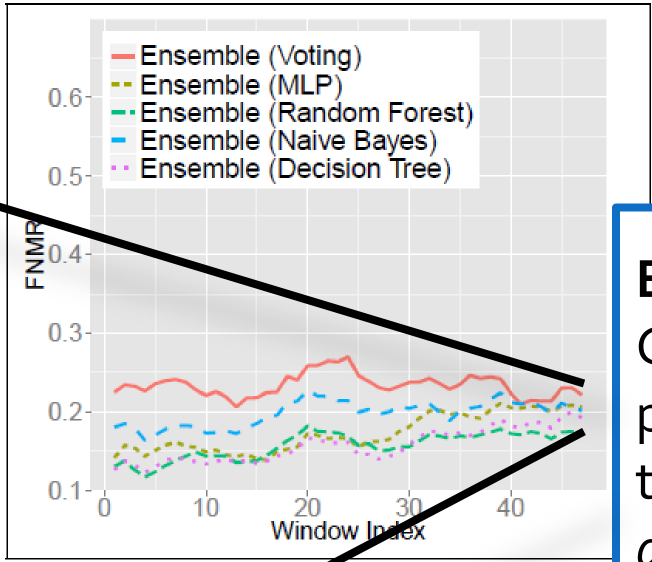
Staking: lower FNMR (may be a result of the imbalanced biometric data stream)

Overall performance

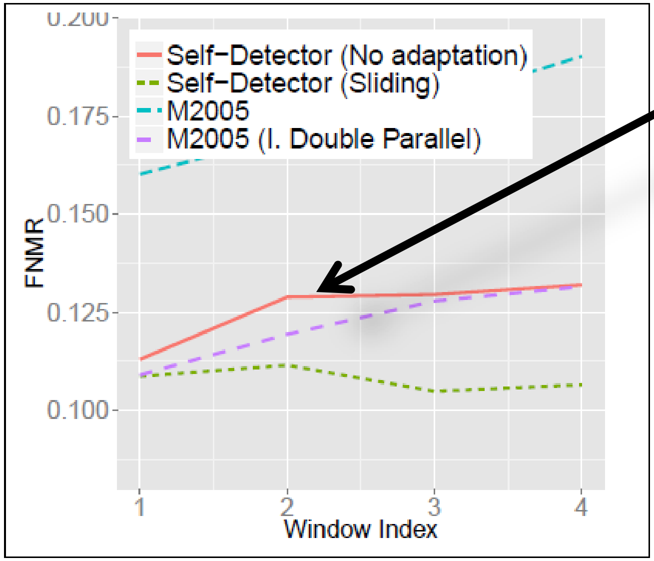
Experimental Results



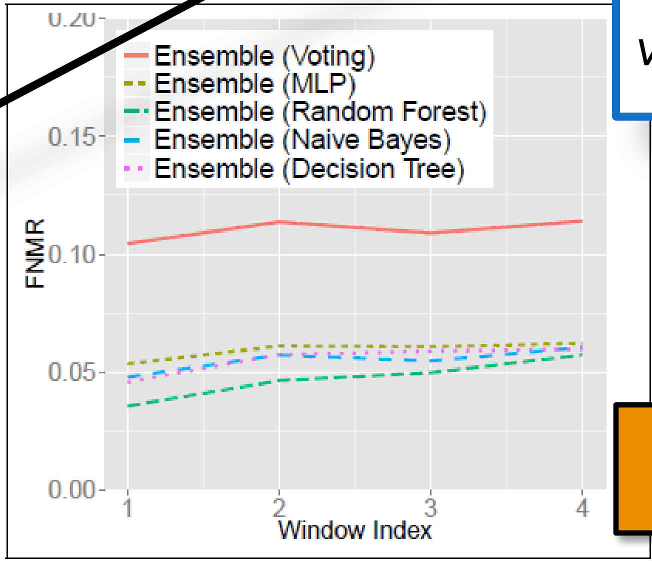
(a) Baselines (CMU).



(b) Ensemble (CMU).



(c) Baselines (GREYC-Web).

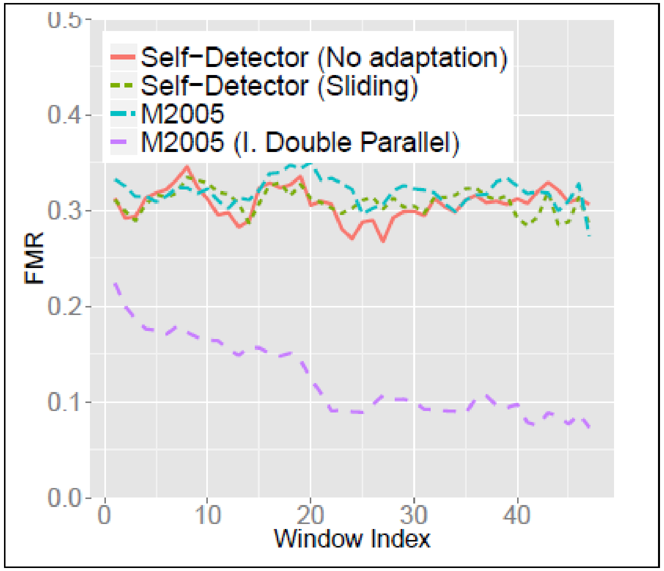


(d) Ensemble (GREYC-Web).

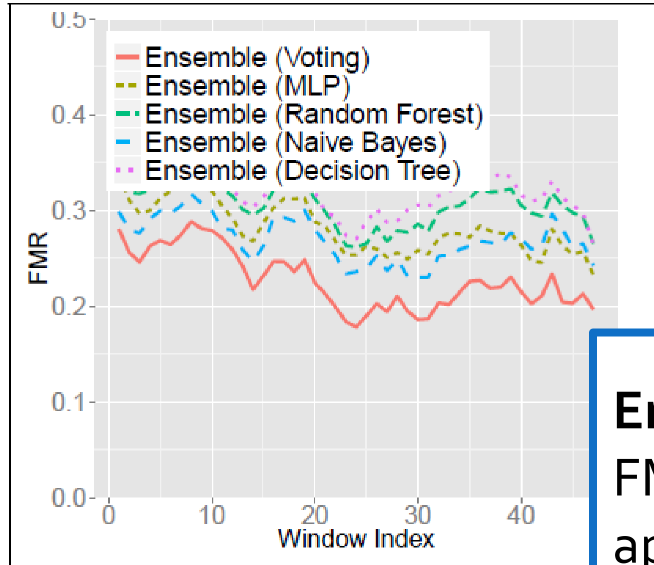
Ensembles:
Good FNMR performance over time (*static algorithms tend to increase FNMR values*)

FNMR

Experimental Results

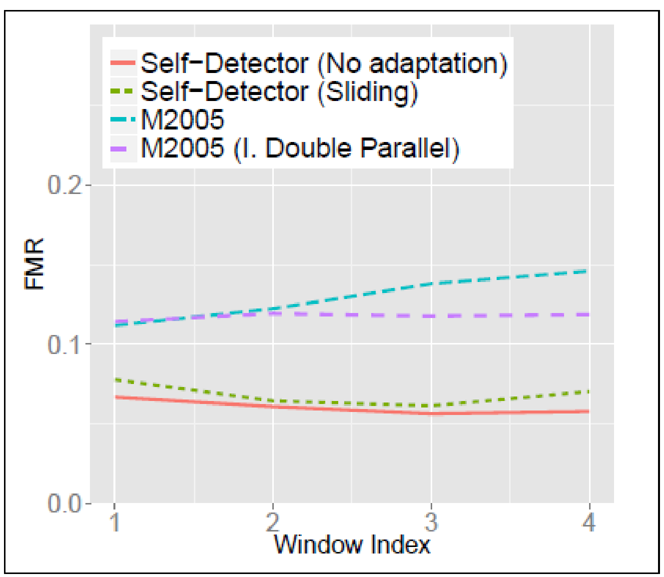


(a) Baselines (CMU).

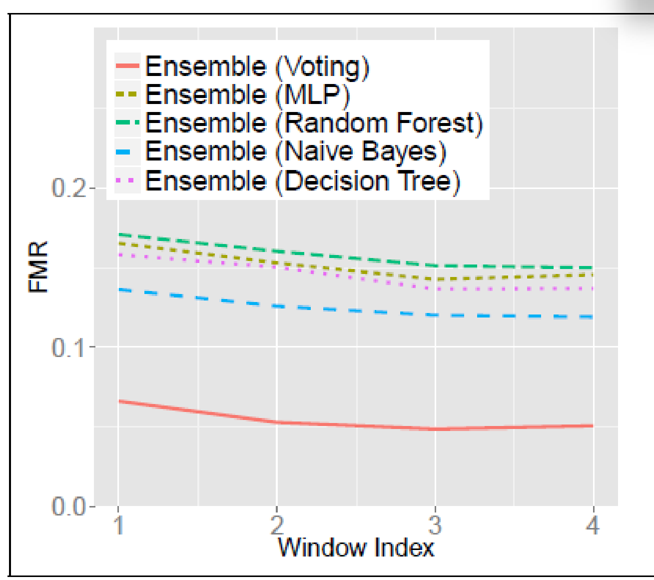


(b) Ensemble (CMU).

Ensembles:
FMR similar to other approaches



(c) Baselines (GREYC-Web).



(d) Ensemble (GREYC-Web).

FMR

1.
Introduction

2.
Ensembles in Adaptive Biometric Systems

3.
Experimental Results and Conclusion

Conclusion

- This paper investigated the use of **ensemble approaches** for adaptive biometric systems (and how to implement them in this context).
- Ensemble approaches resulted in consistent high predictive performance over all datasets;
- Majority Voting (the simplest one) obtained accuracy better than baselines on two datasets;
- Although ensemble implies in high use of computational resources, it may justify its use by the high predictive performance.

- **Future Work**:
  - Change the way of selecting data for stacking classifier training;
  - Additional ensemble approaches.

Ensemble of Adaptive Algorithms for Keystroke Dynamics

- Universidade de São Paulo (USP)
  - Instituto de Ciências Matemáticas e de Computação (ICMC)

- Acknowledgements:
  - FAPESP
  - CAPES
  - CNPq

Paulo Henrique Pisani

Universidade de São Paulo

phpisani@icmc.usp.br

Ana Carolina Lorena

Universidade Federal de São Paulo

aclorena@unifesp.br

André C. P. L. F de Carvalho

Universidade de São Paulo

andre@icmc.usp.br

References

- [1] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4–20, 2004.
- [2] F. Roli, L. Didaci, and G. Marcialis, "Adaptive biometric systems that can improve with use," in Advances in Biometrics, N. Ratha and V. Govindaraju, Eds. Springer London, 2008, pp. 447–471.
- [3] A. Rattani, G. Marcialis, and F. Roli, "Self adaptive systems: An experimental analysis of the performance over time," in Computational Intelligence in Biometrics and Identity Management (CIBIM), 2011 IEEE Workshop on, 2011, pp. 36–43.
- [4] N. Poh, A. Rattani, and F. Roli, "Critical analysis of adaptive biometric systems," Biometrics, IET, vol. 1, no. 4, pp. 179–187, 2012.
- [5] S. Fenker, E. Ortiz, and K. Bowyer, "Template aging phenomenon in iris recognition," Access, IEEE, vol. 1, pp. 266–274, 2013.
- [6] P. H. Pisani, A. C. Lorena, and A. C. P. L. F. de Carvalho, "Adaptive positive selection for keystroke dynamics," Journal of Intelligent & Robotic Systems, pp. 1–17, 2014.
- [7] P. Kang, S.-s. Hwang, and S. Cho, "Continual retraining of keystroke dynamics based authenticator," in Advances in Biometrics, ser. LNCS. Springer Berlin / Heidelberg, 2007, vol. 4642, pp. 1203–1211.
- [8] R. Giot, C. Rosenberger, and B. Dorizzi, "Hybrid template update system for unimodal biometric systems," in Biometrics: Theory, Appli- cations and Systems (BTAS), 2012 IEEE Fifth International Conference on, 2012, pp. 1–7.
- [9] A. Lumini and L. Nanni, "Ensemble of on-line signature matchers based on overcomplete feature generation," Expert Systems with Applications, vol. 36, no. 3, Part 1, pp. 5291 – 5296, 2009.
- [10] C. Pagano, E. Granger, R. Sabourin, G. Marcialis, and F. Roli, "Adaptive ensembles for face recognition in changing video surveillance environments," Information Sciences, vol. 286, pp. 75 – 101, 2014.
- [11] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," The Scientific World Journal, pp. 1–24, 2013.
- [12] K. Killourhy and R. Maxion, "Why did my detector do that?! predicting keystroke-dynamics error rates," in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science, S. Jha, R. Sommer, and C. Kreibich, Eds. Springer Berlin / Heidelberg, 2010, vol. 6307, pp. 256–276.
- [13] R. Giot, M. El-Abed, and C. Rosenberger, "Greyc keystroke: a benchmark for keystroke dynamics biometric systems," in *IEEE Int. Conf. on Biometrics: Theory, Applications and Systems. IEEE Computer* Society, 2009, pp. 419–424.

References

- [14] R. Giot, M. El-Abed, and C. Rosenberger, “Web-based benchmark for keystroke dynamics biometric systems: A statistical analysis,” in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth Int. Conf. on*, 2012, pp. 11–15.
- [15] A. Messerman, T. Mustafic, S. Camtepe, and S. Albayrak, “Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics,” in *Biometrics (IJCB), Int. Joint Conf. on, 2011, pp. 1–8.*
- [16] T. G. Dietterich, “Ensemble methods in machine learning,” in *Proceedings of the First Int. Workshop on Multiple Classifier Systems, ser. MCS* ’00. Springer-Verlag, 2000, pp. 1–15.
- [17] L. I. Kuncheva, *Combining Pattern Classifiers: Methods and Algorithms. Wiley-Interscience, 2004.*
- [18] P. H. Pisani and A. C. Lorena, “A systematic review on keystroke dynamics,” *Journal of the Brazilian Computer Society, vol. 19, no. 4*, pp. 573–587, 2013.
- [19] P. H. Pisani, A. C. Lorena, and A. C. de Carvalho, “Adaptive approaches for keystroke dynamics,” in *Neural Networks (IJCNN), The 2015 International Joint Conference on, 2015.*
- [20] T. Stibor and J. Timmis, “Is negative selection appropriate for anomaly detection,” *ACM GECCO, pp. 321–328, 2005.*
- [21] S. T. Magalhaes, K. Revett, and H. M. D. Santos, “Password secured sites: Stepping forward with keystroke dynamics,” in *Proceedings of the*
- *International Conference on Next Generation Web Services Practices,* ser. NWESP ’05. IEEE Computer Society, 2005, pp. 293–298.
- [22] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, “The weka data mining software: An update,” *SIGKDD Explor. Newsl., vol. 11, no. 1, pp. 10–18, 2009.*
- [23] P. H. Pisani, A. C. Lorena, and A. C. Ponce de Leon Carvalho, “Adaptive algorithms in accelerometer biometrics,” in *Intelligent Systems (BRACIS), 2014 Brazilian Conference on, Oct 2014, pp. 336–341.*
- [24] H. Zhang, “The optimality of naive bayes,” in *Proceedings of the Seventeenth International Florida Artificial Intelligence Research Society Conference (FLAIRS 2004), V. Barr and Z. Markov, Eds. AAAI Press,* 2004.
- [25] J. Demˇsar, “Statistical comparisons of classifiers over multiple datasets,” *J. Mach. Learn. Res., pp. 1–30, 2006.*