

CNN-based fast source device identification: supplementary materials

Sara Mandelli, Davide Cozzolino, *Member, IEEE*, Paolo Bestagini, *Member, IEEE*, Luisa Verdoliva, *Senior Member, IEEE*, and Stefano Tubaro, *Senior Member, IEEE*

Abstract—In this document, we report additional materials about our main paper on fast source device identification by means of convolutional neural networks (CNNs). Specifically, we provide more detailed results for the closed-set problem, i.e., identifying the image source among a finite pool of devices, drawing also confusion matrices of the estimation. Moreover, we exploit the BOSARIS Toolkit to generate detailed results for the open-set problem, i.e., tackling source identification in case of *unknown* cameras. Results depict the receiver operating characteristic (ROC) curves and the detection error trade-off (DET) curves for each experiment. Furthermore, we report the equal error rate (EER), the minimum clr and the minimum DCF point of each curve. In order to give the possibility to catch even the smallest details of the shown graphics, we report at this link¹ a complete list of the MATLAB “.fig” files used to generate these materials.

I. CLOSED-SET RESULTS

The following results expand Fig. 3 reported in the original paper. For brevity’s sake, Fig. 3 draws the closed-set accuracy score A_{cs} as a function of both patch-size and required computational time. In order to ease the readability of the reported results, here we expand the reported results in two distinct figures, i.e., one depicting A_{cs} versus patch-size and another one depicting the required computation time versus patch-size.

Moreover, in order to show the effectiveness of the proposed method in differentiating among devices of the same camera model, we provide the confusion matrices of the estimation. In doing so, we consider all the 87 investigated PRNUs belonging to the closed-set pool.

S. Mandelli, P. Bestagini and S. Tubaro are with the Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano 20133, Italy (e-mail: name.surname@polimi.it).

D. Cozzolino is with the Dipartimento di Ingegneria Elettrica e Tecnologie dell’Informazione, University Federico II of Naples, 80125 Naples, Italy (e-mail: davide.cozzolino@unina.it).

L. Verdoliva is with the Dipartimento di Ingegneria Industriale, University Federico II of Naples, 80125 Naples, Italy (e-mail: verdoliv@unina.it).

This material is based on research sponsored by DARPA and Air Force Research Laboratory (AFRL) under agreement number FA8750-16-2-0173. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA and Air Force Research Laboratory (AFRL) or the U.S. Government. Hardware support was generously provided by the NVIDIA Corporation.

¹<https://github.com/polimi-ispl/cnn-fast-sdi>

A. Accuracy versus patch-size

Fig. 1 reports the behaviour of the accuracy A_{cs} as a function of the chosen crop size. The higher A_{cs} , the better the attribution.

B. Computation time versus patch-size

Fig. 2 reports the required computation time as a function of the chosen crop size.

C. Confusion matrices

Figs.3-6 report the confusion matrices achieved by PCE and the proposed CNNs in correspondence of crop size $P = 288$. For the sake of brevity, we draw results achieved by PCE (i.e., the standard approach), PCN, INC and EFB4 architectures, as the remaining CNNs report very similar results. Specifically, Fig. 3 depicts PCE results, while Fig. 4, Fig. 5, Fig. 6 draw the confusion matrices for PCN, INC and EFB4, respectively. The first 32 devices belong to Vision dataset, while the remaining 55 come from Dresden database. For what concerns Vision dataset, device nomenclature is that of [1].

II. OPEN-SET RESULTS

We resort to Bosaris Toolkit [2] to generate a complete overview of the open-set results achieved during our experimental campaign. Precisely, the following figures expand Fig. 4 reported in the original paper. Indeed, in Fig. 4, any value of accuracy AUC_{os} reports a compact evaluation metrics for the actual receiver operating characteristic (ROC) curve of the problem, which draws the relationship between true positive rate (TPR) and false positive rate (FPR). In the following lines, we show all the ROC curves that have been merged in Fig. 4.

Moreover, as suggested by [3], we also plot the detection error trade-off (DET) curves, which describe false positive rate (typically defined as false alarm rate) versus missed detection rate. Contrarily to ROC curves, DET curves are very useful to better distinguish different well performing strategies [3].

In addition to the curves, we show other compact metrics which can be useful to better evaluate the results. Specifically, we report the equal error rate (EER), the minimum clr and the minimum DCF point of each curve. Given that these metrics are very well defined in the user guide of [2], for brevity’s sake we do not provide theoretical definitions in this document. However, we refer the interested reader to [2], where a complete and thorough explanation of all these metrics is provided.

A. ROC curves

Fig. 7 reports all the ROC curves achieved for any network configuration and patch-size. The higher the curve, the more correct the detection.

B. DET curves

Fig. 8 reports all the DET curves achieved for any network configuration and patch-size. Each DET curve is associated to a minDCF point, drawn by means of the function `fast_minDCF.m` provided in [2]. To compute the minDCF point of the curve, we suppose to have equal cost of missed detections and false alarms and a target prior of 0.5. Both DET curve and minDCF point are useful to evaluate the goodness of the scores returned by the system.

C. Equal Error Rate

Fig. 9 reports the equal error rate (EER) related to each ROC curve. EER values are computed using the function `rocch2eer.m` provided in [2]. The lower the EER, the better the detection.

D. Minimum cllr

Fig. 10 reports the minimum cllr value related to each patch-size. It has been drawn by means of the function `min_cllr.m` of [2]. As the EER, the lower the value of the minimum cllr, the better the detection.

REFERENCES

- [1] D. Shullani, M. Fontani, M. Iuliani, O. Al Shaya, and A. Piva, "VISION: a video and image dataset for source identification," *EURASIP Journal on Information Security*, vol. 2017, no. 1, p. 15, 2017.
- [2] "BOSARIS Toolkit," <https://sites.google.com/site/bosaristoolkit/home>.
- [3] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET curve in assessment of detection task performance," *National Inst of Standards and Technology Gaithersburg MD*, 1997.

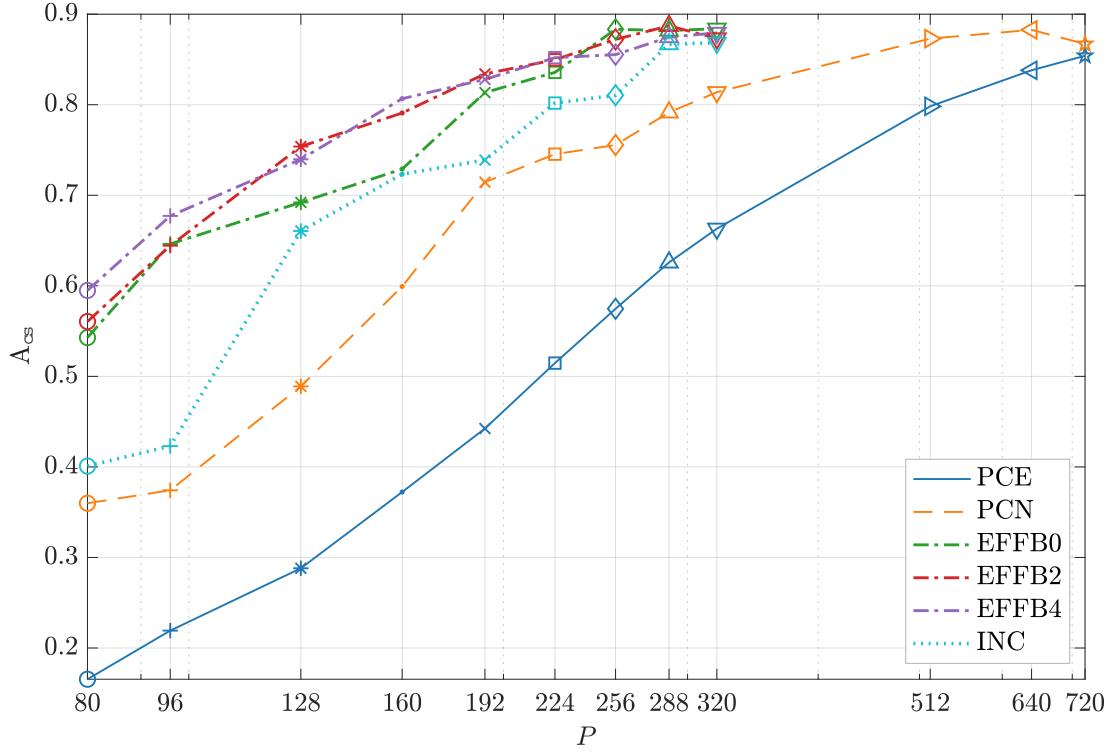


Fig. 1. Accuracy A_{cs} as a function of crop size P .

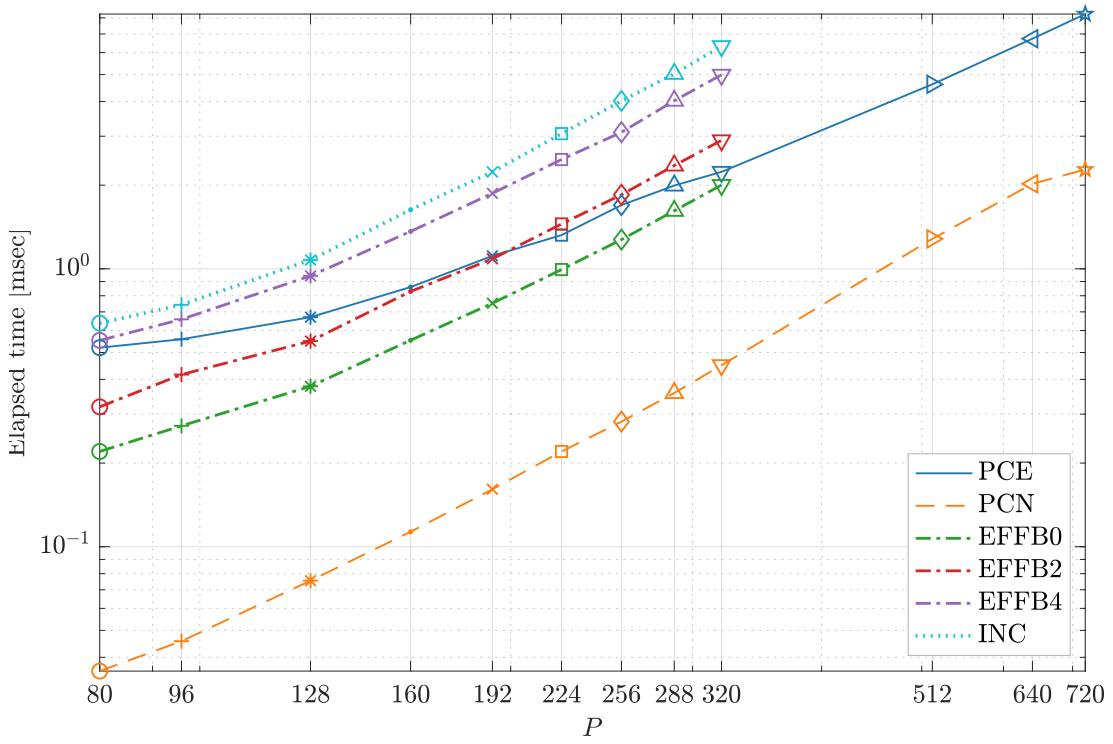


Fig. 2. Required computation time as a function of crop size P .

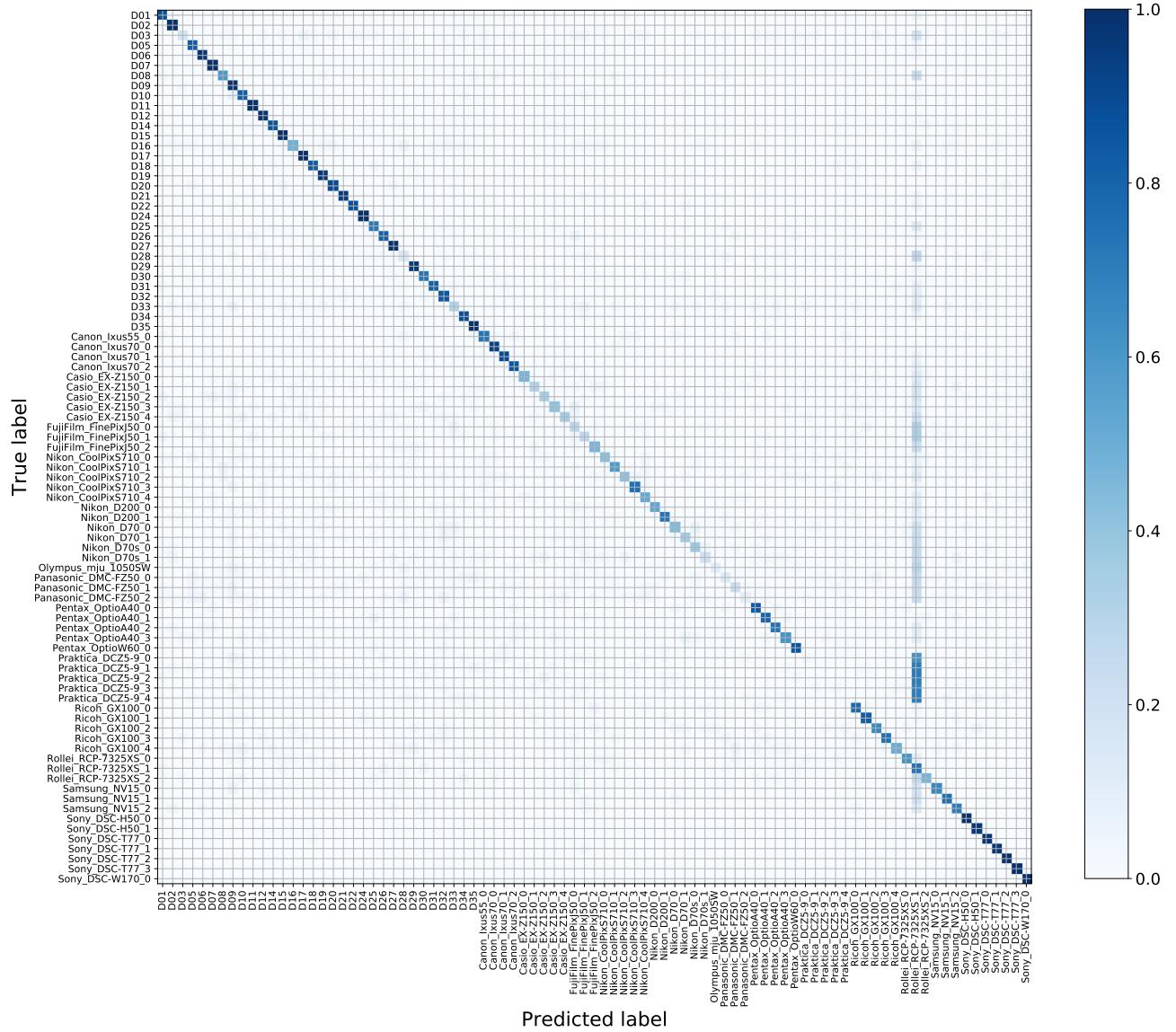


Fig. 3. Confusion matrix of the closed-set problem achieved by PCE approach, testing a patch-size $P = 288$.

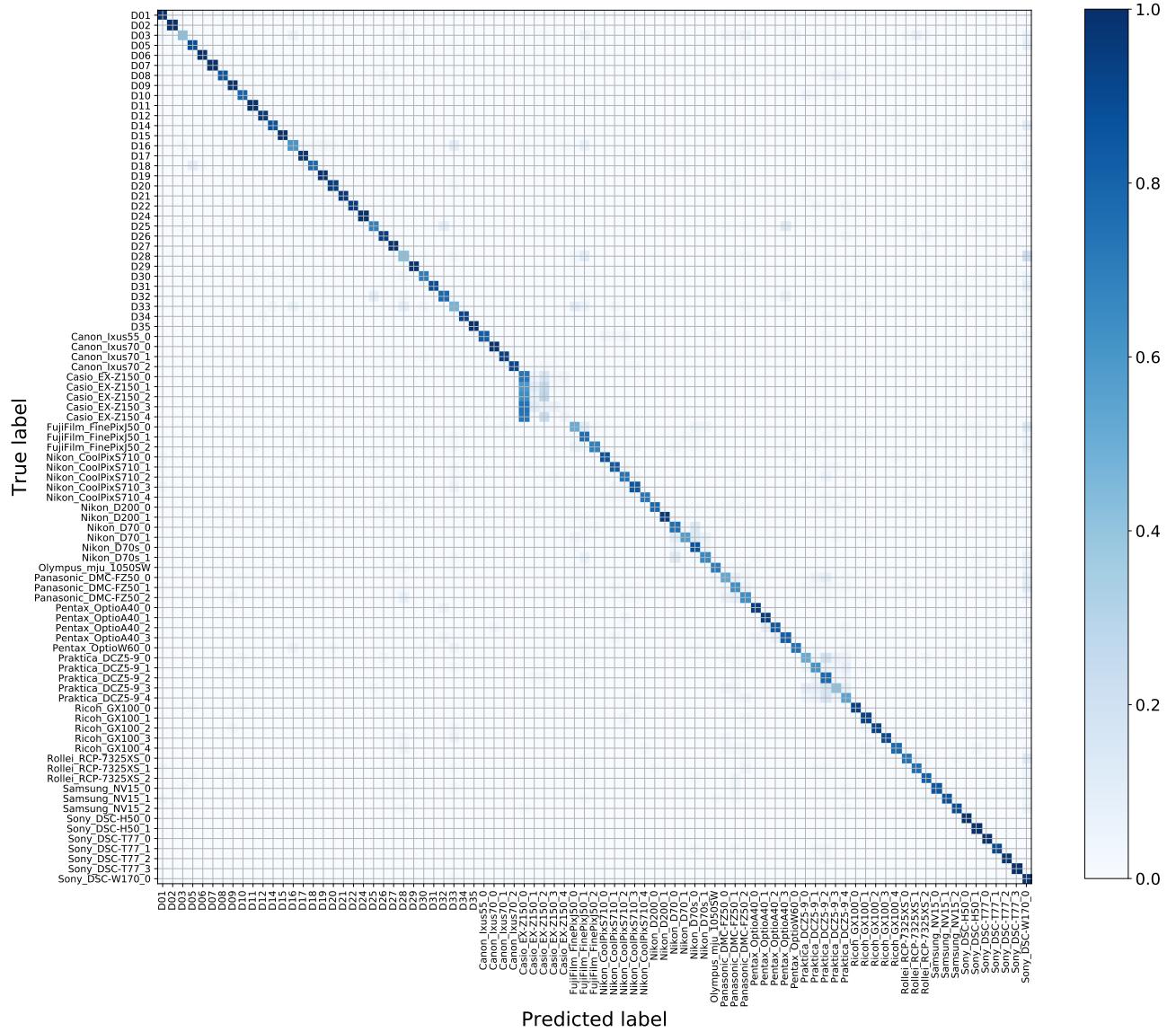


Fig. 4. Confusion matrix of the closed-set problem achieved by PCN, testing a patch-size $P = 288$.

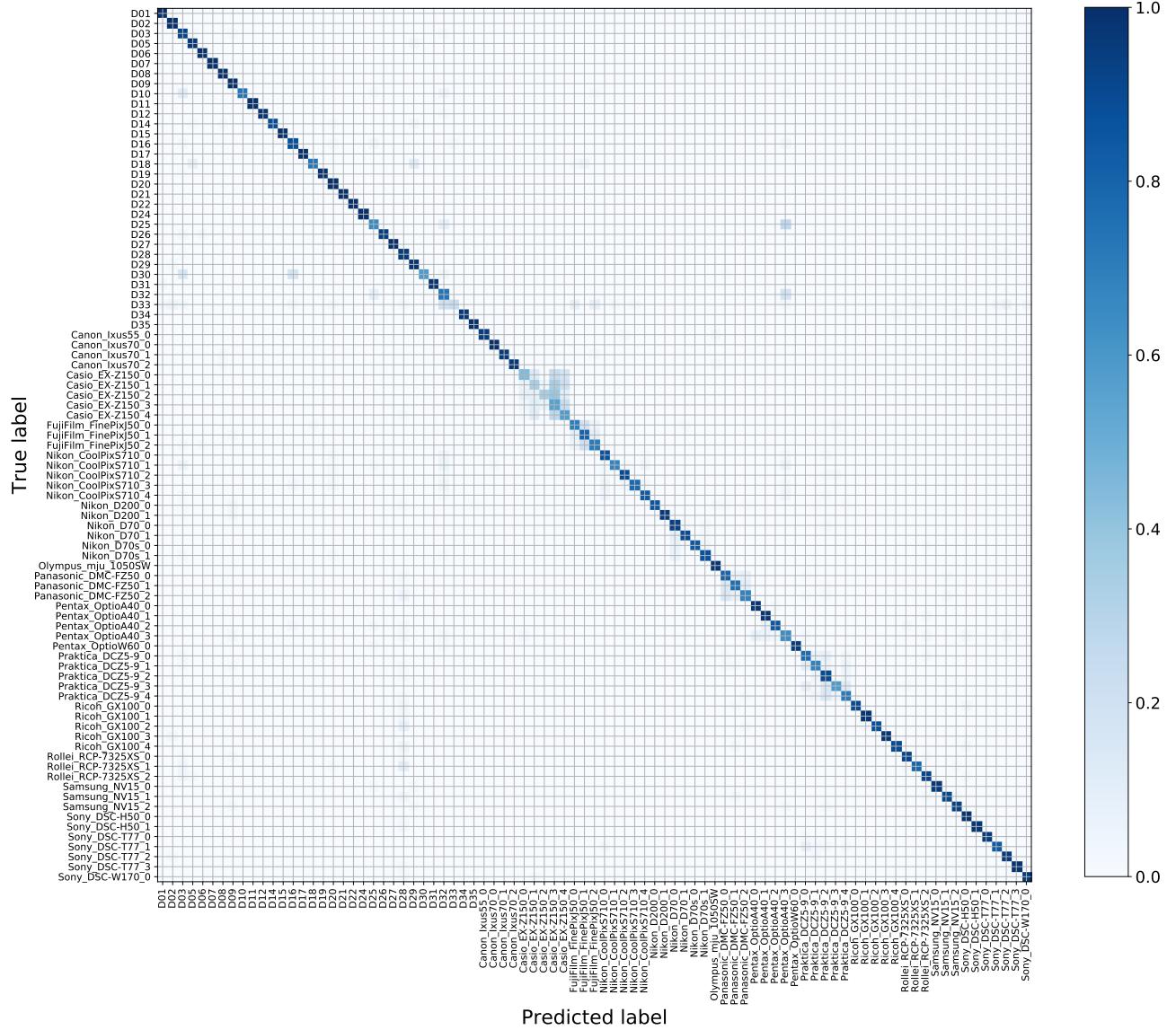


Fig. 5. Confusion matrix of the closed-set problem achieved by INC, testing a patch-size $P = 288$.

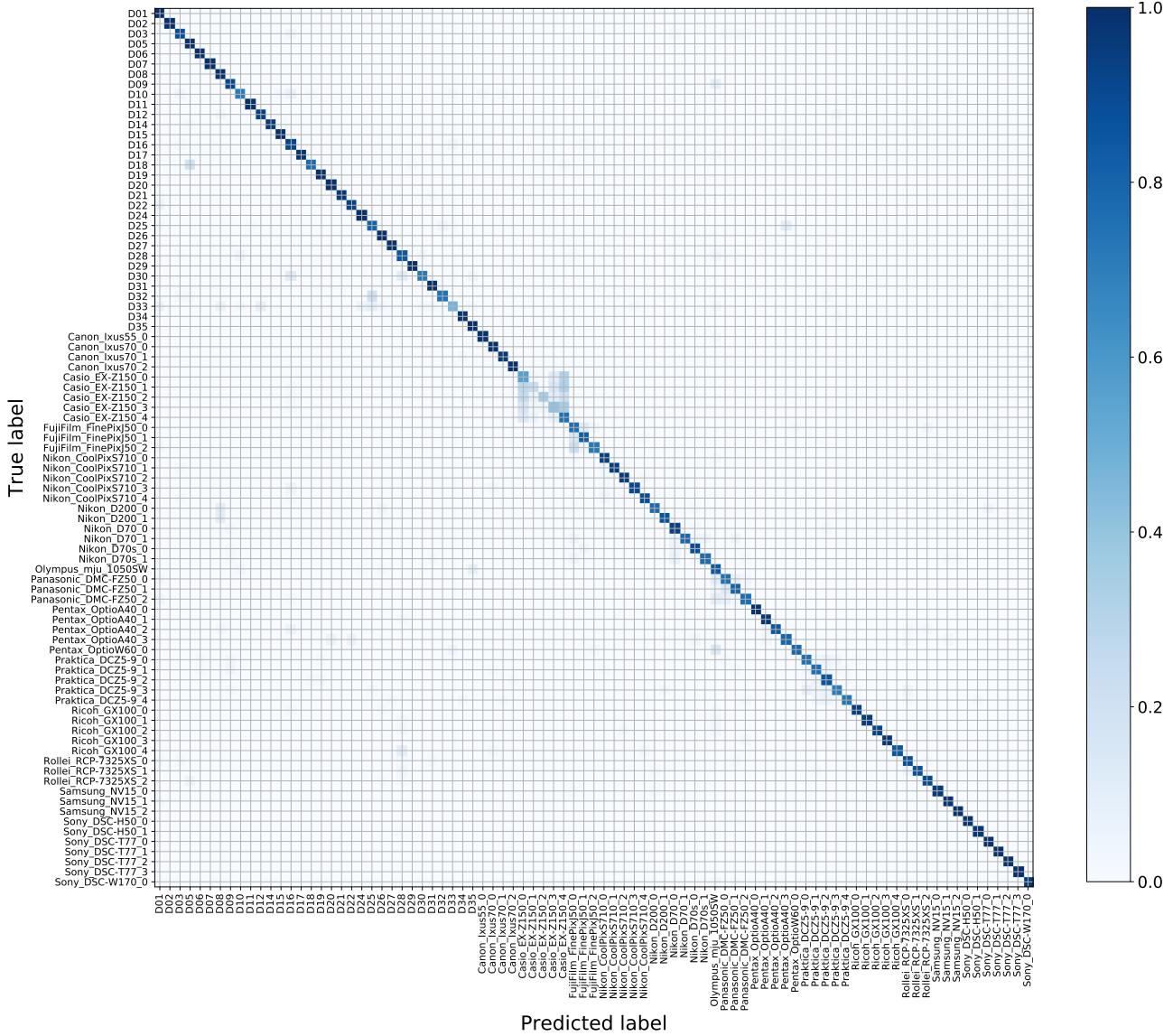


Fig. 6. Confusion matrix of the closed-set problem achieved by EBB4, testing a patch-size $P = 288$.

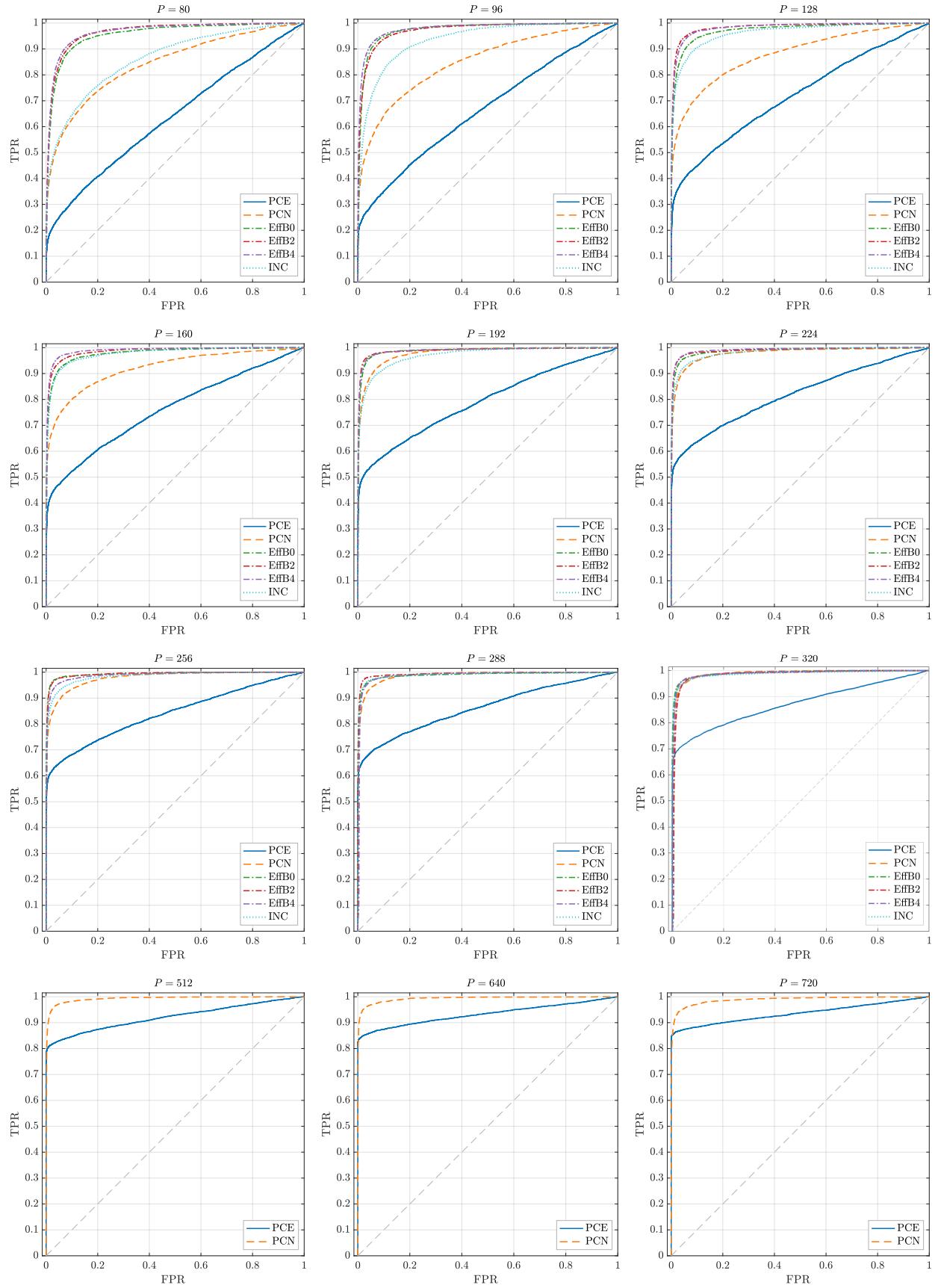


Fig. 7. ROC curves as a function of crop size P .

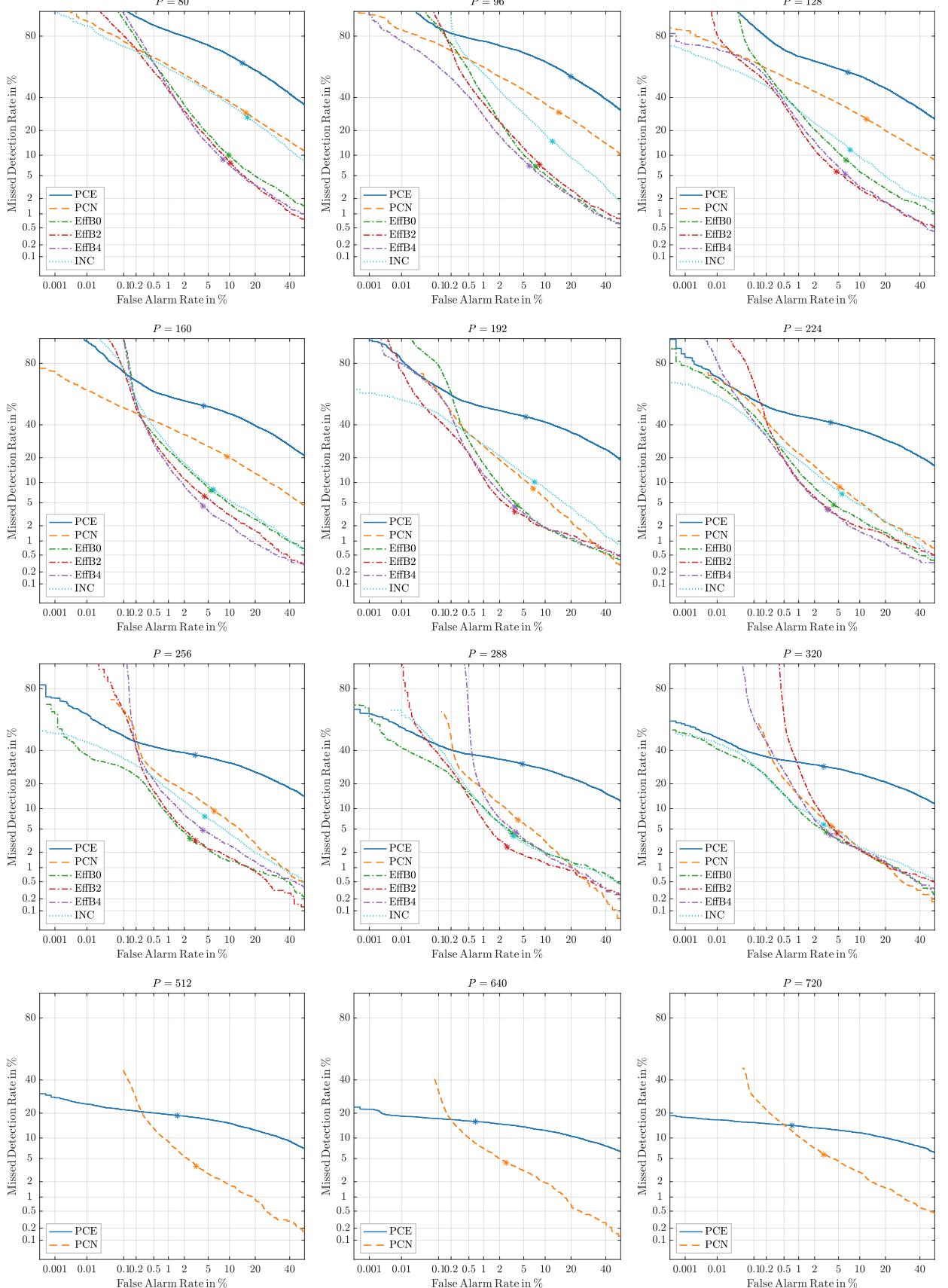


Fig. 8. DET curves as a function of crop size P . * represents the minDCF point of each curve, considering an effective prior probability equal to 0.5.

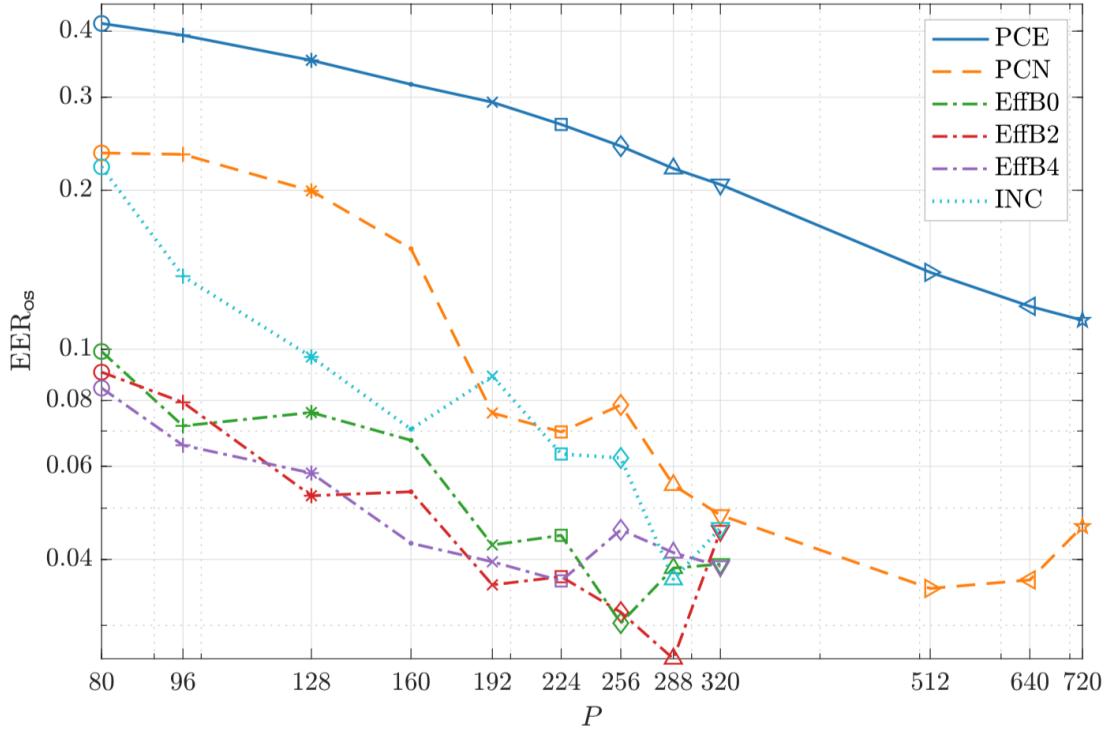


Fig. 9. Equal Error Rate of ROC curves as a function of crop size P .

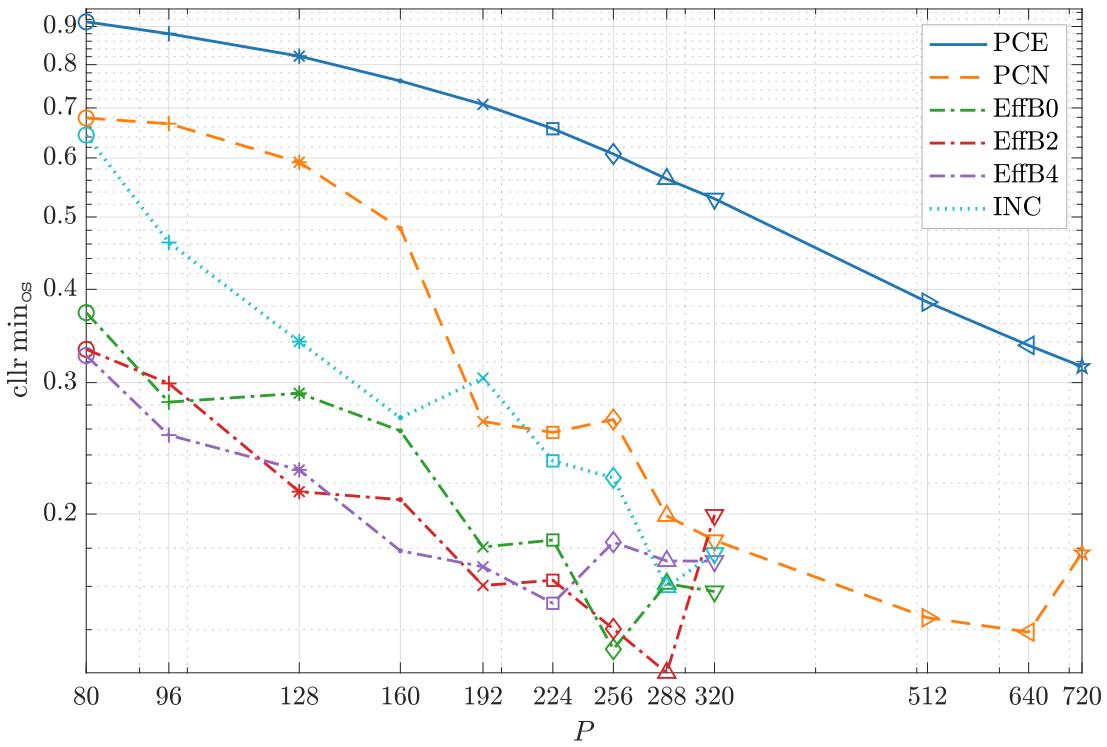


Fig. 10. Minimum value of clr measure as a function of crop size P .