Security of printed documents

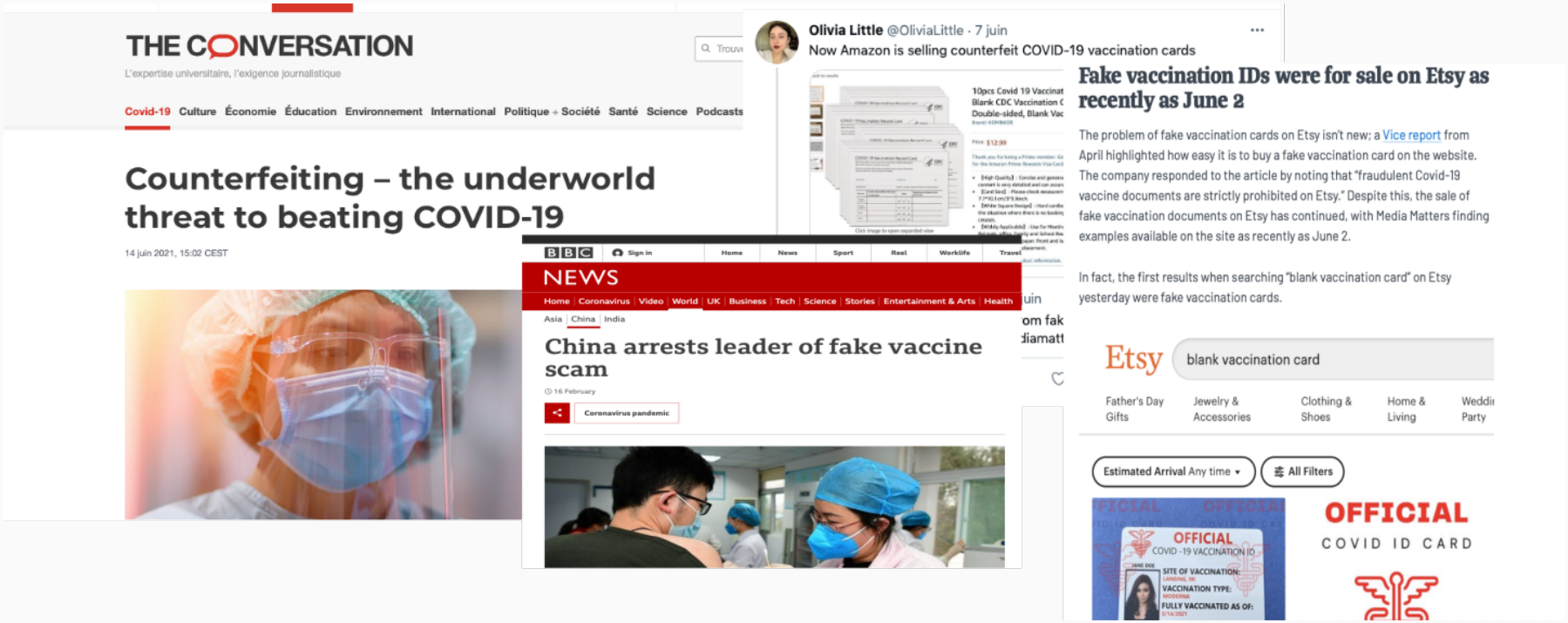
Risks of estimation attack

Iuliia Tkachenko

July 1, 2021

LIRIS, Uiversité Lumière Lyon 2, CNRS

Motivation



Counterfeiting risks

- Danger for life
- Identity theft
- Losses for the market
- Damage to the brand reputation

Document types

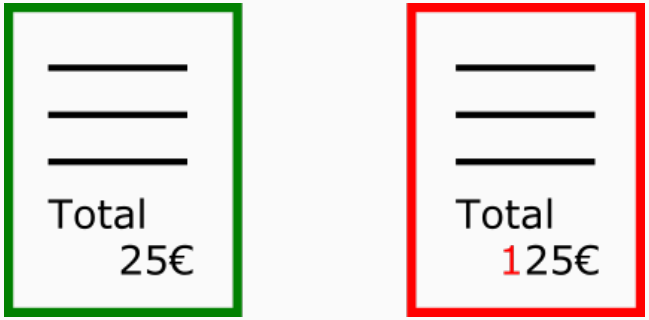
- ID documents:
  - passports
  - visas
  - professional cards
- Administrative documents:
  - invoices
  - vaccination cards
- Packaging:
  - medicines
  - cosmetics
  - wines
  - baby food

Approaches for document protection

1. Document integrity check

Approaches for document protection

1. Document integrity check

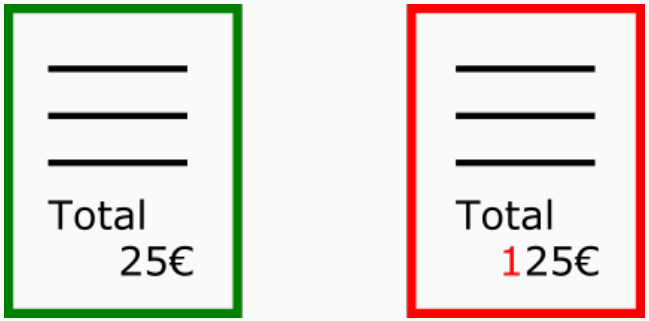


2. Anti-copy approaches

source: originalideas.info

Approaches for document protection

1. Document integrity check
2. Anti-copy approaches
   - Material unclonable characteristics
     - Measurable But Not Duplicable characteristics [Goldman *et al.*]
     - Paper PUF [Wong *et al.*]
   - Printed anti-copy elements
     - Copy detection pattern [Picard]
     - Two level QR code [Tkachenko *et al.*]
     - Watermarked QR code [Nguyen *et al.*]
   - Printer forensics

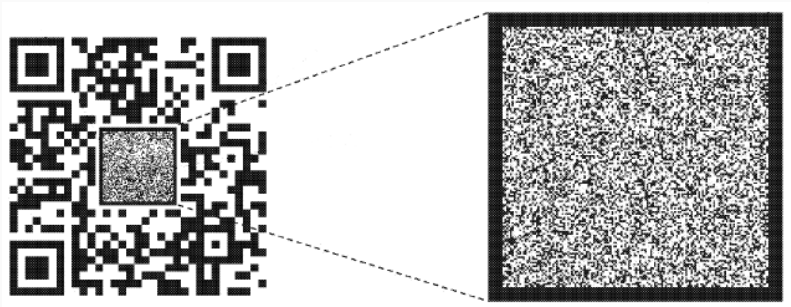


source: originalideas.info

Copy Detection Pattern (1/2)

CDP (Copy Detection Pattern) is a small random or pseudo-random digital image which is printed at an optimal resolution so that the pattern pixel distribution is significantly impacted during duplication.
CDP coverage rate is $50 \pm 5\%$.

[Picard 2004]

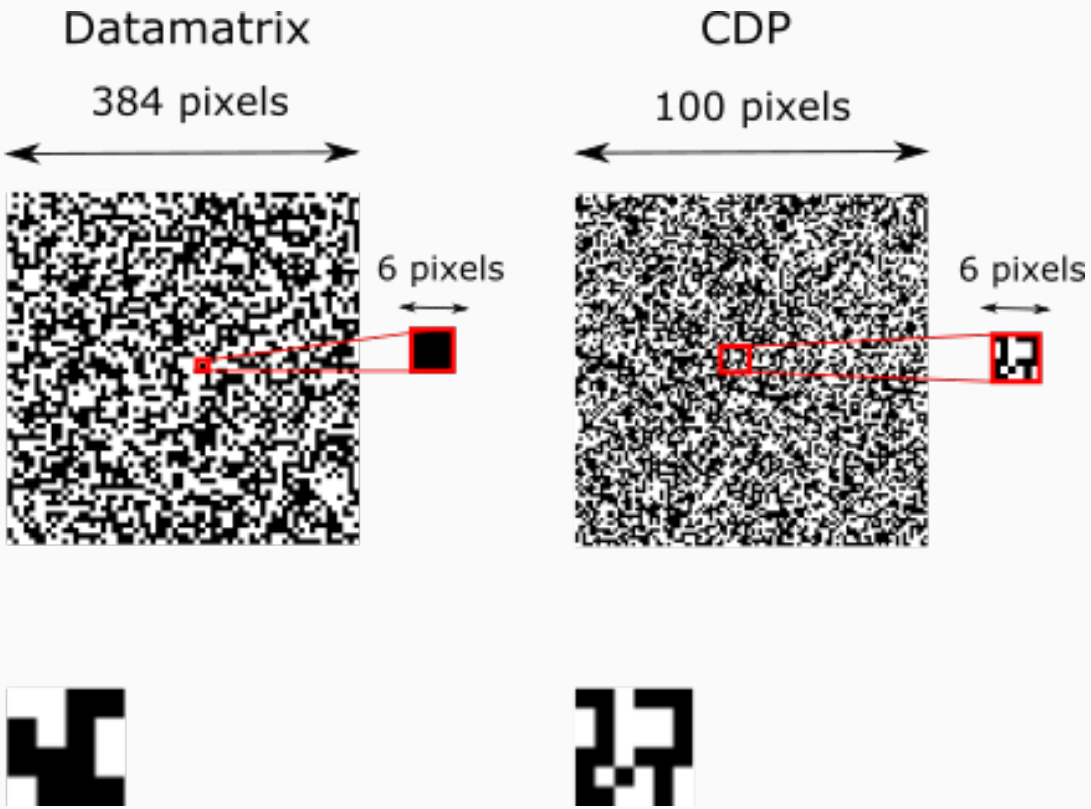


[Picard 2017]

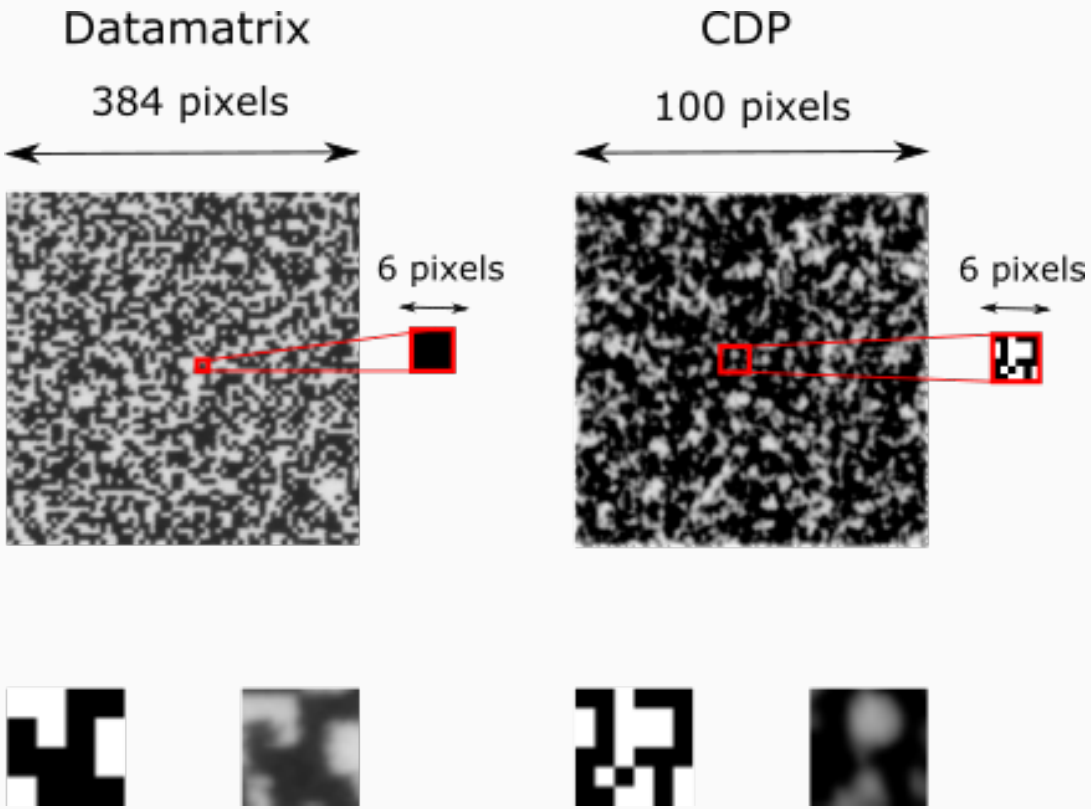
J. Picard, “Digital authentication with copy-detection patterns,”
Electronic Imaging 2004, pp. 176–183

J. Picard, P. Landry, “Two dimensional barcode and method of authentication of such barcode,”
US Patent 9 594 993, 2017.

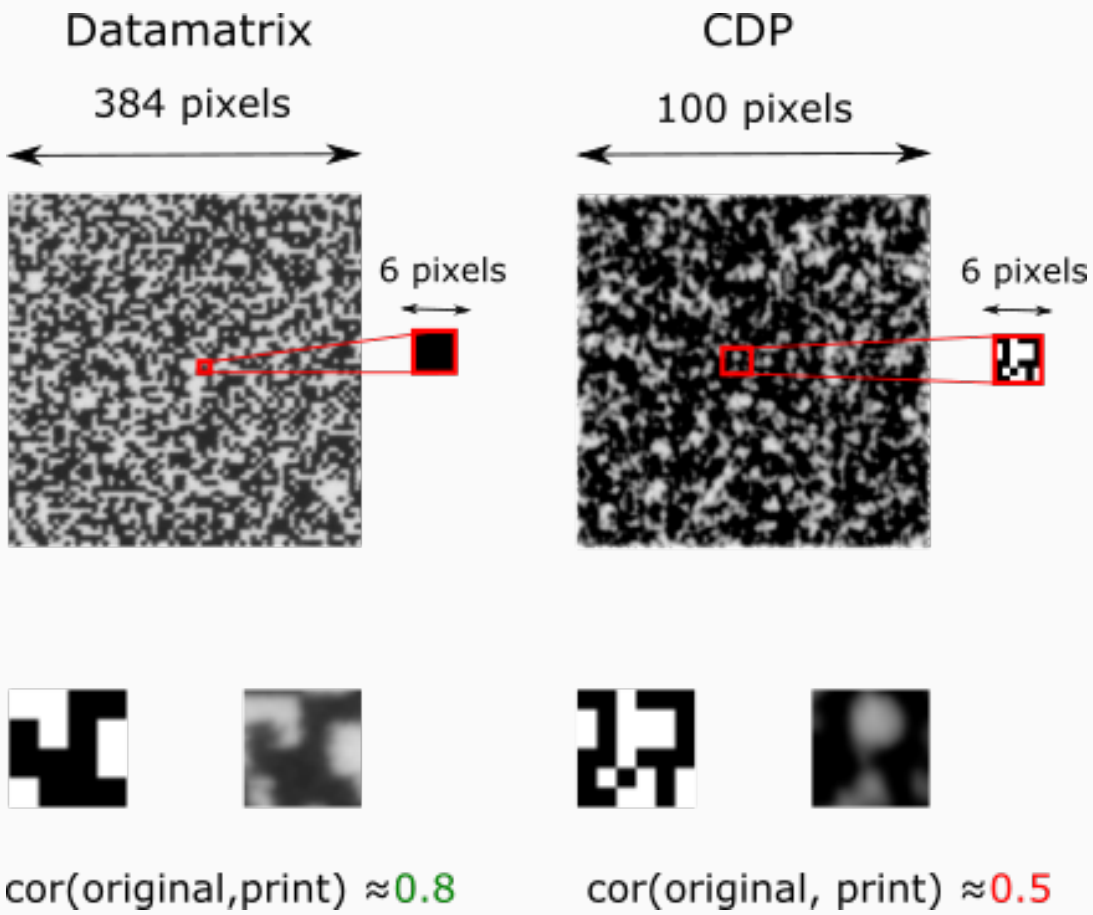
Datamatrix vs CDP: digital



Datamatrix vs CDP: printed



Datamatrix vs CDP: information loss



Copy Detection Pattern (2/2)

Authentication test : made by the comparison of the P&S version with the original digital CDP

- performed in the spatial (or frequency) domain,
- using a correlation coefficient (or a distance),
- with a predefined decision threshold.

Robust to duplication and estimation using an inverted P&S model [Dirik *et al.*].
Theoretically can be estimated from a reasonable number of genuine CDPs [Baras *et al.*].
What about estimation attack?

A.E. Dirik, B. Haas, "Copy detection pattern-based document protection for variable media," IET Image Processing 2012, 6(8), 1102–1113.

C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," EUSIPCO 2012, pp. 1760–1766.

Estimation attack

Digital CDP	I
Printed CDP	$\Pi(I)$
Captured CDP	$\tilde{I} = \Sigma(\Pi(I))$
Copy of captured CDP	$\tilde{\tilde{I}} = \Sigma(\Pi'(\Sigma'(\Pi(I)))) = \Sigma'(\Pi'(\tilde{I}))$

Estimation attack

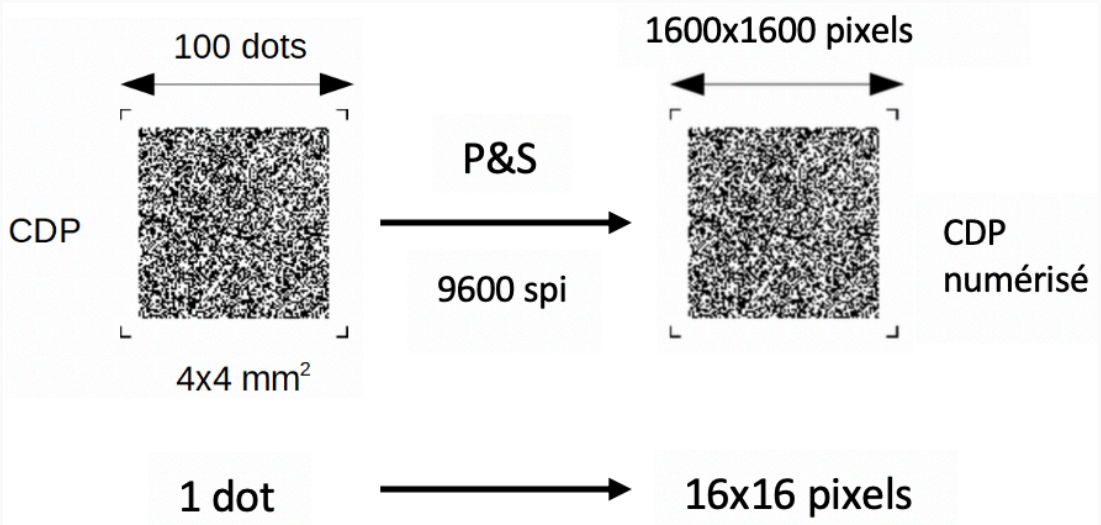
Estimated CDP	$\hat{I} = E(\Sigma'(\Pi(I)))$
Captured estimated CDP	$\tilde{\hat{I}} = \Sigma(\Pi'(\hat{I}))$

Authentication test (in case of correlation measure used) :

$$H_0 : f(I, \tilde{\hat{I}}) > Th$$

Binarization based on supervised learning (1/2)

- Each pixel of code I is represented by $n \times n$ pixels of printed code $\tilde{I}$.



- 5 types of features are extracted.
- Binarization is done by the classification of pixels (in classes "white pixels" and "black pixels") using conventional classification methods.

M. L Diong, P. Bas, C. Pelle, and W. Sawaya

Document authentication using 2D codes: Maximizing the decoding performance using statistical inference.
In IFIP International Conference on Communications and Multimedia Security. Springer, 39–54, 2012.

Binarization based on supervised learning (2/2)

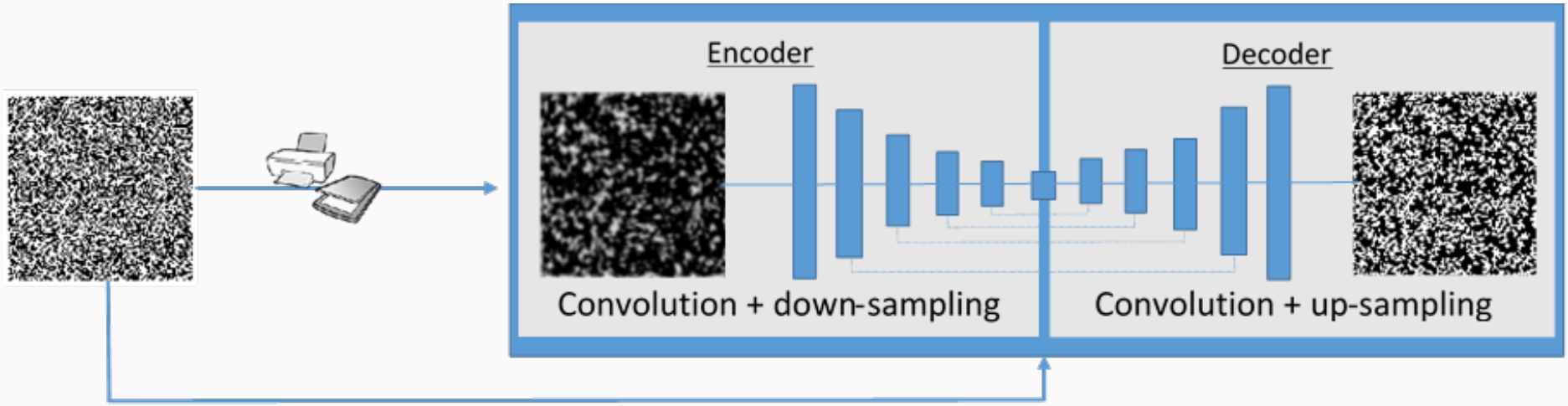
Supervised classification can dramatically increase the quality of counterfeit codes ($n = 16$).

Features	Database dimension	BER	std
LDA F3	5 images	22.60%	4.1%
QDA F3	5 images	26.00%	2.9%
Naive bayesian F3	5 images	35.00%	1.2%
K-means + SVM F3	5 images	22.10%	3.9%

M. L Diong, P. Bas, C. Pelle, and W. Sawaya

Document authentication using 2D codes: Maximizing the decoding performance using statistical inference.
In IFIP International Conference on Communications and Multimedia Security. Springer, 39–54, 2012.

Binarization based on neural network (1/2)



Database is online

`www.univ-st-etienne.fr/graphical-code-estimation`.

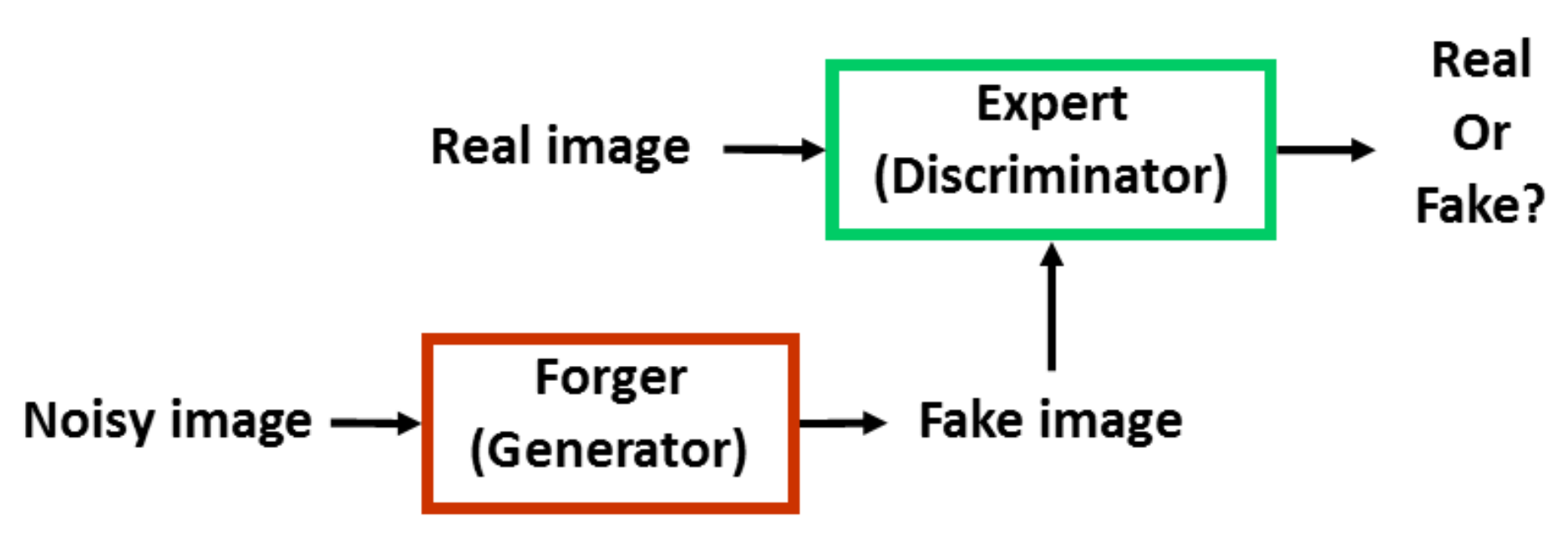
J. Calvo-Zaragoza, A.-J. Gallego

A selectional auto-encoder approach for document image binarization.
Pattern Recognition 86 (2019), 37–47, 2019.

R. Yadav, I. Tkachenko, A. Trémeau, T. Fournel

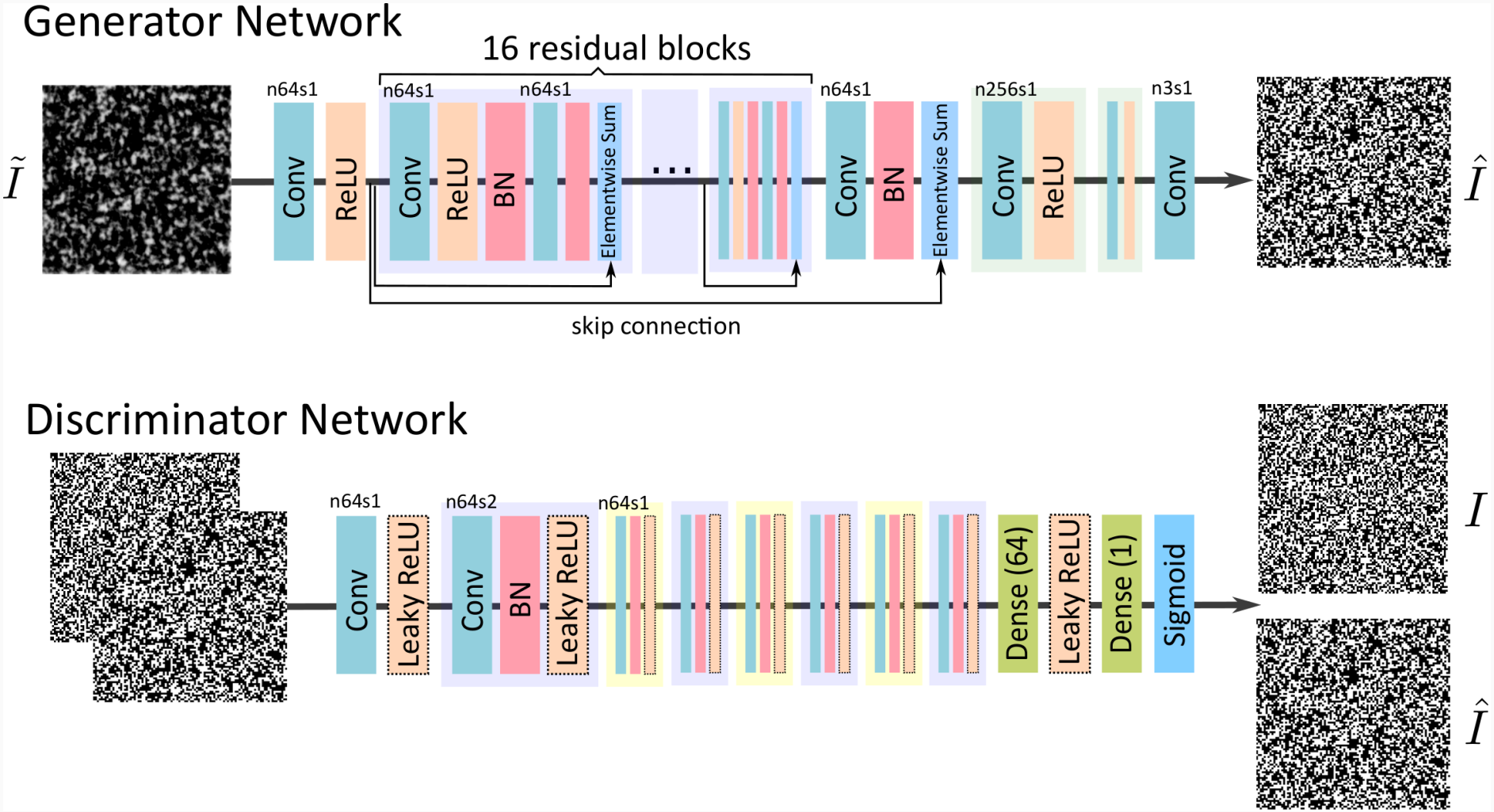
Estimation of copy-sensitive codes using a neuronal approach.
IH&MMSec 2019, July 2019, Paris, France.

Binarisation by GAN



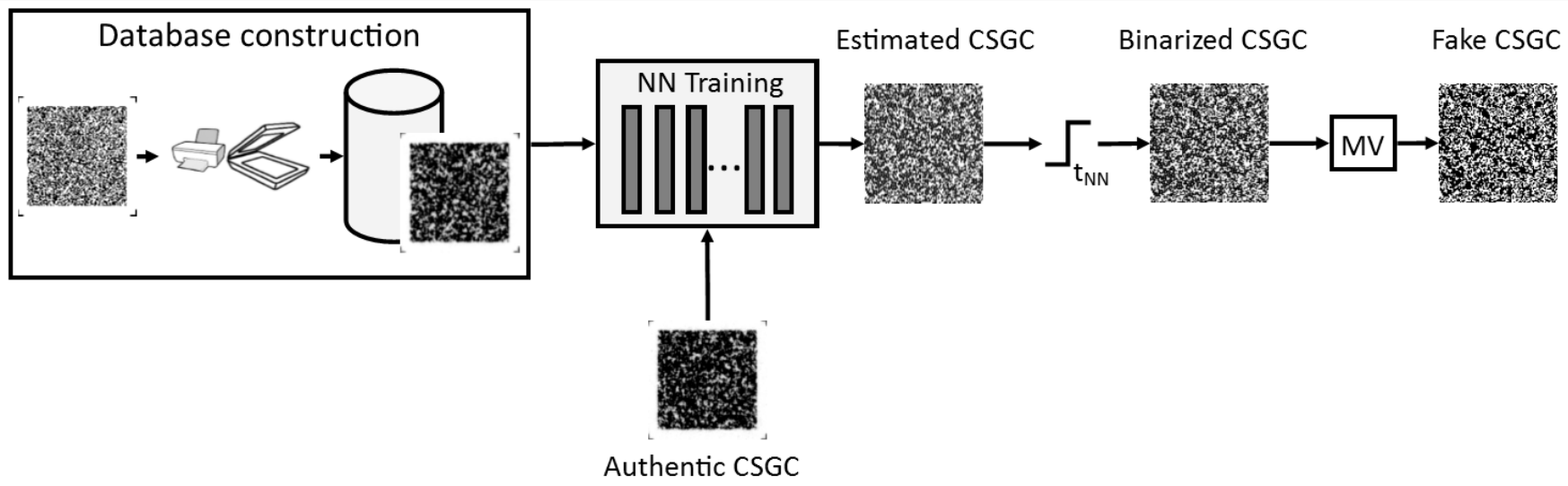
GAN architecture where a generator is trained to estimate the current real image from a noisy image, so that it can trick a discriminator trained at the same time to distinguish the real images from the estimated images.

Binarization based on neural network (2/2)



C. Ledig, L. Theis, F. Huszar, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, and Z. Wang
Photo-realistic single image super-resolution using a generative adversarial network.
In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 4681–4690, 2017.

Estimation attack pipeline



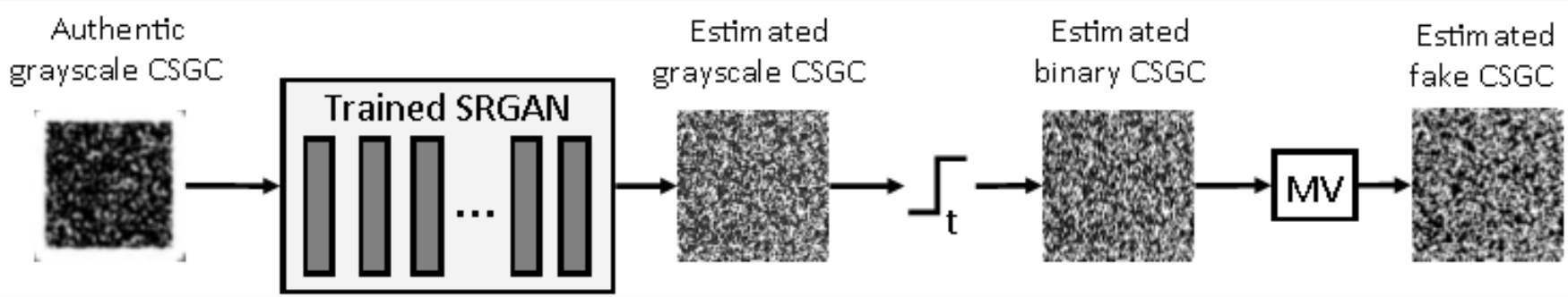
Estimation results

Method used	BER	Best BER
Elementary unit size $s = 8^2$ p/e		
LDA F3 (8×8)	26.86%	25.57%
BN DNN* (8×8)	14.2%	12.06%
SAE (8×8)	10.04%	8.32%
GAN (8×8)	**9.50%**	**7.53%**

* O. Taran, S. Bonev, and S. Voloshynovskiy

Clonability of anti-counterfeiting printable graphical codes: a machine learning approach.
In IEEE International Conference on Acoustics, Speech and Signal Processing. Brighton, United Kingdom, 2019.

Increase the resolution using SR GAN



Estimation results

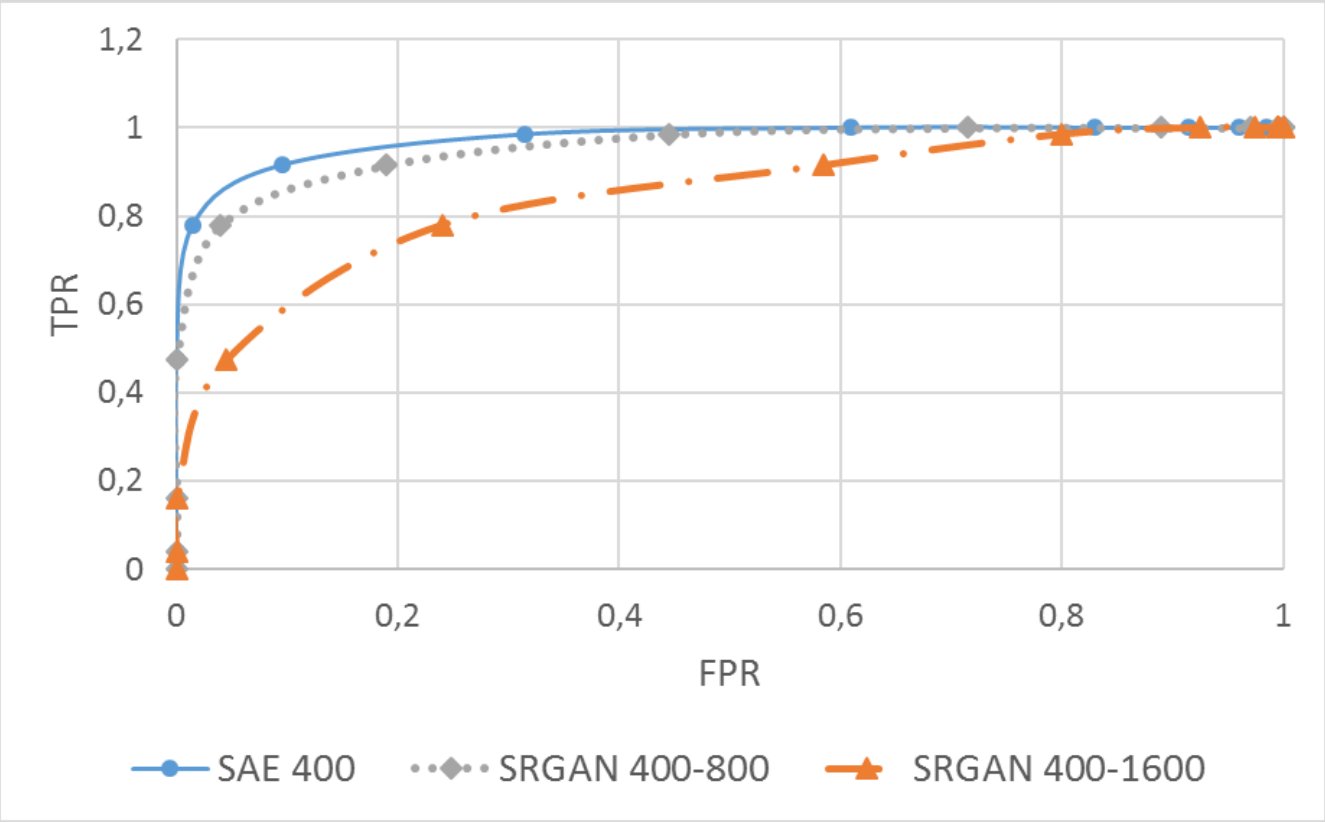
Method used	BER	Std	Best case	Worst case
SAE 400 $\longrightarrow$ 400	11.26%	1.59%	8.83%	19.84%
SRGAN 400 $\longrightarrow$ 800	**9.27%**	**1.04%**	**7.14%**	**15.47%**
SAE 800 $\longrightarrow$ 800	10.04%	0.82%	8.32%	13.65%
SRGAN 400 $\longrightarrow$ 1600	**9.18%**	**0.96%**	**7.52%**	**15.21%**
SAE 1600 $\longrightarrow$ 1600	10.42%	1.02%	8.53%	15.51%

R. Yadav, I. Tkachenko, A. Trémeau, T. Fournel

Copy sensitive graphical code estimation : Physical vs numerical resolution.

in IEEE Workshop on Information Forensics and security 2019, Delft, Netherlands.

Authentication after estimation by SR GAN



R. Yadav, I. Tkachenko, A. Trémeau, T. Fournel

Copy sensitive graphical code estimation : Physical vs numerical resolution.

in IEEE Workshop on Information Forensics and security 2019, Delft, Netherlands.

Conclusions and future work

Take home message:

- Copy-sensitive codes can help protect valuable documents or packaging from unauthorized copying.
- The estimation attack can produce fake codes.
  - A statistical approach using classical binarization methods is a bad strategy.
  - A neural network approach can produce codes that pass the authentication test.
- Good news: authentication test is not based on BER.

Future work:

- Improve the estimation results taking into account the image resolution.
- Build novel authentication test merging the anti-copy and the forensics approaches.
- Study adversarial examples while using ML authentication tests.

Special Session WIFS 2021

Special Sessions

1 – Forensics and Security of Physical Objects

Organizers

Iuliia Tkachenko (LIRIS, CNRS, Université Lumière Lyon 2, France)
Justin Picard (Scantrust)
Slava Voloshynovskiy (University of Geneva, Suisse)

Short description

Globalization and improvements in digital scanning and printing technologies have made counterfeiting more prolific and easier to perform than ever. According to a report commissioned by the International Chamber of Commerce, the entire global economy is on track to lose €3.7 trillion to counterfeiting and piracy with 5.4

https://perso.liris.cnrs.fr/itkachenko/public_html/CFP_SS_WIFS2021.pdf

We also have two open post-doc positions in LIRIS!

Questions ?

iuliia.tkachenko@liris.cnrs.fr