Clonability of printable graphical codes

a machine learning approach

Olga Taran, Slavi Bonev and Slava Voloshynovskiy

Department of Computer Science

May 16, 2019

Outline

State-of-the-art

Machine learning based attacks

Dataset of DataMatrix codes

Regeneration results

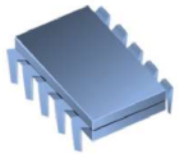
Authentication results

Conclusions

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

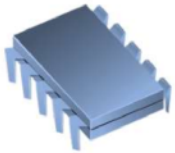
Risks of counterfeiting

- Danger for life
- Market loss
- Damage of brand reputation
- etc.

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

Risks of counterfeiting

- Danger for life
- Market loss
- Damage of brand reputation
- etc.

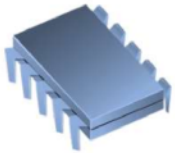
I Special printing Materials or Techniques [WCH+13, MGC+14]

- \- increases the product cost
- \+ expensive & difficult for copying

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

Risks of counterfeiting

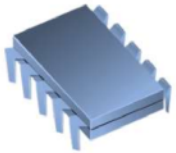
- Danger for life
- Market loss
- Damage of brand reputation
- etc.

- Special printing Materials or Techniques [WCH+13, MGC+14]
  - \- increases the product cost
  - \+ expensive & difficult for copying
- Physical Unclonable Functions *(PUFs)* [VDB+12, WW15]
  - \- verification often requires special equipment
  - \+ unclonable

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

Risks of counterfeiting

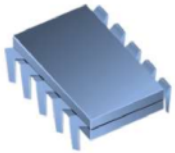
- Danger for life
- Market loss
- Damage of brand reputation
- etc.

- Special printing Materials or Techniques [WCH+13, MGC+14]
  - \- increases the product cost
  - \+ expensive & difficult for copying
- Physical Unclonable Functions *(PUFs)* [VDB+12, WW15]
  - \- verification often requires special equipment
  - \+ unclonable
- Watermarking [MNI+14, XHZT15]
  - \- anti-copying resistance is questionable

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

Risks of counterfeiting

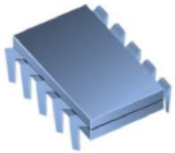
- Danger for life
- Market loss
- Damage of brand reputation
- etc.

- I Special printing Materials or Techniques [WCH+13, MGC+14]
  - \- increases the product cost
  - \+ expensive & difficult for copying
- I Physical Unclonable Functions *(PUFs)* [VDB+12, WW15]
  - \- verification often requires special equipment
  - \+ unclonable
- I Watermarking [MNI+14, XHZT15]
  - \- anti-copying resistance is questionable
- I Anti-copying Pattern [Pic04, WB08]
  - \+ claimed to be **unclonable**

State-of-the-art

ID docs

Certificates



Electronics

Banknotes

Luxury objects

Art objects

Packaging

Risks of counterfeiting

- Danger for life
- Market loss
- Damage of brand reputation
- etc.

- I Special printing Materials or Techniques [WCH+13, MGC+14]
  - \- increases the product cost
  - \+ expensive & difficult for copying
- I Physical Unclonable Functions *(PUFs)* [VDB+12, WW15]
  - \- verification often requires special equipment
  - \+ unclonable
- I Watermarking [MNI+14, XHZT15]
  - \- anti-copying resistance is questionable
- I Anti-copying Pattern [Pic04, WB08]
  - ? is it really **unclonable**?

State-of-the-art

Figure 1: Example of traditional 2D codes.

- Traditional codes are used to encode product info that is used for tracking and tracing

State-of-the-art

Figure 1: Example of traditional 2D codes.

- Traditional codes are used to encode product info that is used for tracking and tracing
- However they are clonable

State-of-the-art

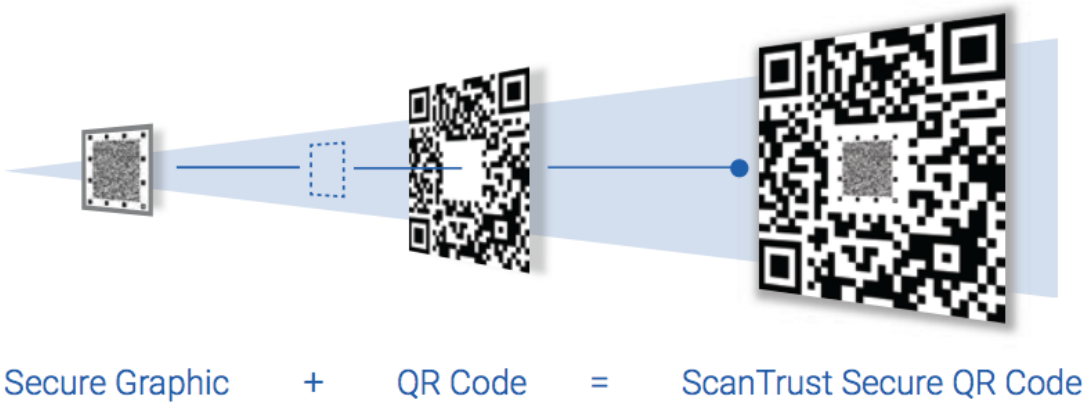


Figure 2: Example of ScanTrust QR code [\§§q I¤¤°°°u H9j§}« §uHnh].

State-of-the-art

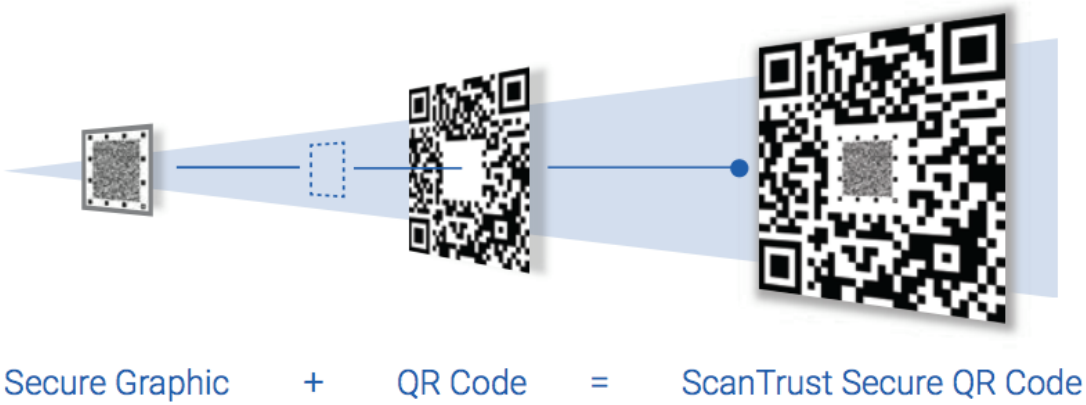


Figure 2: Example of ScanTrust QR code [\§§q I¤¤°°°u H9j§}« §uHnh].

- These codes referred to as Printable Graphical Codes (PGC) are used to distinguish authentic product from fakes and are claimed to be **unclonable** under **hand-crafted** attacks

State-of-the-art

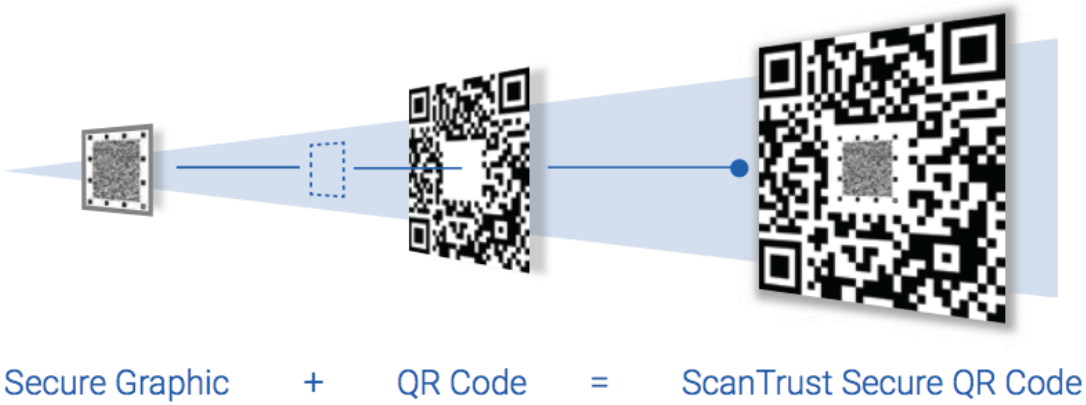


Figure 2: Example of ScanTrust QR code [\§§q I¤¤°°°u H9j§}« §uHnh].

- These codes referred to as Printable Graphical Codes (PGC) are used to distinguish authentic product from fakes and are claimed to be **unclonable** under **hand-crafted** attacks
- What about **machine learning based attacks**?

Machine learning based attacks

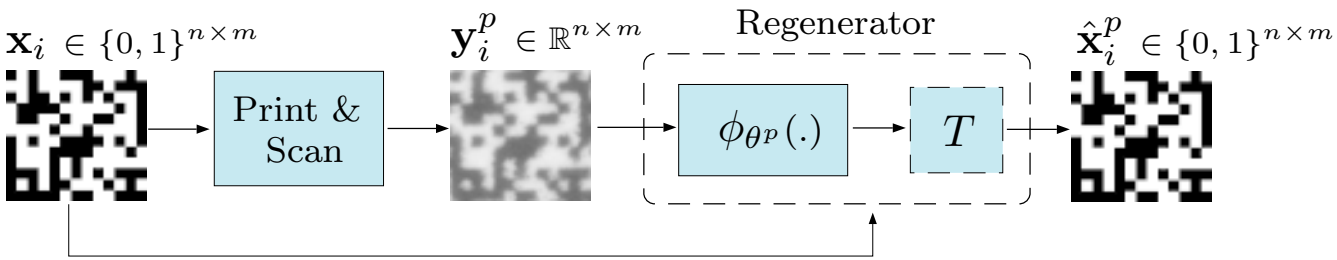


Figure 3: Training procedure based on training samples $f\mathbf{x}_i, \mathbf{y}_i^p g_{i=1}^M$ (p - printer type, M - number of training samples and T - thresholding).

Machine learning based attacks

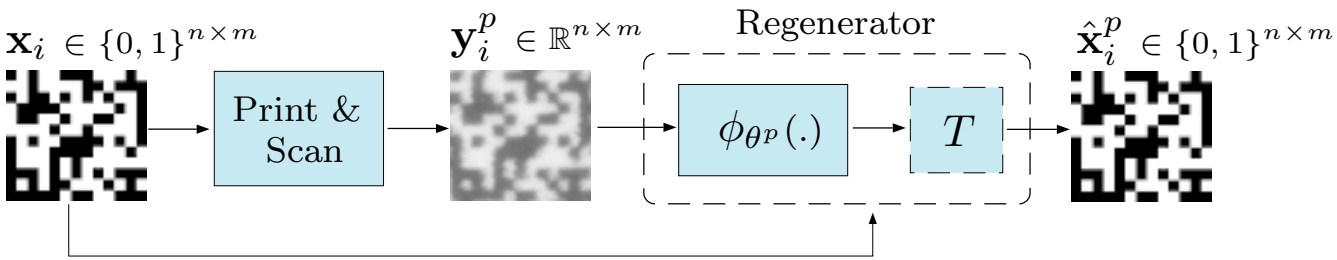


Figure 3: Training procedure based on training samples $f\mathbf{x}_i; \mathbf{y}_i^p g_{i=1}^M$ (p - printer type, M - number of training samples and T - thresholding).

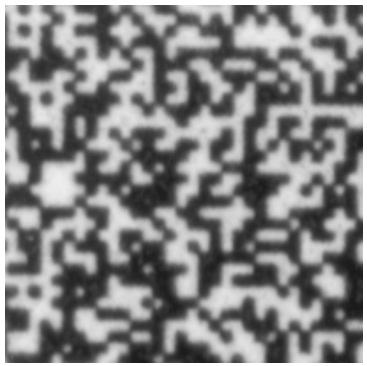
Training:

$$\wedge^p = \arg\min_p \mathbb{X}^{M} L\ \mathbf{x}_i; T(\ _p(\mathbf{y}_i^p)) + \ _p(\ ^p) \quad (1)$$

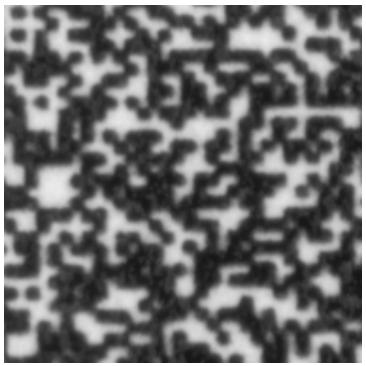
where $L(:)$ is a loss function, $_p$ is a trained model, ^{p} represents the parameters of the trained model for a printer p and $_p(:)$ is a regularizer for the model parameters.

Dataset of *DataMatrix* codes

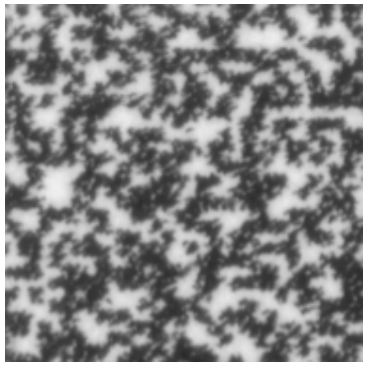
- Printers:
  - *Laser:* Samsung Xpress 430 (*SA*) 600 dpi
  - *Laser:* Lexmark CS310 (*LX*) 1200 dpi
  - *Inkjet:* Canon PIXMA iP7200 (*CA*) 600 dpi
  - *Inkjet:* HP OfficeJet Pro 8210 (*HP*) 1200 dpi



SA



LX

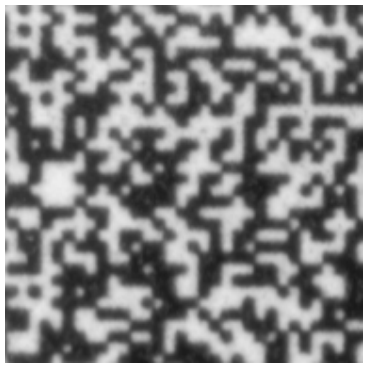


CA

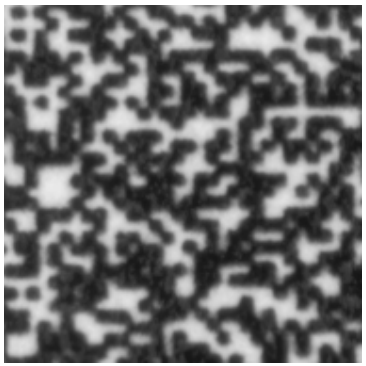
HP

Dataset of *DataMatrix* codes

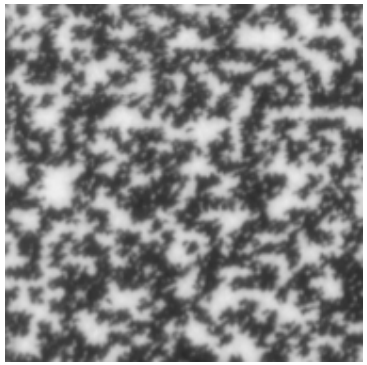
- Printers:
  - *Laser:* Samsung Xpress 430 (*SA*) 600 dpi
  - *Laser:* Lexmark CS310 (*LX*) 1200 dpi
  - *Inkjet:* Canon PIXMA iP7200 (*CA*) 600 dpi
  - *Inkjet:* HP OfficeJet Pro 8210 (*HP*) 1200 dpi
- Scanners:
  - Epson V850 Pro at 1200 ppi



SA



LX

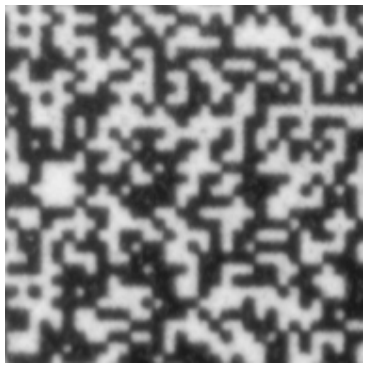


CA

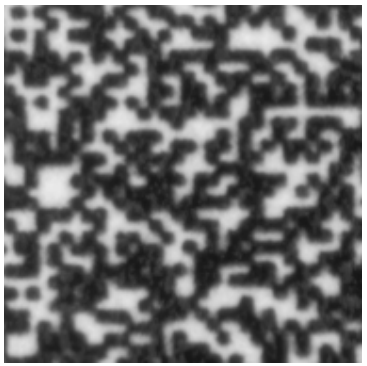
HP

Dataset of *DataMatrix* codes

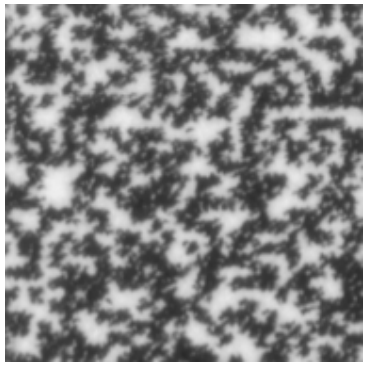
- Printers:
  - *Laser:* Samsung Xpress 430 (*SA*) 600 dpi
  - *Laser:* Lexmark CS310 (*LX*) 1200 dpi
  - *Inkjet:* Canon PIXMA iP7200 (*CA*) 600 dpi
  - *Inkjet:* HP OfficeJet Pro 8210 (*HP*) 1200 dpi
- Scanners:
  - Epson V850 Pro at 1200 ppi
- 384 codes of size 384 × 384 per printer
  - training 100 images:
    25600 sub-images of size 24 × 24
  - validation 50 images:
    12800 sub-images of size 24 × 24
  - test 224 images:
    59904 sub-images of size 24 × 24



SA



LX



CA

HP

Deep FC regenrator

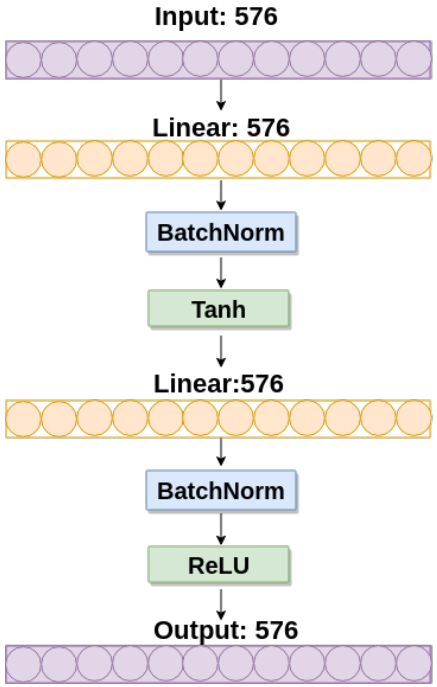


Figure 4: FC 2 layers.

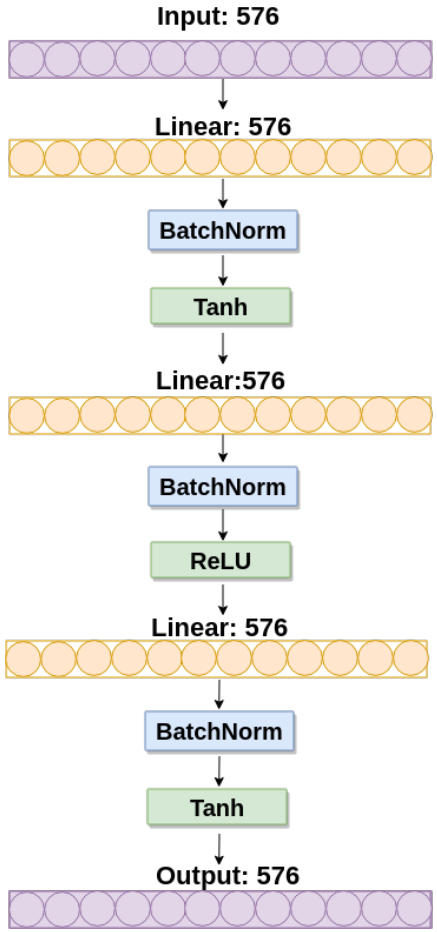


Figure 5: FC 3 layers.

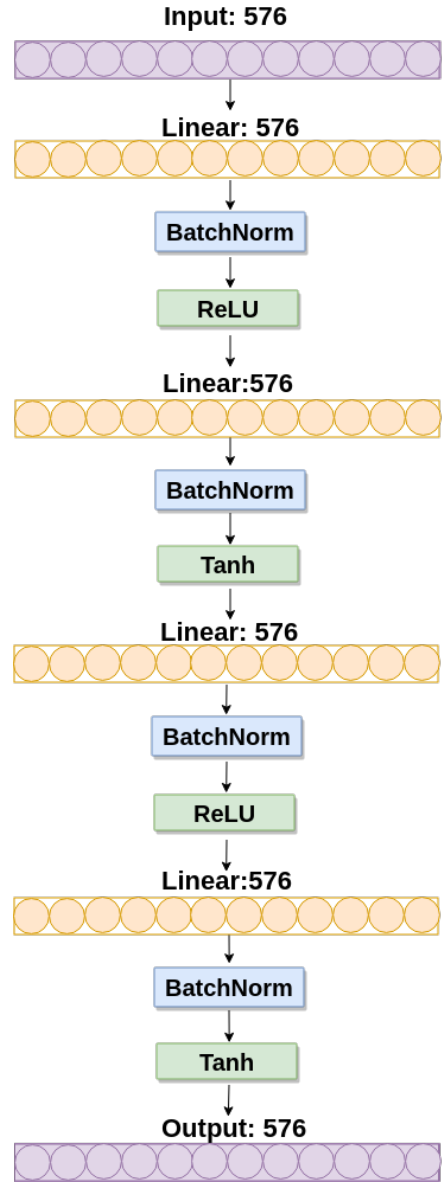


Figure 6: FC 4 layers.

Deep BN regenrator

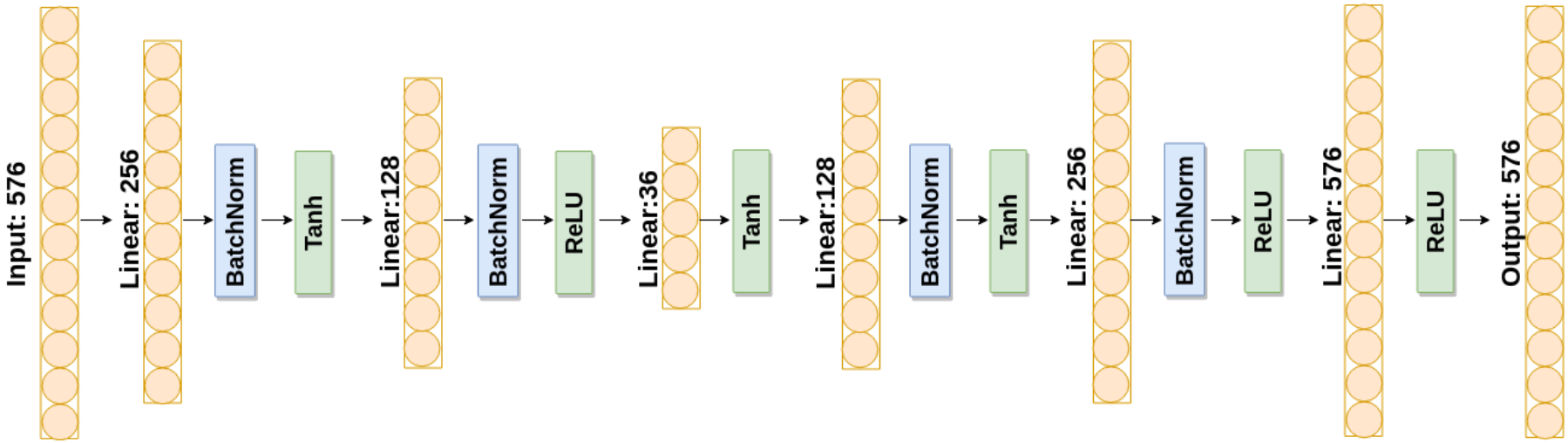


Figure 7: Deep BN regenrator architecture.

Regeneration metrics

- Hamming distance: $\mathbf{x} \in \{0;1\}^{n \times m}$, $\mathbf{y}^p \in \mathbb{R}^{n \times m}$, $T_{t^p}(:)$ - binarization function: (”hard” coding)

$$d(\mathbf{x};\mathbf{y}^p) = \frac{1}{n \cdot m} \sum_{j=1}^{n \cdot m} \mathbf{x}(j) \quad T_{t^p}(\mathbf{y}^p(j)) \tag{2}$$

Regeneration metrics

- Hamming distance: $\mathbf{x} \; 2 \; f0; 1g^{n \quad m}$, $\mathbf{y}^p \; 2 \; \mathrm{R}^{n \quad m}$, $T_{t^p}(:)$ - binarization function: (”hard” coding)

$$d(\mathbf{x}; \mathbf{y}^p) = \frac{1}{n \quad m} \sum_{j=1}^{n \; m} \mathbf{x}(j) \quad T_{t^p}(\mathbf{y}^p(j)) \tag{2}$$

- Pearson correlation [PHMHSB13]: $\mathbf{x} \; 2 \; f0; 1g^{n \quad m}$, $\mathbf{y}^p \; 2 \; \mathrm{R}^{n \quad m}$: (”soft” coding)

$$(\mathbf{x}; \mathbf{y}^p) = \frac{cov(\mathbf{x}; \mathbf{y}^p)}{\mathbf{x} \quad \mathbf{y}^p} \tag{3}$$

Regeneration results

Method	*SA*	*LX*	*HP*	*CA*
		Pearson correlation		
Thr	0.774	0.766	0.742	0.704
FC 2	0.995	0.994	0.982	0.981
FC 3	0.994	0.994	0.982	0.983
FC 4	0.994	0.995	0.981	0.982
BN	**0.996**	**0.996**	**0.986**	**0.984**
		normalized Hamming distance		
Thr	11	12	13	15
FC 2	0.22	0.24	0.93	0.98
FC 3	0.23	0.24	0.90	0.85
FC 4	0.24	0.23	0.95	0.90
BN	**0.21**	**0.22**	**0.69**	**0.76**

Table 1: Regeneration results with respect to original codes.

Results visualisation

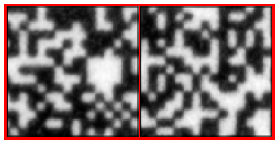
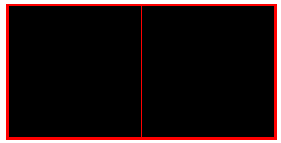
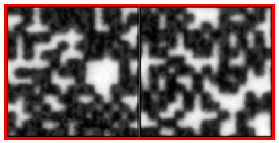
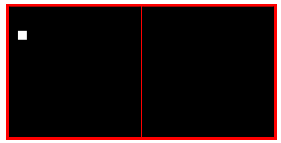
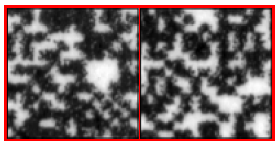
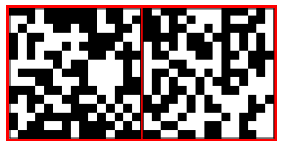
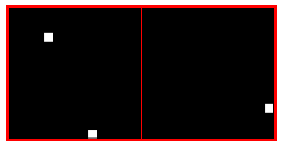
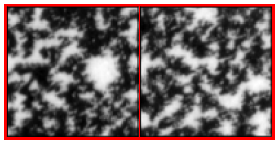
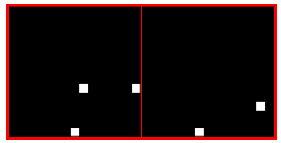
	Printer	Original	Scanned original	Reconstructed (BN)	Difference
Laser printers	SA				
	LX				
Inkjet printers	HP				
	CA				

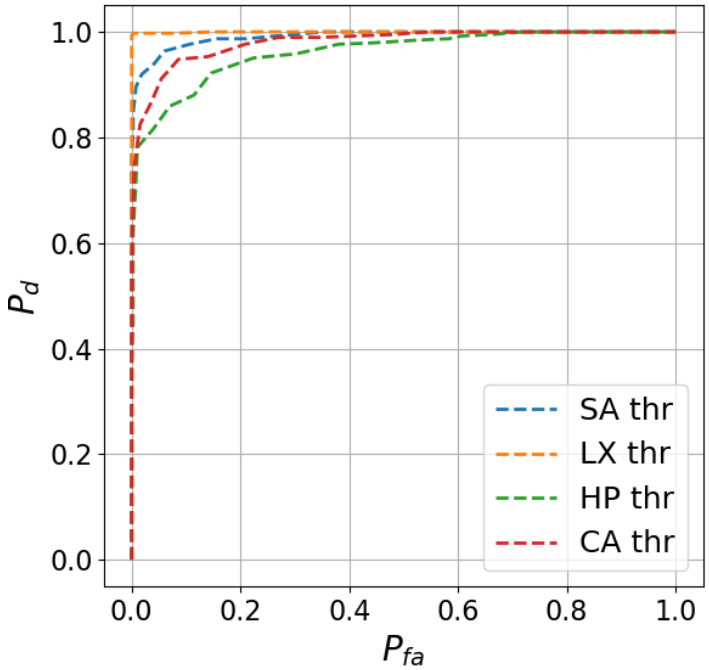
Table 2: Examples of attacks against PGC: two samples of scanned codes, the estimates produced by BN model and the difference between the original and attacked codes.

Authentication metrics

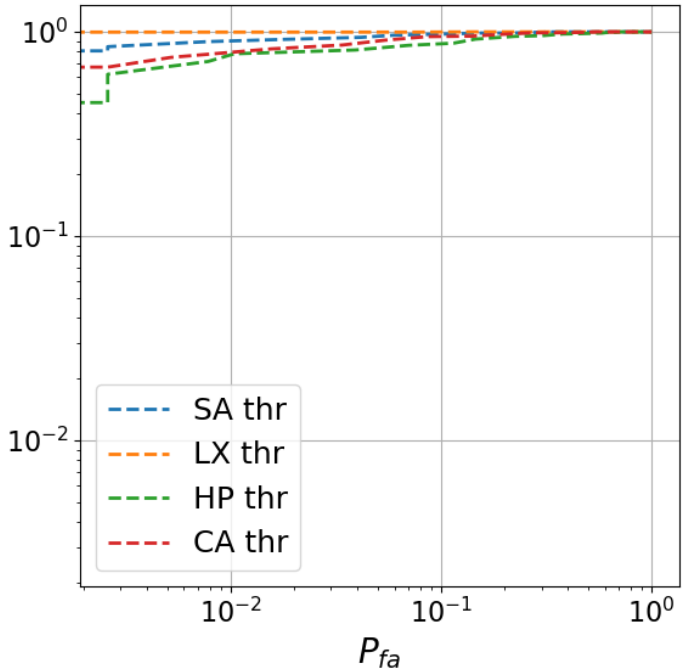
$$
\begin{aligned}
P_d &= \Pr f \quad d(\mathbf{x}_i; \mathbf{y}_i^p) \quad jH_0 g \\
P_{fa} &= \Pr f \quad d(\mathbf{x}_i; \mathbf{y}_i^p) < jH_1 g;
\end{aligned}
\tag{4}
$$

where is the threshold, $d(:)$ is a similarity measure between the original and printed codes, H_0 corresponds to the hypothesis that $\mathbf{y}_i^p$ is an authentic code and H_1 is the hypothesis that $\mathbf{y}_i^p$ is a fake (cloned) code, equals to -1 for the $Pearson\ correlation$ and to 1 for $Hamming\ distance$.

Authentication results



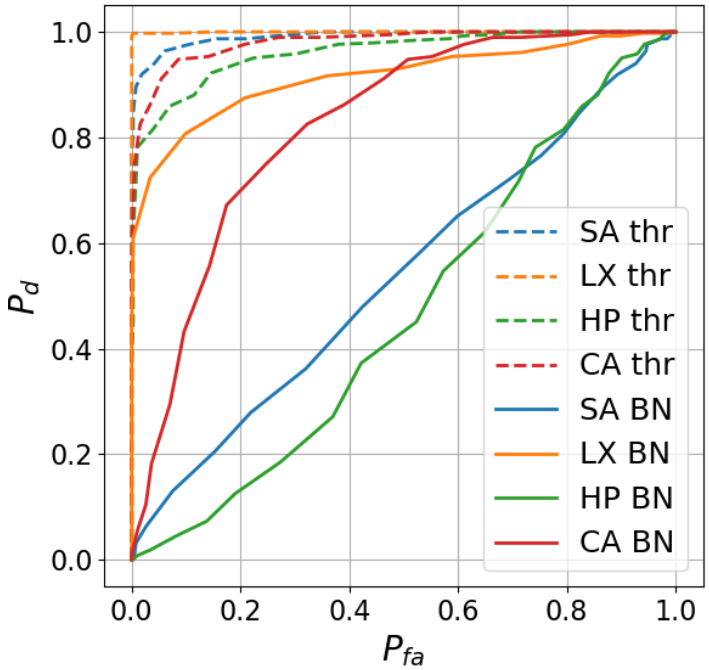
(a) Hamming distance



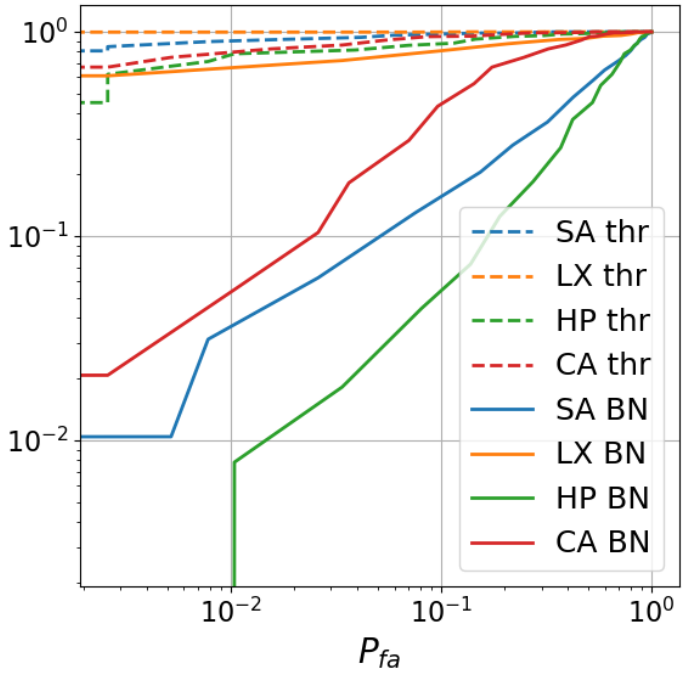
(b) Hamming distance: log scale

Figure 8: The ROC curves for$Hamming\ distance$ between the original and fake printed codes estimated via ¦ \} methods. P_d denotes the probability of the correct detection and P_{fa} is the probability of false acceptance.

Authentication results



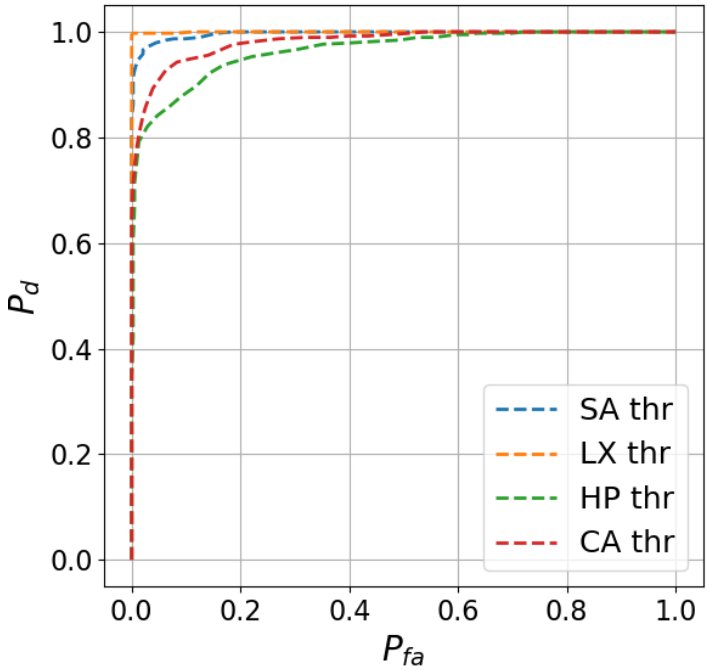
(a) Hamming distance



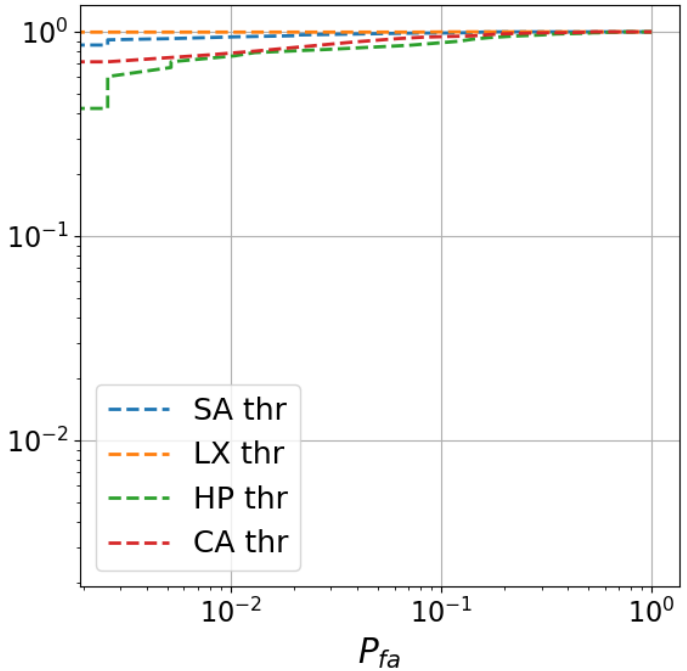
(b) Hamming distance: log scale

Figure 9: The ROC curves for $Hamming\ distance$ between the original and fake printed codes estimated via $?i$ and ¦\} methods. P_d denotes the probability of the correct detection and P_{fa} is the probability of false acceptance.

Authentication results



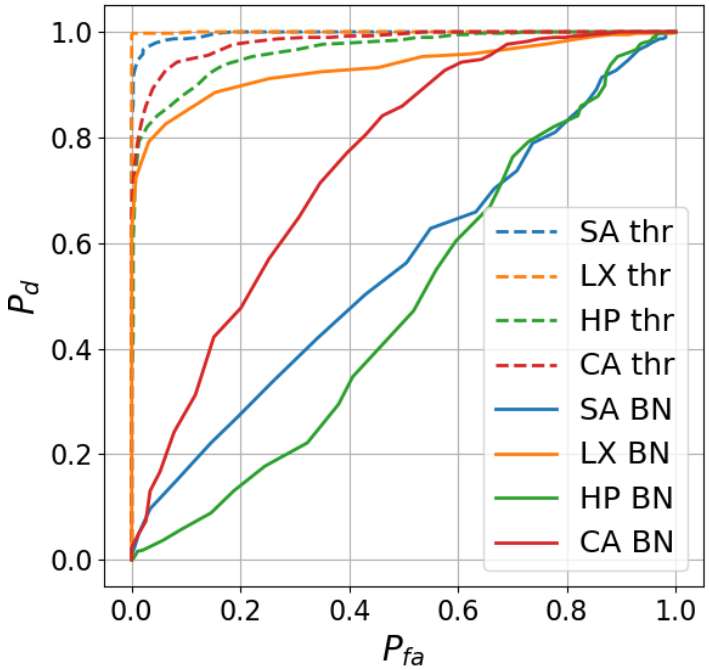
(a) Pearson correlation



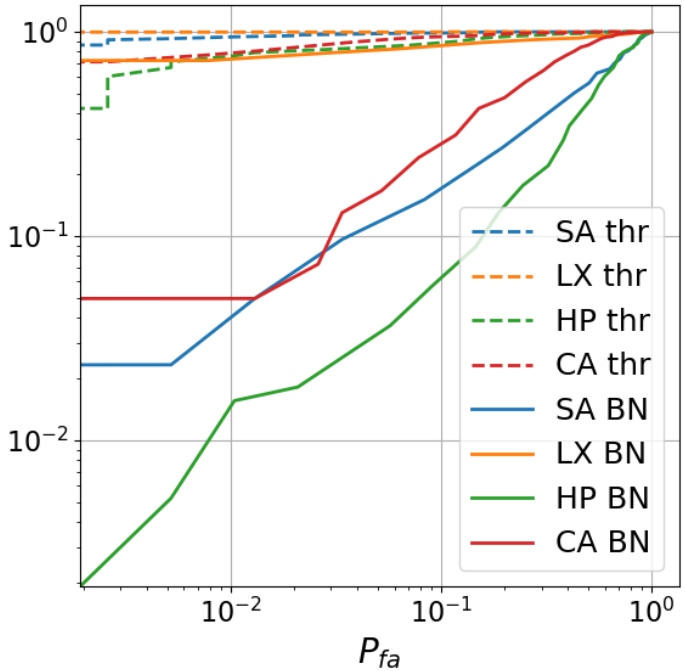
(b) Pearson correlation: log scale

Figure 10: The ROC curves for $Pearson\ correlation$ between the original and fake printed codes estimated via ¦ \} methods. P_d denotes the probability of the correct detection and P_{fa} is the probability of false acceptance.

Authentication results



(a) Pearson correlation



(b) Pearson correlation: log scale

Figure 11: The ROC curves for *Pearson correlation* between the original and fake printed codes estimated via *?i* and ¦\} methods. P_d denotes the probability of the correct detection and P_{fa} is the probability of false acceptance.

Conclusions

- we investigated the clonability of generic printable graphical codes using machine learning based attacks
- we examined the proposed framework on real printed codes reproduced with 4 printers
- we demonstrated a possibility of sufficiently accurate cloning of the PGC from their printed counterparts
- this should serve as a warning that more research are needed on the colonability of PGC

web-page:

`http://sip.unige.ch/projects/snf-it-dis/publications/icassp-2019`

GitHub:

`https://github.com/taran0/clonability-of-printable-graphical-codes`

Dataset:

`http://sip.unige.ch/projects/snf-it-dis/datasets/dp0e/`

References I

Xavier Marguerettaz, Frédéric Gremaud, Aurélien Commeureuc, Vickie Aboutanos, Thomas Tiller, and Olivier Rozumek, *Identification and authentication using liquid crystal material markings*, June 3 2014, US Patent 8,740,088.

Takeru Maehara, Kentaro Nakai, Ryo Ikeda, Koutaro Taniguchi, and Satoshi Ono, *Watermark design of two-dimensional barcodes on mobile phone display by evolutionary multi-objective optimization*, 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS), IEEE, 2014, pp. 149–154.

Anh Thu Phan Ho, Bao An Mai Hoang, Wadih Sawaya, and Patrick Bas, *Document authentication using graphical codes: impacts of the channel model*, Proceedings of the first ACM workshop on Information hiding and multimedia security, ACM, 2013, pp. 87–94.

References II

Justin Picard, *Digital authentication with copy-detection patterns*, Optical Security and Counterfeit Deterrence Techniques V, vol. 5310, International Society for Optics and Photonics, 2004, pp. 176–184.

Sviatoslav Voloshynovskiy, Maurits Diephuis, Fokko Beekhof, Oleksiy Koval, and Bruno Keel, *Towards reproducible results in authentication based on physical non-cloneable functions: The forensic authentication microstructure optical set (famos)*, 2012 IEEE International Workshop on Information Forensics and Security (WIFS), IEEE, 2012, pp. 43–48.

Bernhard Wirnitzer and Slavtcho Bonev, *Matrix print data storage and method for encoding the data*, August 21 2008, US Patent App. 11/572,591.

Hsi-Chun Wang, Ya-Wen Cheng, Wan-Chi Huang, Chia-Long Chang, and Shih-Yun Lu, *Using modified digital halftoning technique to design invisible 2d barcode by infrared detection*, Intelligent Technologies and Engineering Systems, Springer, 2013, pp. 179–186.

References III

Chau-Wai Wong and Min Wu, *A study on puf characteristics for counterfeit detection*, 2015 IEEE International Conference on Image Processing (ICIP), IEEE, 2015, pp. 1643–1647.

Rongsheng Xie, Chaoqun Hong, Shunzhi Zhu, and Dapeng Tao, *Anti-counterfeiting digital watermarking algorithm for printed qr barcode*, Neurocomputing **167** (2015), 625–635.