Secure printing for labels and packaging using industrial digital printers: authentication of printed matrix codes with smartphone cameras

Slavtcho Bonev[1,2] and Sviatoslav Voloshynovskiy[1]

[1]Stochastic Information Processing Group, Computer Science Department, University of Geneva
[2]Epyxs GmbH, Gutacher Ring 4, 68239 Mannheim, Germany

E-mail: s.bonev@epyxs.com; svolos@unige.ch

Short Abstract

In a previous publication (Bon, 2010) the feasibility of a product security concept based on authentication of printed matrix codes was demonstrated. The security features were printed using an offset press and scanned by a flatbed scanner. A comparison of the extracted authentication signatures has confirmed the high discriminative power (very low Equal Error Rates (EER) achieved) and leaded to a successful validation of the product protection approach using both standard (DataMatrix) and special (DataGrid) matrix codes. Two main issues remained a subject of further investigation. First, the used offset printing process led to similarities of the authentication signatures within a printed batch introduced by the printing plate, which resulted in multiple matches causing an ambiguity at conducting a database search. Second, to check the security features a high-resolution scanning was necessary, which required the usage of special scanning devices and made the verification more difficult for the end-user. In the current work we extend the previous findings to industrial digital printing and image acquisition by smartphone cameras.

Keywords: product protection, industrial digital printing, authentication, matrix codes, smartphone cameras

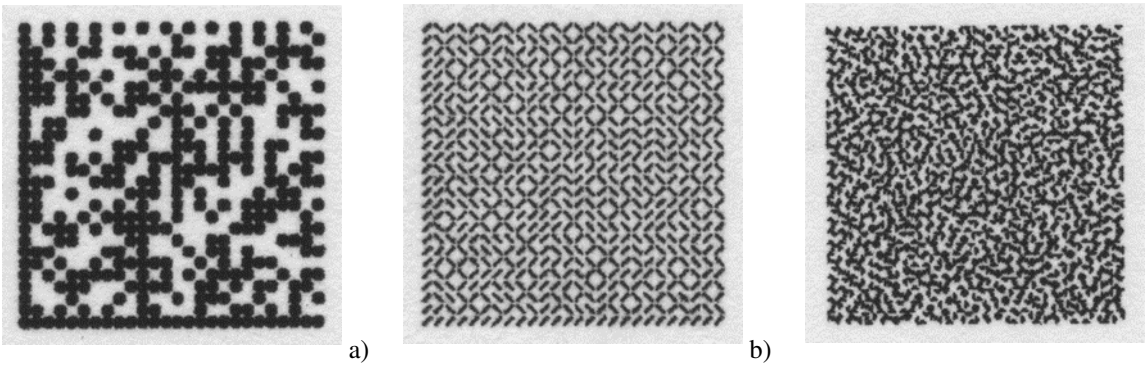
1. Introduction and background

Millions of dollars a year are on the line for companies as they seek ways to ensure that the products sold with their logos and branding are authentic and are delivered via the authorized distribution chains. The proliferation of counterfeiting requires brand owners and their converter/printer partners to work together to create a multi-layered protection plan so that their packaging and labels protect their brands and deter those trying to profit at their expense (Weymans, 2013; Bonev, et al., 2010).

The improvements in industrial digital printing and smartphone camera technologies over the last years enable an adaptation of the product security concept towards better usability, economic efficiency, and environmental sustainability.

Recent trends show that many brand owners are looking for a complement to traditional offset printing - a solution that matches the desired output to the right technology efficiently and cost effectively. Printing tests on the industrial digital printer Primefire 106 (Lohmann, 2017), which uses the SAMBA™ drop-on-demand printhead of the FUJIFILM Group (Yoshinori, 2014), have shown that a 95 percent coverage of the Pantone color space is possible. In addition, an offset-like result was achieved on the substrates used. The technology also has other advantages, so for example, the water-based inkjet ink is recyclable and thus contributes to even higher environmental friendliness of cardboard boxes. In addition, material will be saved, since there would be little waste and resource efficiency could be increased.

Since their introduction in the latter half of the 2000s, smartphones have consistently gained market share and become more than simple gadgets, as they combine the best features of cellular phones, personal computers, and digital cameras. The built-in megapixel camera sensors combined with high-quality optics and autofocus lenses can meanwhile be used to solve complex document examination tasks. Therefore, it is natural to expect that the smartphone can be used for the verification of the brand protection features (Diephuis, et al., 2014).



a) b) c)

Figure 1: Printed matrix code samples: DataMatrix (a), DataGlyphs (b), and DataGrid (c)

There are substitutes (Figure 1) for the standard codes (International Organization for Standardization, 2006) used as product identifiers (DIN 66401) in the last decades. DataGlyphs (Xerox) and DataGrid (Epyxs) represent a new class of differential codes which have two crucial advantages over the unipolar DataMatrix and QR codes. First, the proportion of printed to non-printed area in the code symbol is constant (Figure 2). This allows to check the dot gain and the uniformity of the symbols for the purpose of printing quality control just by calculating the mean value of the symbol pixels in the scanned image.

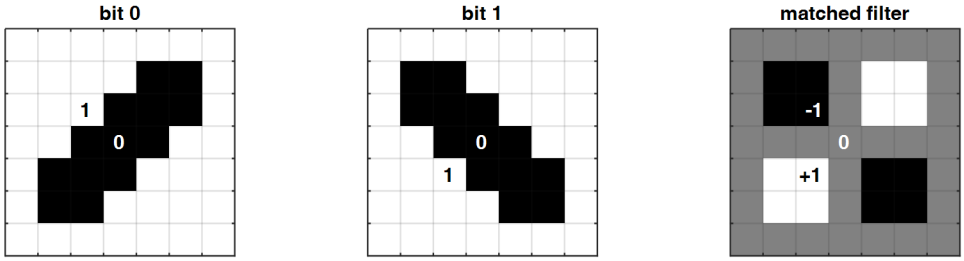


Figure 2: Graphical information encoding using DataGlyphs symbols

Second, after applying the matched filter (Figure 3) and sampling the corresponding symbol values, a bit decision is made using a constant zero-threshold. Thus, the bit decision is robust against dot gain and non-uniform illumination. The decision threshold for unipolar codes, which has to be calculated for each scanned code leads to great bit error rates for high dot gain levels or non-uniform illumination.

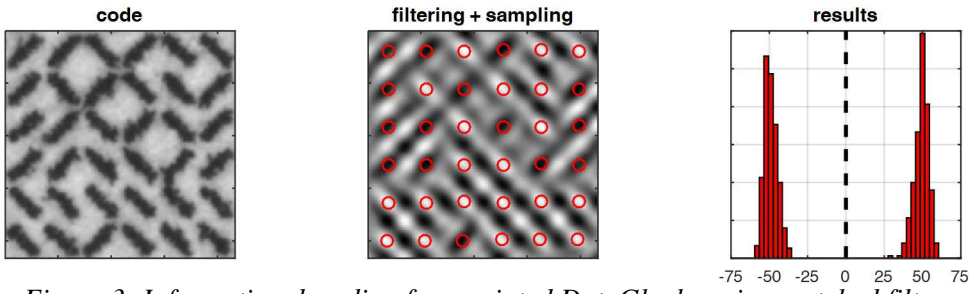


Figure 3: Information decoding from printed DataGlyphs using matched filter

The increase of data storage density represents an additional advantage (Table 1).

Table 1: Matrix codes and their properties

Nr.	Matrix code	Symbol size	Bits/symbol	Modulation	Communication theory
1	DataMatrix	6x6 dots	1	amplitude	OOK: On-Off Keying
2	DataGlyphs®	7x7 dots	1	phase	BPSK: Binary Phase-Shift Keying
3	DataGrid	6x6 dots	2	phase	QPSK: Quaternary Phase-Shift Keying

The terms identification and authentication are widely used in the area of human biometrics, but are often misused when it comes to matrix codes as printed security features. The content of the matrix code is used as a product identifier (ID). At the same time, the stochastic signal caused by the interaction between medium (ink) and substrate (paper) is unique for each print and can be used as an authentication signature (AS) of the printed matrix code.

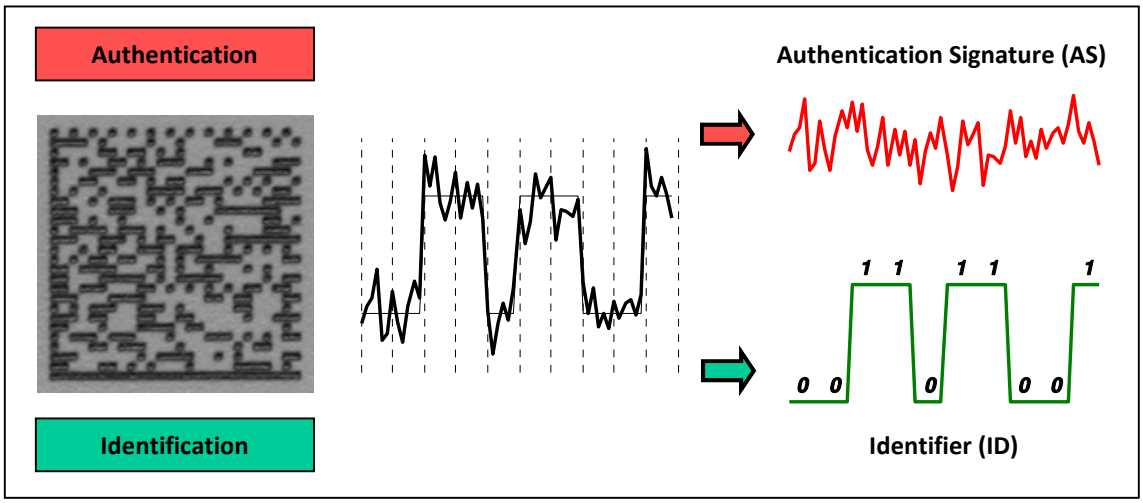


Figure 4: Identification and authentication using matrix codes

We formulate some new research questions regarding the product security concept and try to address them in this publication:

- Which discriminative power can be achieved with industrial digital printing using the authentication signatures of different matrix codes?
- How good we distinguish originals from copied codes on counterfeited products?
- Can the digital printing press be identified based on the extracted stochastic signal?

2. Materials and Methods

2.1 Printing devices

In the previous article (Bon, 2010) an offset printing press at 2400 dpi was used. The codes were printed relatively small to produce enough process deviations (fingerprint) and were not suitable for scanning with smartphone camera. Real serialization cannot be realized since the offset image remains the same for all items on each printed sheet. Even if each item on a sheet is marked individually, there are N identical items in a batch, which leads to ambiguous authentication results.

Through the usage of digital printers with VDP (Variable Data Printing) option (Ben, 2006), a unique identifier (Din, 2011) is printed on each item and printed sheet. The authentication effort is reduced from a 1:N comparison (offset printing, check all authentication signatures in a batch of N sheets) to a 1:1 comparison (digital printing, check only the authentication signature corresponding to the registered ID)!

Office inkjet printers are used in the proof of concept phase and industrial printers in the product development phase. The binary code images are generated as 1-bit TIF images and are printed using the native resolution according to device datasheet. Tables 2 and 3 summarizes the used office and industrial printers.

Table 2: Home office digital printers

Nr.	Digital printer	Abbreviation	Print technology	Native resolution
1	Canon PIXMA iP7200	CA	thermal inkjet	600 x 600 dpi
2	Epson WorkForce WF-2010	EP	piezo inkjet	720 x 720 dpi
3	HP OfficeJet Pro 8210	HP	thermal inkjet	600 x 600 dpi

Table 3: Industrial digital printers

Nr.	Digital printer	Abbreviation	Print technology	Native resolution
1	FX DocuColor 1450 GA	FX1	EA toner xerography	2400 x 2400 dpi
2	FUJIFILM Jet Press 720S	FJ7	high-speed piezo inkjet	1200 x 1200 dpi
3	HP Indigo 8000	HP2	liquid ink electrophotography	812 x 812 dpi

2.2 Scanning devices

Flatbed scanners at 1200 dpi were used to achieve optimal scanning conditions implying low spatial distortion and uniform illumination. A scanning resolution of 1200 dpi was also reached using a smartphone camera (Table 4) at a distance of 90 mm. This was considered as an indication that the authentication is possibly practicable for the end-users of the protected products. Table 4 summarizes the used scanning devices.

Table 4: Scanning devices

Nr.	Scanning device	Type	Optical resolution	Scanning resolution
1	Canon CanoScan 9000F	flatbed scanner	4800 dpi	1200 dpi
2	Epson Perfection V850	flatbed scanner	4800 dpi	1200 dpi
3	Samsung Galaxy S6	smartphone (mobile)	1200 dpi	1200 dpi

Two scanning scenarios (Figure 5) were simulated:

a) Optimal scanning: the smartphone is parallel to the substrate (0° tilt), no image distortions
b) Freehand scanning: the smartphone is tilted to the substrate, perspective image distortion

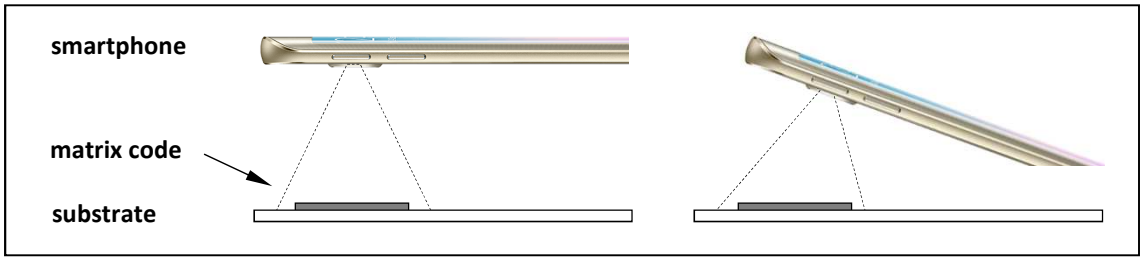


Figure 5: Scanning scenarios

2.3 Methodology

DataGrid codes (Wirnitzer and Bonev, 2004) are used as reference codes with maximized discriminative power through high-detail code symbols. Similar differential matrix codes DataGlyphs (Bloomberg, et al., 2000) consisting of low-detail code symbols are used for comparison. Both matrix codes consist of 24x24 information symbols. According to the recommendations of DIN 66401, only single module DataMatrix and QR codes with a maximum of 24x24 code symbols and maximum size of 11x11 mm can be used as Unique Identification Marks (UIM) for product marking and track-and-trace purposes.

The copies (counterfeits) of each matrix code are created using the original binary image and printing device, and are printed in the neighborhood of the original code to make batch scanning easier. This approach differs from the usual procedure of scanning, (optional) binarization, and reprinting of the codes and represents the worst case counterfeiting scenario whereby the original pattern and the printing technique are known to the counterfeiter.

The evaluation procedure was fully described in a previous work (Bonev, et al., 2010). The first scanning device according to Table 4 is used for AS registration, and both other devices – scanner and smartphone – are used for AS verification. The authentication signature (AS) represents the decoding error signal using an optimal filtering method (Figure 4). The correlation coefficient of different AS represents the authentication result. Respective EERs are calculated for each pair of printing and scanning devices using Gaussian result distribution models (Figure 7). The aim is to show that the discriminative power of the authentication signature is significantly higher than those achieved for human fingerprints (Pankanti, Prabhakar and Jain, 2002) and human iris (Daugman, 2015), which both have worst-case EER values of around 10^{-3}.

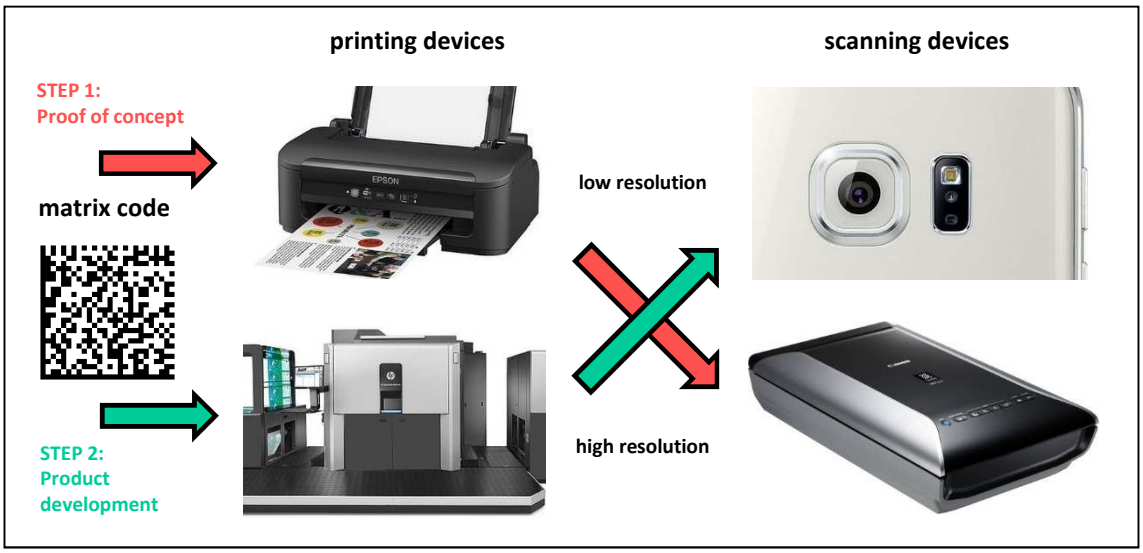


Figure 6: Two-step evaluation methodology

3. Results and Discussion

The experimental results for a single printing device results are exemplary presented in Figure 7 in order to emphasize the main characteristics of the authentication approach. The authentication performance is expressed by its corresponding EER value, and is presented in Table 5 for each combination of components – matrix code, printer, and scanning device. For each involved component a clear systematical influence on the EER was expected and identified.

The type of matrix code has an influence on the EER achieved. Due to the higher detail content of the code symbols, DataGrid leads to systematically lower EER values compared to DataGlyphs.

The type of used scanning device also shows a clear tendency regarding the authentication results achieved. Due to better optical transfer function (OTF) the scanner leads to systematically lower EER values compared to the smartphone camera. The JPEG image compression artifacts, which are introduced in the digital images by the mobile scanning device OS, additionally reduce the digital image quality.

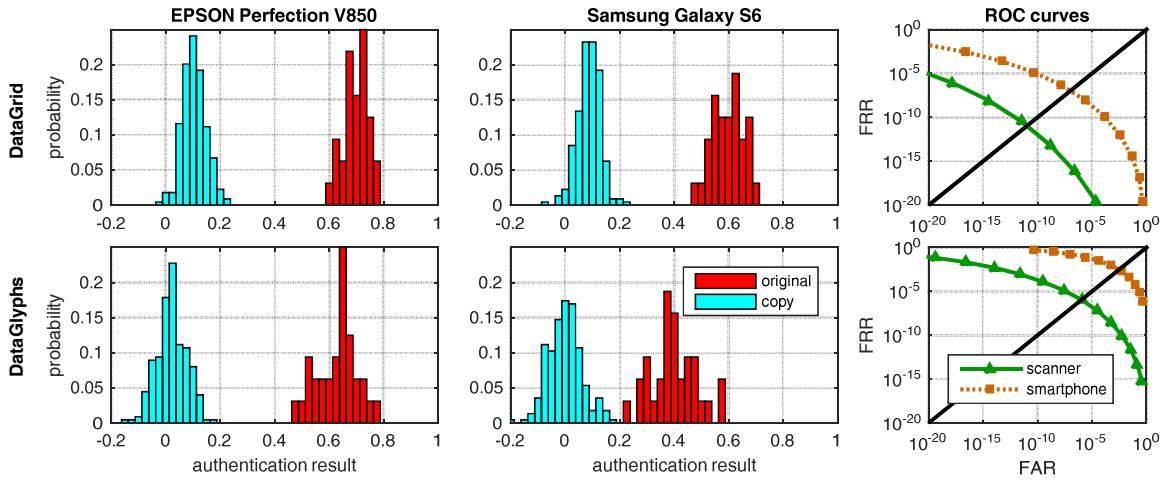


Figure 7: Authentication result distributions and corresponding ROC curves for the CA printer

The used printing device has the greatest influence on the EER. The CA and HP printer show EERs of 10^{-11} and 10^{-21} (third column of Table 5), respectively. The great EER difference of several decades cannot necessarily be derived from the difference between the printed code patterns with an area of 5x5 mm shown in Figure 8. The interaction between ink and paper is a stochastic process which is expressed by different types of distortions (Figures 8 and 9) of the printed patterns compared to the original binary patterns of the code symbols shown in Figure 2. The resulting EER depends highly on the AS extraction algorithm and can be estimated only empirically.

Table 5: Authentication performance using different codes and printing/scanning devices

Nr.		**EER DataGrid**		**EER DataGlyphs**			**EER DataGrid**		**EER DataGlyphs**	
	device	scanner	mobile	scanner	mobile	device	scanner	mobile	scanner	mobile
1	CA	10^{-11}	10^{-7}	10^{-6}	10^{-3}	FX1	10^{-10}	10^{-6}	10^{-5}	10^{-3}
2	EP	10^{-10}	10^{-6}	10^{-11}	10^{-4}	FJ7	10^{-7}	10^{-4}	10^{-6}	10^{-4}
3	HP	10^{-21}	10^{-15}	10^{-13}	10^{-6}	HP2	10^{-8}	10^{-5}	10^{-7}	10^{-4}

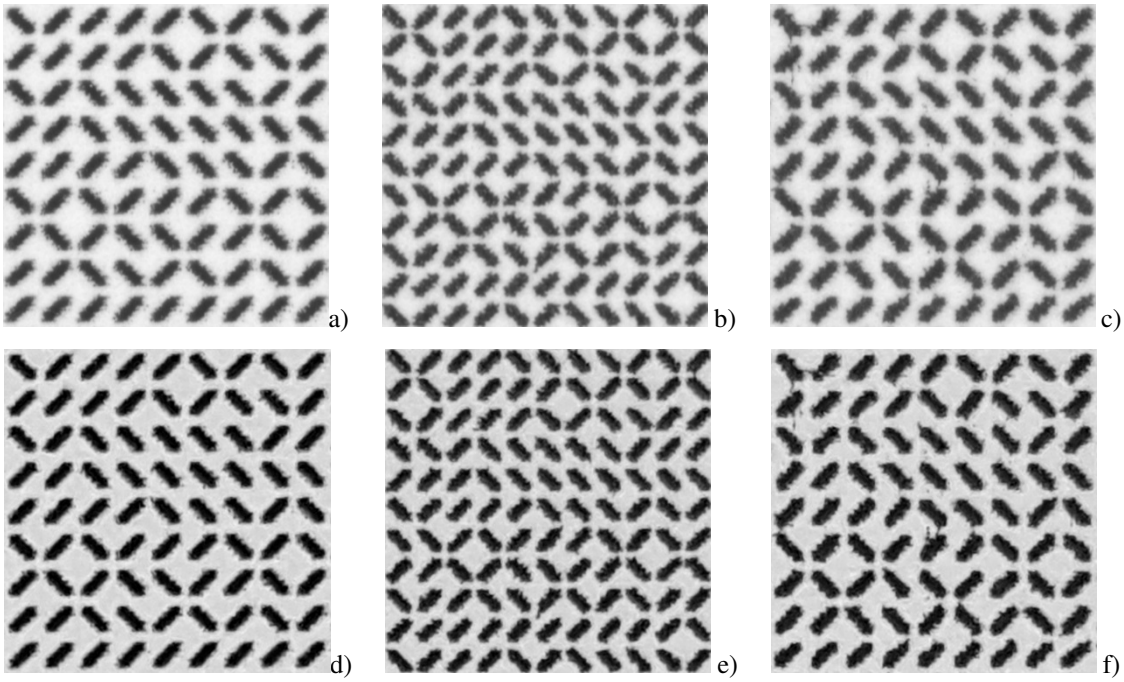


Figure 8: Typical distortions of DataGlyph symbols printed by different home office printers and scanned using scanner (upper row) and smartphone (lower row): CA (a,d), EP (b,e), and HP (c,f)

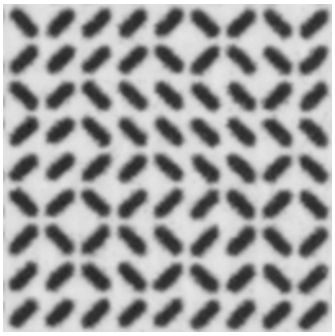
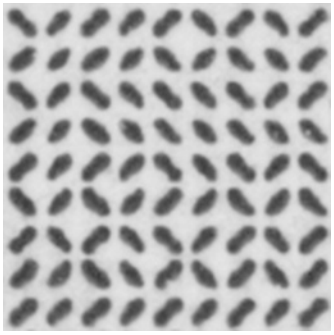

a)

b)

Figure 9: Typical distortions of DataGlyph symbols printed with HP Indigo 8000 at 812 dpi (b) compared to high quality print from FX DocuColor 1450 at 2400 dpi (a)

4. Conclusions

The concept of authenticating printed matrix codes using a smartphone camera (scanning resolution around 1200 dpi) proved to be successful with reached minimum ERR of 10^{-15} with office inkjet printers (printing resolution around 600 dpi, code size 12x12 mm) and ERR of 10^{-5} with industrial inkjet printers (printing resolution around 1200 dpi, code size 6x6 mm, FX1 printer excluded). All printed codes were conform to the requirements of DIN 66401 - Unique Identification Mark for serial product marking. The successful transfer of the authentication concept from offset printing and stationary scanning to digital printing and mobile scanning is expected to support the development and implementation of new brand protection applications with increased cost efficiency and usability.

It was shown that printing processes with lower printing quality lead to lower EER values, respectively to higher authentication performance. The usage of smartphone camera as authenticating device at around 1200 dpi reduces the authentication performance while working at its optical resolution limit and introducing compression artifacts in the scanned image. As expected, for smaller codes (industrial printers) the image degradation led to the decrease of authentication performance. Both differential matrix codes DataGrid (Epyxs) and DataGlyphs (Xerox) achieved results above the stated minimum threshold of 10^{-3}, whereby systematically lower EER values were reached using the DataGrid matrix code. Due to its higher detail information coding symbols, the authentication signature of DataGrid has shown higher discriminative power.

Acknowledgements

We gratefully acknowledge the experimental support of Mr. Hongyu Sun and Mr. Pai Peng from Shenyang AnChuang Information Technology Co. Ltd. in the area of industrial digital printing.

References

Bennett, P.K., 2006. *The Handbook for Digital Printing and Variable-Data Printing*. Graphic Arts Technical Foundation, ISBN: 978-0883625644

Bonev, S., Gebhardt, R. and Wirnitzer, B., 2010. *Quality measurements in anti-counterfeit offset print production.* Advances in Printing and Media Technology, Montreal, Canada, Vol. XXXVII, pp. 117-126, ISBN 978-3-9812705-2-6

Bloomberg, et al., 2000. *Self-clocking glyph shape codes*. US Patent Office, Patent number: 6,076,738

Daugman, J., 2015. *Information Theory and the IrisCode.* IEEE Transactions on Information Forensics and Security, Volume: 11, Issue: 2, DOI: 10.1109/TIFS.2015.2500196

M. Diephuis, F. Beekhof, S. Voloshynovskiy, T. Holotyak, N. Standardo, and B. Keel, 2014. *A framework for fast and secure packaging identification on mobile phones*. Proceedings of SPIE Photonics West, Electronic Imaging, Media Forensics and Security V, San Francisco, USA

DIN, 2011. *DIN 66401: UIM - Unique Identification Mark - Application standard for very small items using matrix symbols*

ISO, 2006. *ISO/IES 16022: Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification*

Lohmann, F., 2017. *Heidelberg: MPS Obersulm is the first pilot user of the Primefire 106.* [online] Available at: <http://www.print.de/News/Produkt-Technik/Heidelberg-MPS-Obersulm-erster-Pilotanwender-der-Primefire-106_4049> [Accessed February 2018]

Pankanti, S., Prabhakar, S. and Jain, A.K., 2002. *On the individuality of fingerprints*. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, Issue: 8, DOI: 10.1109/TPAMI.2002.1023799

Weymans, F., 2013. *Label and Packaging Security: Brand Protection Tools in Printing and Packaging*. Retrieved from: http://whattheythink.com/articles/62758-label-packaging-security-brand-protection-tools-printing-packaging/

Wirnitzer, B. and Bonev, S., 2007. *Method for encoding data via matrix print data storage*. European Patent EP 1771813

Yoshinori, K. ,2014. *FUJIFILM Group's Inkjet Printhead and Technology*. [online] Available at: <http://www.fujifilm.com/about/research/report/059/pdf/index/ff_rd059_007_en.pdf> [Accessed February 2018]