# Security Printing Techniques Based on Substrate and Print-Process Individualities

Stoyan Maleshliyski*, Reinhold Günter*

**Keywords:** Anti-counterfeiting, security printing, substrate fingerprint, print-process individuality

## 1. Abstract

According to the international chamber of commerce: “the international trade in counterfeit and pirated goods costs the world economy about 250 billion USD annually.” Economic losses from this phenomenon “put over 2.5 million legitimate jobs at risk in the G20 countries” (ICC, 2009). One way to minimize these effects is to protect products with security features.

This paper investigates the status quo in the security printing world based on substrate and print-process individualities. The authors present the milestones in the development of security printing applications and review relevant works in this field.

Based on the reviews a categorisation of the presented techniques is created arranging them in groups with respect to their reliability, security, speed, complexity of the extraction/verification device, and nature (extrinsic/intrinsic). At the end, three common use cases are reviewed and the technologies which are suitable for these cases are proposed.

## 2. Introduction

The evaluation of the authenticity of a product or document gets more important everyday. The existence of powerful technical tools, at affordable prices, allows counterfeiters to create fakes, which practically look just like the originals.

The classic anti-counterfeiting solution is still the addition of a handwritten signature or a seal of the issuing party. At the time when the authenticity of the documents needs to be proved, the existence of the original signature or seal on it confirms its originality and authenticity. Nowadays these simple techniques are no longer adequate for the protection of important documents and expensive products.

*Institute of Digital Signal Processing, Faculty of Computer Engineering, Mannheim University of Applied Sciences, Paul-Wittsack-Strasse 10, 68163 Mannheim, Germany

Today there are many ways to protect a document from being counterfeited: using special paper, special ink, complex print marks and symbols, nonstandard resolutions, etc. The number and complexity of methods can be confusing without experience and know-how. Therefore this paper tries to order and categorize the different techniques and gives an overview of fingerprinting approaches. These are still under development and therefore not widely applied for product protection.

In Chapter 3 widely used methods in the field of security printing are shortly described and categorized. The next chapters deal with fingerprinting techniques beginning with their historical development in the fourth chapter. Chapter 5 contains summaries of the reviewed methods and explains the ideas of each of the research groups. The evaluation of the methods and their applicability in different solutions are analysed in Chapter 6. The last chapter deals with still unsolved problems in the security printing world affecting also fingerprinting technologies.

Before starting, the term “security printing” and other terminology have to be considered. The terminology in this field is not consistent and used differently from one author to another. Especially terms like “counterfeit,” “tamper,” “copy,” “imitate,” and “falsify” are used in different circumstances and meanings. In this document the term “counterfeit” is used as a generic term. The reader should be aware of the fact that not every method prevents all three kind of counterfeiting. Different solutions could prevent, e.g., the copying, imitating, or falsifying of a document.

## 3. State of the Art

As mentioned above, there are numerous methods which can be used to protect a document or package from being counterfeited. By analyzing their keynote a basic classification is performed, and the most common techniques have been combined in the following main categories:

- *Use of nonstandard materials, techniques, and devices:* The methods contained in this group rely on special, not standard, means to prevent the forger from imitating an original product. This includes, for example, application of special inks (sometimes even not at the free market), utilisation of special papers, and usage of not widely spread techniques and devices. The methods in this group are secure as long as the forger is not able to get access to the technical means or it is not profitable to reproduce a counterfeited original.

- *Use of cryptographic and other information security methods:* One of the well-known methods deals with digital signatures and their transmission over printed documents. Usually the contents of the

document are digitally signed, the signature is encoded in machine-readable code and printed on the document. Another widespread method is the so-called serialisation in which an individual number is generated for each document. The algorithm for the generation of the number is complex and secret so that only the owner of the document/package can generate it. These techniques have the security of cryptographic algorithms and represent very reliable tools for guaranteeing the integrity of a given document/package. These provide on the other hand no security against copying.

- *Use of fingerprinting techniques:* The common idea of the methods contained in this group is to extract a virtually unique identifier from each physical copy of a document/package and thus be able to identify illegal copies. Some of the techniques evaluate the surface of the substrate, others the individuality of the print process. The analysis of material and color individualities is also possible. It is relied on the fact that each of these features is of stochastic nature, thus providing a reliable identifier for each individual copy or for copies from the same batch. During the production process the fingerprint of each document/package is extracted and saved for later verification. In the verification phase the fingerprint of a document/package is extracted and compared with the saved fingerprints, which are known to be original. If a match is found the document/product is genuine; otherwise it is an illegal copy. An advantage of these methods is that no special inks or substrates are used.

The methods which use fingerprinting techniques are of main interest in this paper.

## 4. Historical Development

The fact that the surface of non-reflective substrates is unique in its structure is well known. Since the suggestion of Goldman (1986) there have been many works dealing with the creation of a security printing solution based on the evaluation of the uniqueness of the surface. The idea has been developed further amongst others by Metois et al. (2002), Buchanan et al. (2005) and Clarkson et al. (2009).

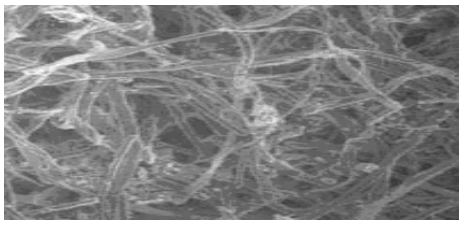

***Figure 1.*** *The surface of non-reflective substrates is unique (here normal paper).*

An alternative method is the verification of the signature of the printing process. This approach has been investigated by Zhu et al. (2003) and Mikkilineni et al. (2004), who evaluated the ink splitter caused by the randomness in the digital printing process.

An approach which combines both methods, the paper&print fingerprint, has been proposed and investigated by Wirnitzer et al. (2003, 2005, 2007), Bonev et al. (2008), and Maleshliyski et al. (2007, 2009). In this case a special pattern is printed. Because of the influence of the irregularities of the printing process combined with the uniqueness of the substrate's surface the shape of this pattern slightly changes.

Based on the research in the field and the technical papers presented so far, the fingerprinting applications have been classified according to their approaches in the following categories:

*a)* *Technologies evaluating substrate individualities:* These research groups are motivated by the fact that many substrates have an individual structure. Most methods in this group use special devices (such as laser or high-resolution scanners) or apply complex scanning routines (scanning from different directions) to get the texture of the surface. In some of these methods there is no need to print any special patterns and they can be used as well before printing of content as after printing it. A disadvantage could be that the structure of the substrate is easily damaged if the substrate is handled roughly (wrinkles, stains, etc.). The identification security of the methods would sink noticeably.

*b)* *Technologies evaluating print-process individualities:* The methods in this category investigate the individualities of the print process. Digital printing as well as offset printing is a physical process, which inevitably includes random components. Some groups have developed methods to enhance the influence of these components (e.g., a manipulation of the drivers of a laser printer can set up a custom speed of the drum rotations, thus adding a custom signature to all documents printed with this particular printer).

c) *Technologies evaluating the combination of substrate and print-process individualities:* The combination of both individualities is a very good identifier to be used in security printing applications. The group in this category analyses the stochastic component from the medium-substrate interaction combined with the stochastic component from the irregularities from the printing process. A special pattern is printed which provokes a microscopic ink smudging because of its form. This smudging combined with the irregularities in the printing process creates a reliable, content-relevant identifier. Thanks to signal theory algorithms damages in the identifier can be detected and excluded from analysis. A disadvantage of this method is the fact that a pattern needs to be printed.

## 5. Reviewed Techniques

**a) Technologies evaluating substrate individualities**

*J. Buchanan et al. – "Fingerprinting documents and packaging"*
*L. Bruell, M. Friedrich (Bayer Technologies) – "Laser-Streulichtmessungen zur Verpackungsidentifizierung und –verfolgung"*

The most basic form of fingerprinting techniques is analogous to the biometric fingerprint and inspects the surface of materials. This research is done in Buchanan et al. (2005) with a low-cost portable laser scanner using the effect of laser speckle.

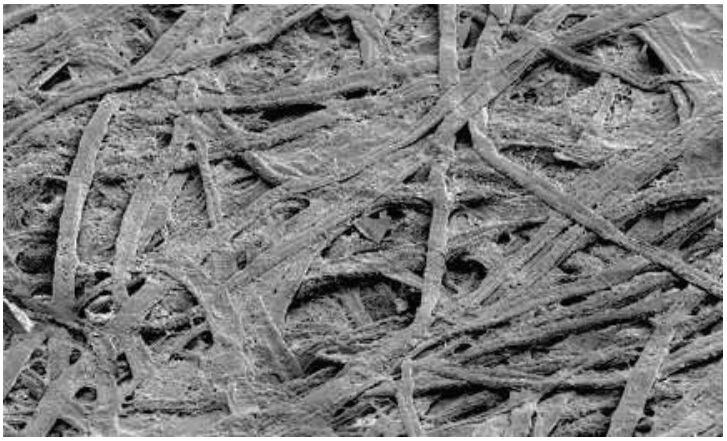

***Figure 2.*** *Surface of a substrate under the microscope (Source: Buchanon et al. (2005)).*

Generally speaking all non-reflective surfaces have the feature of intrinsic roughness that can be used as a security feature because of its randomness. This roughness has been inspected with a laser scanner to measure the fine structure

along a line at a certain position on the material. The measured signals of two different sheets of paper and two scans of the same piece of paper have been cross-correlated. The first result featured no significant peak, whereas the second result showed a strong peak at zero positional shift. The amplitude of this peak can be used as a quality measurement of the uniqueness.

The tests were made with different materials, e.g., paper, paperboard, and plastic. The used paper was "roughly handled," including baking, screwing, scrubbing, and submerging in cold water. The method proved to be also resistant against displacements of up to 1 mm and rotations of up to 2°. The size of the measured fingerprint is 200–500 bytes and resulted in equal error rates of $10^{-20}$ to $10^{-72}$.

A commercial application of this technology is presented in Bruell et al. (2007). The size of a fingerprint in this solution is 150–750 Bytes and its storage in a database is a core component of the system.

*E. Metois et al. – "FiberFingerprint Identification"*

The "FiberFingerprint" developed by Escher Labs uses the individual structure of the fibres of the substrate in a specially marked area of documents or packages. For the extraction of the security features, a so-called "FiberFingerprint verifier" is used, which consists of consumer-grade camera, lens, and lightning apparatus in a specially developed case. The region of interest is marked with registration dots, used for compensation of translation, rotation, and scaling distortions in the captured greyscale image. Within this area the fibre information is extracted along a custom pathway called "signal path."

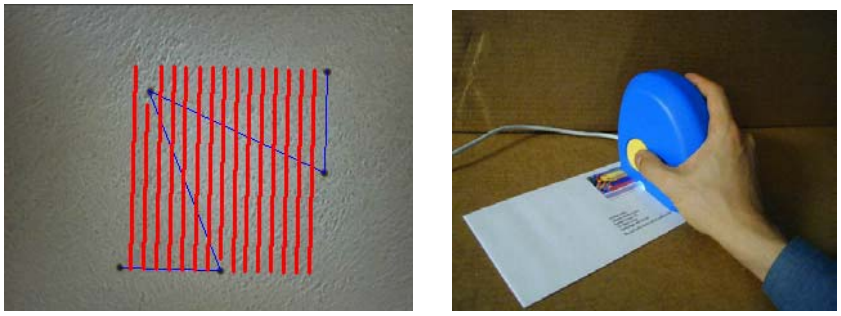

***Figure 3.*** *a) The FiberFingerprint method; b) Verification device used to extract the substrate individualities (Source: Metois et al. (2002)).*

This system has many parameters, e.g., the signal path. One of the most important configuration parameters is the sampling frequency, which results in FiberFingerprints of different lengths from 50 to 300 samples.

The extracted FiberFingerprint is stored, beside the systems configuration, in a database after the enrolment step. During the verification process the FiberFingerprints from the present object and the database are compared by means of an error rate based on correlation coefficients.

The performance is measured amongst others in equal error rates. Depending on the size of the FiberFingerprints equal error rates of $10^{-2}$ to $10^{-7}$ have been achieved.

*J. Smith, A. Sutherland – "Microstructure Based Indicia"*

In Smith et al. (1997) a system for anti-counterfeiting in the field of indicia is presented by using the microscopic paper structure of, e.g., letters without the need of a database.

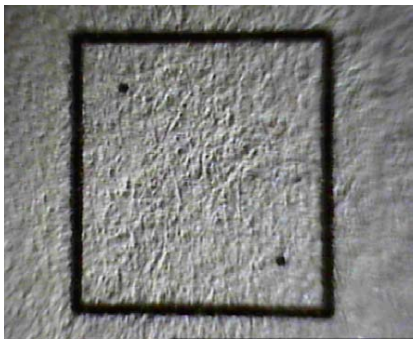

***Figure 4.*** *The texture of paper in a certain area, captured with a video camera (Source: Smith et al. (1997)).*

The texture of paper in a certain area is scanned using a video camera. The area is marked by printing two round spots on the paper. These registration marks are used to compensate rotation and translation. The scanned texture is converted into a so-called "texture hash string" which can be achieved by discrete wavelet transform, discrete cosine transform, or discrete Fourier transform.

Instead of storing this security feature in a database the information is encrypted, coded in machine-readable form, and printed on the same sheet of paper. The authentication can now be done by extracting and converting the texture, decoding the texture hash string stored on the letter, and subsequently comparing both. Thereby no database is needed and the authentication can be done offline.

*W. Clarkson et al. – "Fingerprinting Blank Paper Using Commodity Scanners"*

The method proposed by Clarkson et al. (2009) measures the 3-D texture of paper using no exotic equipment. It produces a specific fingerprint without

modifying the content of a document and could be applied before or after the content is printed.

A scan of the document in four directions—0°, 90°, 180°, and 270°—allows an exact extraction of the surface texture. The texture information is used to create a feature vector describing the structure of the paper. The feature vector is supplied with redundancy to enable channel error correction. At the end a one-way hash function is applied so that a possible forger would not be able to determine the feature vector, even if he gets access to the fingerprint.

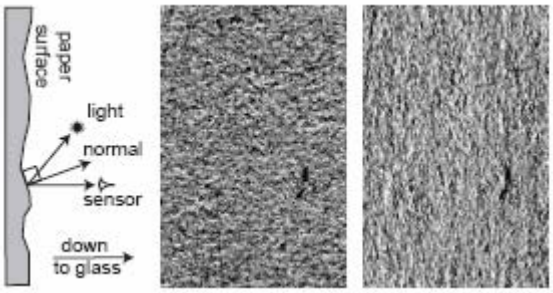


***Figure 5.*** *The surface of a substrate, taken with a commodity scanner. The principle of the method proposed by Clarkson et al. is presented on the left (Source: Clarkson et al. (2009)).*

The authors do not extract the feature vector from a single region of the document but compute it from a collection of representative subsections. The location of these sections originates from the locations of a Voronoi distribution. To initialise these pseudorandom locations the algorithm uses a random seed stored in the fingerprint. Using only certain locations complicates the verification process and introduces an additional burden for a potential forger. The security of the technique is measured in equal error rates (EER). Under ideal handling conditions, the system achieves an EER of $10^{-148}$. The authors performed several tests for the resistance of the algorithm against non-ideal handling conditions. The EER values become worse, but even in the case of wetting and then drying the document they still have a reasonable value.

**b) Technologies evaluating print-process individualities**

*E. Kee, H. Farid – "Printer Profiling for Forensics and Ballistics"*
*J. Oliver et al. – "Use of Signature Analysis to Discriminate Digital Printing Technologies"*

Instead of analysing the paper, or more generally the substrate of printed documents, it is also possible to extract security features from the printed information itself. In Kee et al. (2008) a method is described for how to identify different printers by examination of the geometric degradation of characters

from, e.g., a letter. This “printer profiling” method uses a standard flatbed scanner to digitize a printed document. In the image, characters of the same kind are selected and, after a compensation of different luminance conditions, their alignment is adjusted. These aligned characters are packed into a matrix and processed with a Principal Component Analysis (PCA). PCA is a well-established method in digital signal processing and amongst others used in biometrical methods, e.g., iris scan and face recognition (Jiali Cui, 2004) and in OCR applications. The main idea of PCA is the rotation of the coordinate system so that the new dataset is sorted by their variance which means that they are ranked by their significance. Results show that only a small subset of the principal components is relevant. So a significant printer profile consists of the mean of the character and its first principal component. With this it is possible to reconstruct every character of that type printed on the researched printer. If the reconstruction error is significant then the character probably was printed with another printer.

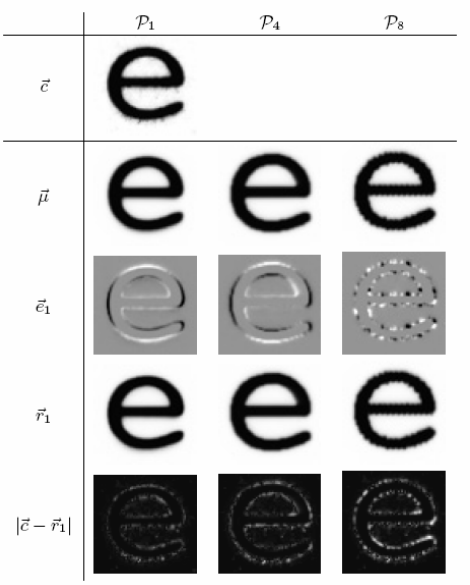


***Figure 6.*** *Differences between three printouts of the character “e”. (Source: Kee et al. (2008)).*

The individuality of the printer profile is good enough to determine whether two documents were printed on a printer of different make and model. The classification results are about 99% to 100% of correctly identified printers. But it is not possible to differ between the same make and model. Another possible solution with the printer profile is to verify whether a single document was printed with one or more printers.

Another method of identifying printers is described in J. Oliver et al. (2002). An automatic machine-vision-based print quality analyzer is used to differentiate between different digital printing technologies and even different printer models.

*A. Mikkilineni et al. – "Signature-Embedding In Printed Documents For Security and Forensic Applications"*

In Mikkilineni et al. (2004) methods to use banding of digital laser printing for both intrinsic and extrinsic signatures are presented.

Banding is an artefact that arises from fluctuations in the movement of the OPC Drum of a digital laser printer. It results in a quasi periodic imperfection of the printed document. After the document is scanned at 2400 dpi it is divided into small areas. Within these areas characters are analyzed in process direction using a fast Fourier analysis (FFT). Now it is possible to extract the outstanding frequency and use it as a characteristic feature.

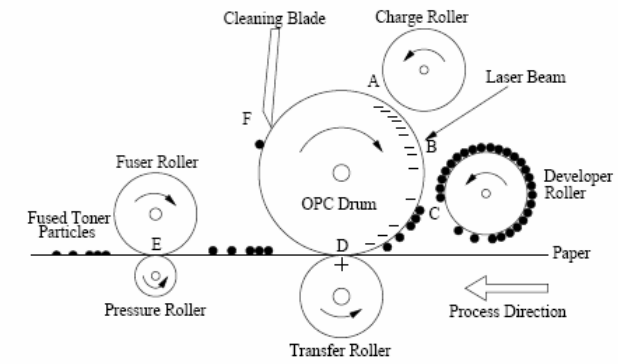


***Figure 7.*** *The principle of a digital printer. This group evaluates the fluctuations of the speed of the OPC Drum. (Source: Mikkilineni et al. (2004)).*

If the "natural" banding of the laser printer is analyzed and processed the security feature is called "intrinsic signature." That way the make and model of the printer used to print a document can be determined.

Another method, called "extrinsic signature," is to influence the printing process itself. By manipulating the process via a driver, special software, or embedded in the printer firmware, the banding can be actively controlled to create a watermark.

*B. Zhu et al. – "Print Signatures for Document Authentication"*

Zhu et al. (2003) developed a method for evaluation and extraction of the non-repeatable randomness existing in the printing process. For this purpose a secure pattern together with several auxiliary landmarks for alignment is used. In the next step the shape of the printed pattern is extracted and analysed. The shape of the pattern, together with unique information from the document, forms a secure identifier for the each document. The generated identifier is then printed on the document as a machine readable code or an OCR font.

To verify the authenticity and originality of the document, the secure pattern is extracted and compared with the information coded in the machine readable code. If the results match, the document is authentic; otherwise it is considered to have been counterfeited.

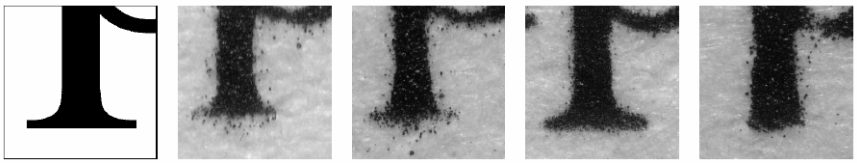

***Figure 8.*** *The character "P" on the left in raw format. The next four images show the character printed with different printers. (Source: Zhu et al. (2003)).*

The presented technique measures the shape of the printed secure pattern, simply calculating its centroid, segmenting it and identifying the radii of each segment from the centroid to the perimeter.

Typical problems for pattern recognition applications, like scaling, rotation, and translation, are not relevant to that system because of the existence of alignment landmarks.

The performance of the system is measured in false acceptance rates (FAR). The number of selected segments (N) influences the FARs strongly: for N = 32 the FAR is $10^{-15}$, for N = 72 the FAR becomes $10^{-34}$.

The whole analysis of the paper is based on experiments with digital printing devices (at 600 dpi). In the conclusion the authors suggest that the method can be extended to other document types such as offset-printed, inkjet-printed, and even manually signed documents.

*S. Simske et al. – "Effect of Copying and Restoration on Color Barcode Payload Density"*

Simske et al. (2009) correctly outline that the simplest means of counterfeiting a document or package is to make a high-quality copy of the original. In this study the team explores the impact of various factors on color barcode payload density. In the multiple experiments performed in the test, different color deterrents are being printed. To optimize the readability of the codes a spectral pre-compensation is performed.

***Figure 9.*** *Color-optimized barcodes, created by HPLabs, and their copies. (Source: Simske et al. (2009)).*

The printed deterrents are scanned with an off-the-shelf scanner. For authentication and detection of copies two algorithms are used. The first one, the so-called "RGB approach," calculates the minimum Euclidean distance between the code symbol's mean and the values of the calibration areas. The second authentication approach, the "Hue approach," calculates the minimum angular distance between the hue of each code symbol's color and the hues of the calibration elements. That is the minimum absolute hue difference between the element's mean RGB value and the hue of the calibration elements.

Using these algorithms the group is able to identify an image of a security deterrent which has already undergone the print-scan process. The tests indicate that copying (or undergoing the print-scan resp. scan-print process) produces a consistent reduction of the payload density by approximately 55% under all tested conditions (different sizes of the deterrents).

The implications of the findings described in this paper are that advanced and complex printing and imaging optimization techniques should be used for security-related color barcodes.

**c) Technologies evaluating the combination of substrate and print-process individualities**

*B. Wirnitzer et al. – "Paper&Print Fingerprint"*

Wirnitzer et al. suggest the printing of a special pattern. Because of the influence of the irregularities of the printing process, combined with the uniqueness of the substrate's surface, the shape of this pattern slightly changes.

The group created a special 2-D barcode, the DataGrid, which can store up to 720 bytes/cm$^2$ printed at 1200 dpi. The shape of the printed DataGrid code differs from the shape of the raw DataGrid code. This difference the authors refer to as the "EpiCode." There are two components that contribute to the occurrence of the EpiCode: the stochastic component from the medium-substrate interaction and the stochastic component from the irregularities of the printing process. The interaction of these two components produces a virtually unique signal which, because of its stochastic nature, is robust against forgery and can be used for identification of counterfeited documents, packages, etc.

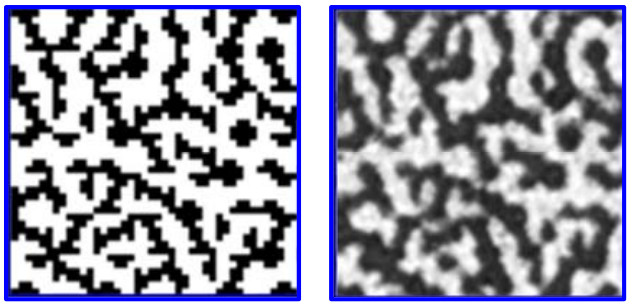

***Figure 10.*** *The raw DataGrid and an image of a printed DataGrid on the right. (Source: Maleshliyski et al. (2009)).*

The idea is to print the DataGrid and then scan it in a following step. After analysing the image of the DataGrid, the EpiCode can be extracted. The authors propose two solutions for saving the EpiCode for the verification step: printing it in a second DataGrid or storing it in a database. The first approach allows a self-sufficient solution, because during the verification step no connection to an external database is needed. The disadvantage of this solution is the need of an additional printing step after the main print process. The second solution does not require an additional printing, but it needs an external database connection so that the extracted EpiCode could be compared with the one stored in the database.

The group has also developed other security features which can be applied in different application scenarios. The ClusterCode is a special term used to explain the phenomenon, that the EpiCodes of products printed at the same position of the printing plate (in offset printing applications) comprise a common component. This occurs because of the individualities of the printing plate in an offset printing press.

Another feature is the NanoGrid, which is a slight manipulation of the DataGrid, at sub symbol level. If the DataGrid is copied, the NanoGrid is changed by the noise of the print process, as it is near its physical limitations. This approach is known in literature as the "copy detect pattern approach."

The group investigates also the individualities of different colors, which would add an additional component to the standard 2-D EpiCode.

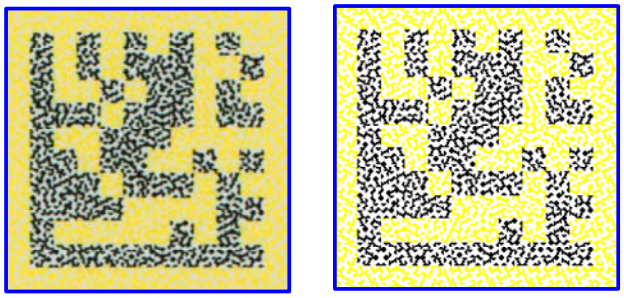

***Figure 11.*** *A macrocode is superimposed over the normal black-and-white DataGrid, simply changing the color of DataGrid symbols. On the left: an image of a printed DataGrid, on the right: the raw image. (Source: Maleshliyski et al. (2009)).*

Even though the DataGrid is specially designed to stimulate the flowing of the ink, any printed 2-D barcode will possess such security features like the EpiCode and the ClusterCode. Because of the fewer edges in standard 2-D barcodes, a special extraction method is needed and currently researched in order to guarantee a high security level.

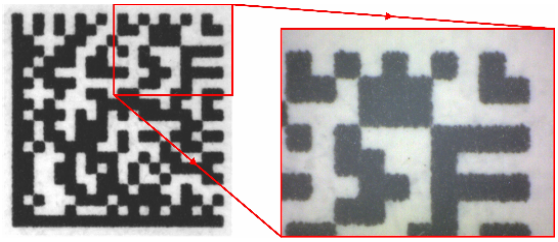

***Figure 12.*** *The symbols of a standard Datamatrix code also possess individualities.*

After various tests the calculated Equal Error Rate (EER) of the system achieved, when printing a security printing pattern with an area of 17 $mm^2$ at 1200 dpi, are not worse than $10^{-18}$ for digital printing and $10^{-33}$ for offset printing (Bonev et al., 2008)

An advantage of the technology is that it does not require any special inks or papers and as extraction resp. verification device a normal off-the-shelf flatbed scanner can be used.

## 6. Evaluation

As each of the reviewed papers had a different focus, it is difficult to find common criteria for evaluation. Although adapted from an ISO proposal, the following terms are not standardized and may be used with different meanings.
The following criteria, based on the experience of the authors, are used to evaluate the reviewed techniques: *security level achieved, complexity of input device, speed, overt/covert, reliability*.

- **Security:** This criterion evaluates the equal error rates of the methods. It is an important property of a security printing system because it measures the probability that the system would incorrectly reject a legitimate original or incorrectly accept a fake as an original. This security is dependant on the evaluated area. The method proposed by Clarkson et al. provides an equal error rate of $10^{-148}$. This is an extremely low value which makes that system virtually error-free. The methods of Buchanon et al. ($10^{-72}$), Zhu et al. ($10^{-34}$), Wirnitzer et al. ($10^{-33}$), and Metois et al. ($10^{-7}$) are also worth mentioning.

- **Reliability:** This is the ability of a person or system to perform and maintain its functions in routine as well as unexpected circumstances. It measures the robustness of each method, evaluating its resistance to harsh handling or maloperation by personnel. The method proposed by Wirnitzer et al. is reliable because of its special pattern which has implemented error-correcting and reliable detection algorithms. The method of Buchanon et al. also provides the needed certainty according to the tests described in the paper. In this aspect the methods evaluating only the surface of the substrate have a minor disadvantage because of their noise sensitivity and the need of exact positioning.

- **Overt/Covert:** This criterion evaluates the necessity of an additional pattern. The methods using only the surface of the substrate (and not needing any additional orientation landmarks) have an advantage in this aspect. The techniques presented by Buchanon et al., Metois et al., and Clarkson et al. deliver covert solutions which can be used before or after the content of a document has been printed.

- **Verification/extraction Speed:** This criterion evaluates the time needed to extract or verify the security features from a document or a product. According to the paper Bruell et al. (2007) the speed achieved with their technique is 5m/s. Beside it the technologies proposed by Wirnitzer et al. and Simske et al. provide a real-time application at low costs.

- **Complexity of verification/extraction device:** This criterion evaluates the complexity of these devices as well as how common they are among consumer households. Depending on the application Wirnitzer et al., Zhu et al., Simske et al., and Mikkilineni et al. provide solutions which can be applied with a simple off-the-shelf flatbed scanner or even a cell phone.

These categories contain only the groups with best results in their fields. When building a solution, there is never just a single factor which is relevant. A reliable and robust solution depends on a number of complex interactions between the factors mentioned before.

The following examples show how the criteria showed above can be combined to form a use case for an application. And depending on the use case different methods become more suitable:

a) *High security application*: The best methods are the ones proposed by Buchanon et al. and Clarkson et al. The latter achieve an Equal Error Rate of $10^{-148}$ when evaluating an A4 sheet of paper. The method relies on the unique structure of the substrate. As an extraction/verification device the authors propose a standard flatbed scanner, which is available in many households. To measure the texture of the surface of the substrate it needs to be scanned from four different directions. This fact slows the process up and makes it not appropriate for production line speeds.

*b)* *Covert security application:* Another common requirement for security printing solutions is that the design of the products should not be changed. This excludes all methods requiring an additional pattern or landmark to be printed. The techniques based on the substrate individuality can be applied. Most of them provide a high level of security but medium reliability, especially in industrial conditions. Another restriction for some is that a special device is needed. This allows verification only for a selected circle of users.

*c)* *Security printing solution for mass-production:* If a security printing solution for the mass-market is needed, which is to be verifiable by normal users without special equipment, the method proposed by Wirnitzer et al. can be used. Its main advantage is the combination of security features with high-capacity data storage matrix codes, established in the mobile tagging word, providing *a priori* information which allows a fast, easy, and robust detection. The applicability in offset printing productions is provided by the high speed of extraction/verification and the occurrence of security features even when high-quality printing techniques are used. The Equal Error Rates of the system ($10^{-33}$) guarantee its security, and the error correction algorithms raise the reliability additionally. As the security features occur

already at 600 dpi (Bonev et al., 2008), the resolution of standard flatbed scanners and modern cell phone cameras is sufficient and these can be used as extraction/verification devices, thus enabling virtually anyone to verify products.

## 7. Conclusion

The analysis in the previous chapter shows that there are numerous methods available to create a reliable anti-counterfeiting solution based on substrate and print-process individualities. Each approach has its advantages and disadvantages, and its application in a given situation is to be evaluated on the boundary conditions and criteria mentioned in the previous chapter.

The fact that there has been so much research in the field and that so many different concepts have been created provides great flexibility.

There is still the question why some excellent methods are not so famous and have remained just as theoretical research projects. The answer is maybe given by a study of the international chamber of commerce which showed that "80% of consumers admit they regularly buy fakes, with little remorse or concern about the impacts of those purchases" (ICC, 2009).

There is much turbulence in the field of security printing at the moment and many ways in which the industry could develop. But one is for sure: as long as there are products, there will be counterfeiters, and as long as there are counterfeiters, security printing will be needed.

## 8. Acknowledgments

The authors wish to thank the BMBF (Federal Ministry of Education and Research) of Germany for the financial support (EpiCode3D, Project FKTZ PNT51503).

## Literature Cited

Bonev, S. and B. Wirnitzer. 2008. "Security printing for product packaging in industrial printing applications," *Proceedings of IARIGAI 35th International Research Conference*, Valencia, Spain.

Bruell, L. and M. Friedrich. 2007. "Laser-Streulichtmessungen zur Verpackungsidentifizierung und –verfolgung," atp 2007, Heft 5, S. 45, Germany.

Buchanon, J., R. Cowburn. A.-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D.A. Allwood, and T. Bryan. 2005. "Forgery: 'Fingerprinting' documents and packaging," *Nature*, vol. 436, p. 475.

Clarkson, W., T. Weyrich, A. Finkelstein, N. Heninger, J.A. Halderman, and E.W. Felten. 2009. "Fingerprinting blank paper using commodity scanners," *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, USA,

Cui, J., Y. Wand, J. Huang, T. Tan, and Z. Sun. 2003. "An Iris Image Method Based on PCA and Super-resolution," *Proceedings of 17th International Conference on Pattern Recognition*, USA.

Goldman, R.N. 1984 US Patent 4568936, "Verification system for document substance and content," 04.02.1984.

International Chamber of Commerce (ICC). 2009. http://www.iccwbo.org/policy/ip/index.html?id=34093, Fifth Global Congress on Combating Counterfeiting and Piracy, Cancun, Mexico.

Maleshliyski, S. and F. García. 2009. "Integration of anti-counterfeiting features into conventional 2D barcodes for mobile tagging," *Proceedings* of *TAGA 61st Technical Conference*, New Orleans, LA, USA.

Metois, E., P. Yarin, N. Salzman, and J.R. Smith. 2002. "FiberFingerprint identification," *Proceedings of 3rd Workshop on Automatic Identification*, New York City, NY, USA.

Mikkilineni, A. K., Ali, G., Chiang, G., Allebach, J., Delp, E. 2004, "Printer profiling for forensics and ballistics", Proceedings of SPIE Interneational Conference on Security, Steganography and Watermarking of Multimedia Contents VI, San Jose, USA, Volume 5306, pp. 455-466

Simske, J., M. Sturgill, and S.A. Jason. 2009. "Effect of copying and restoration on color barcode payload density," HP Labs, USA.

Smith, J.R. and A.V. Sutherland. 1997. "Microstructure Based Indicia," MIT Media Lab, USA.

Wirnitzer, B. 2003. Germany, DE10345669. " Datenträger mit Kopierschutz und Verfahren zum Erzeugen eines Sicherungscodes," 01.10.2003.

Wirnitzer, B. and S. Maleshliyski. 2007. Germany, WO2009071673A1, "Verfahren zur Erzeugung eines Sicherungscodes für einen Rasterdruckdatenspeicher und Gegenstand mit Farbrasterdruckdatenspeicher."

Wirnitzer B. and S. Bonev. 2005. "Fachhefte Grafische Industrie-Bulletin Technique," no. 3, p.30–33, Switzerland.

Zhu, B., J. Wu, M. Kankanhalli. 2003. "Print signatures for document authentication," *Proceedings of 10th ACM Conference on Computer and Communications Security*, Washington, DC, USA.