# Data Storage in Gentelligent Components: A New Way for Self-Authentication

**Ralf Dragon, Prof. Dr.-Ing. Jörn Ostermann**
Institut für Informationsverarbeitung (TNT),
Leibniz Universität Hannover
Phone: +49 511 762 5326, Fax: +49 511 762 5333
E-Mail: {dragon, ostermann}@tnt.uni-hannover.de

**Prof. Dr.-Ing. Berend Denkena, Dr. Bernd Breidenstein, Tobias Mörke**
Institute of Production Engineering and Machine Tools (IFW),
Leibniz Universität Hannover
Phone: +49 511 762 4839, Fax: +49 511 762 5115
E-Mail: {denkena, breidenstein, moerke}@ifw.uni-hannover.de

## Abstract

We propose a new way of authentication for components. Traditionally, hard-to-reproduce patterns like security holograms are attached or inserted into the component for authentication. During the verification, a-priori knowledge is needed. The approach we follow is that this information should also be attached to the component as digital data signed by cryptographically means. Inside the Collaborative Research Center CRC 653, we research gentelligent components, which are components that enable to inherently store digital information as well as an analog fingerprint. Using these components, we enable authentication with virtually no a-priori knowledge.

## Keywords

Self-Authentication, Plagiarism Detection, Inherent Data Storage, Micro-Structuring

## 1 Introduction

Proving the genuineness of values and information is needed since existing of mankind. Relics of many cultures show seals and stamps on deeds to ensure power of attorney was given. Later when handwriting was used, signatures were established as proof. This method of labeling can be used as legitimation because it is hard to reproduce exactly and small variations between original and forgery always exist in analog media. The significance of such variations is almost always detectable. As the patterns of such a label are very specific to its production process e.g., the very stamp or the person signing, these patterns are also called a *fingerprint*. An authentication is performed using a-priori knowledge about the fingerprint.

The concept of a fingerprint cannot be transferred to the digital domain to authenticate digital information. This is due to the fact that digital data can be duplicated exactly with simple means. For the authentication of digital data, the *digital signature* is commonly used as digital label. This signature is specific to the data signed and to a secret key that only the signer knows. The identification is performed with a public key from which the private key cannot be reconstructed.

Both the analog fingerprint as well as the digital signature share in common, that the very creation is unknown but the result is verifiable. For both authentication methods, a-priori knowledge is needed: Knowledge about the true fingerprint and the public key respectively. However, the link between label and genuineness differs for both methods. The link between a fingerprint and the genuineness of a value or a deed is the material it is placed on. A security hologram for example has to be fixed non-detachable to a component in order to authenticate it. The link between the digital label and digital data is the information itself. There is no way to abuse a digital label for information that it was not created for. To summarize: Analog labels authenticate objects, digital labels information.

It is nowadays an accepted fact, that the strength of a digital label is much higher than the strength of an analog one. So it is easier to forge fingerprints than digital signatures. Analog labels have to be improved constantly using new technologies to have an edge on counterfeiters who then also improve their forgery. This cat-and-mouse game could be stopped if a digital label with mathematically-proven strength was used. However, a digital label can only be linked to digital data and may thus not yet authenticate real world material. The here-presented method can fundamentally solve the link from digital data to real world material. Further, it allows authenticating objects with no fingerprint-specific a-priori knowledge.

## 1.1 Gentelligent Components

The work presented in this paper is part of the research on “gentelligent components in their lifecycle” of the Collaborative Research Center (CRC) 653. The vision is to create components that can gather and process information from its environment to improve and learn by transferring the biological principles of the field of genetics into the manufacturing environment. What is learned throughout the manufacturing process and the components lifecycle is stored within the component and will be used to improve the next generation. To allow this, components with new properties, as wells as methods and technologies have been developed which enable an effective communication of the component with its environment. One of the main ideas is to eliminate the physical separation of components and the related information as well as to utilize the inherent component information. This provides a broad field of application such as new ways of planning and controlling the manufacturing, assembling or maintenance processes. For example, the information gathered by a component during its lifecycle can be used to determine the remaining service life and to set up adapted maintenance intervals. Another field of application is the unique identification of the part. This satisfies the growing demand for companies to instantaneously know about the status of components within their manufacturing process and lifecycle [Zho09] as well as the requirements of a protection against plagiarism that becomes more and more important.

The term *gentelligent* describes the previously defined properties of these components. It is composed of the word *genetic* and *intelligent*. In this context, genetic refers to the static storage of basic details of the component like the geometric description to identify or reproduce it. Also details about the manufacturing process and the components properties can be stored. Corresponding to the biological process, unalterable information can be inherited from older generations of components. The term intelligence covers the technical ability to compile, preprocess or store data. For example, by developing a qualified material or sensor the gentelligent component saves the information about the mechanical and thermal loads within its lifecycle. The stored data can then be communicated directly or read out on demand.

To implement the visions and goals of the CRC 653, it is divided into the following five individual research scopes: long term storage, materials as sensors, dynamic magnet data storage, electro-optical systems and combining and utilizing gentelligent technologies. The presented work was conducted within project “long term storage” and shows the usage of inherent data storage on a gentelligent component as a novel idea of self-authentication.

## 1.2 Overview

In Section 2 detailed information is given to explain the method for combining analog and digital signature. Section 3 refers to the inherent data storage in gentelligent components and how this is achieved. The description of the general scheme is followed by the explanation of the mechanical writing process in subsection 3.1. Information

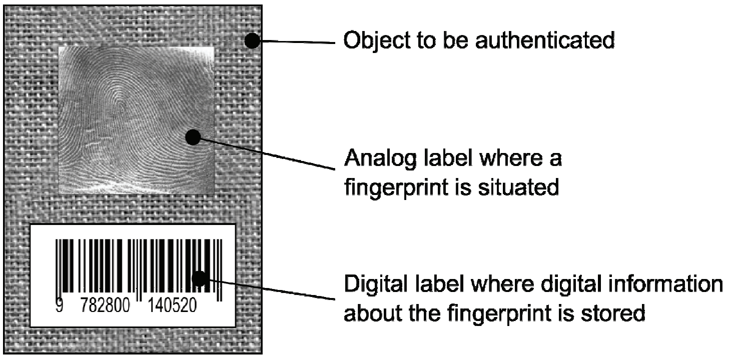

Object to be authenticated
Analog label where a fingerprint is situated
Digital label where digital information about the fingerprint is stored
9 782800 140520

*Figure 1: Mode of operation: Patterns of the fingerprint, which is either inherent or attached as a label, are digitally signed and stored on the component.*

about the optical readout method is given in subsection 3.2. Concluding, a résumé and an outlook are given in Section 4.

## 2 Self-Authentication of Gentelligent Components

The basic idea of self-authentication is displayed in Figure 1. A self-authenticating object contains an analog fingerprint and digital data. This data contains the fingerprint in a digital form which is cryptographically signed. Both the fingerprint as well as the digital data may be component-inherent like in gentelligent components or attached in the form of a label. However if there are labels attached, the fingerprint label must be non-detachable in order to not be used for a different component.

During the signing process, the analog fingerprint is read, and a digital label containing a signed digitalized version of the analog fingerprint is written. During the authentication process, both labels are processed and the fingerprint as well as the digital signature is verified. In the following, both processes are explained in detail.

### 2.1 The Signing Process

First, an analog fingerprint is established for the analog label which is closely linked to the component to be authenticated (S1). Linked means that the analog label is fixed to the object and non-detachable. In contrast to state-of-the-art watermarking methods like used in banknotes, fingerprints may differ from component to component as no a-priori knowledge about the patterns is needed. If the object already contains analog patterns useful for identification like object specific surface structures, these patterns can be used as fingerprint. Otherwise, a fingerprint can be inserted into the object, e.g., a stamp imprint.

In step S2, the fingerprint is extracted. The patterns are converted to a digital notation. Here methods are used that are not susceptible to normal wear and tear of the object to be secured. For metal surfaces, the methods should not be encumbered by rust, for paper, folds should be of no problem. Then, a data structure is created containing the

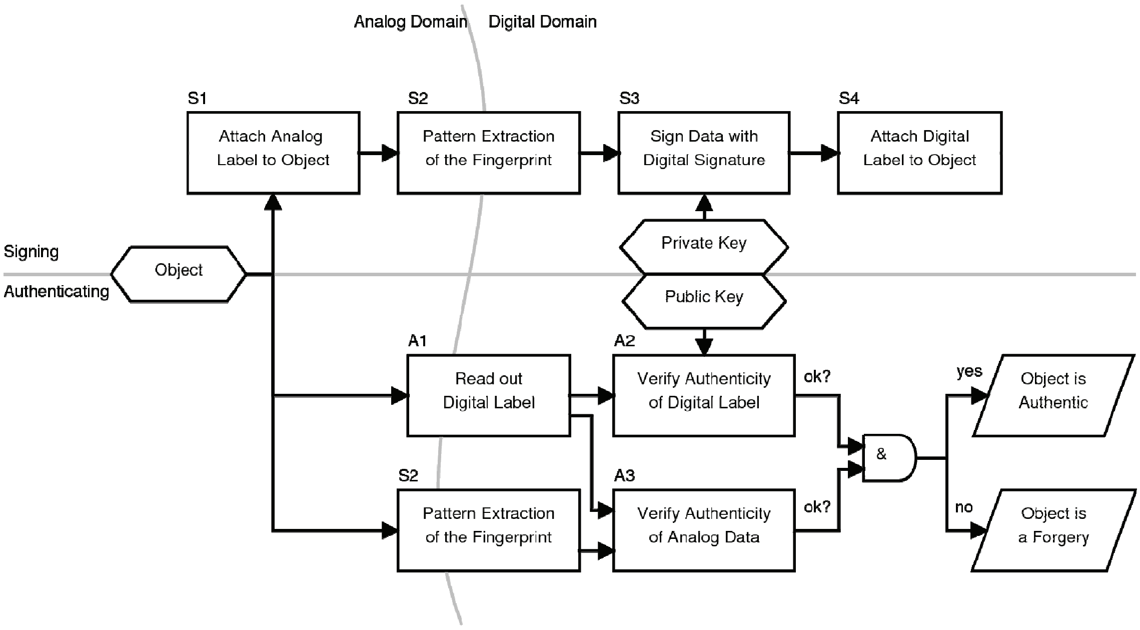

Analog Domain
Digital Domain
S1
Attach Analog Label to Object
S2
Pattern Extraction of the Fingerprint
S3
Sign Data with Digital Signature
S4
Attach Digital Label to Object
Private Key
Signing
Object
Authenticating
Public Key
A1
Read out Digital Label
A2
Verify Authenticity of Digital Label
ok?
yes
Object is Authentic
&
S2
Pattern Extraction of the Fingerprint
A3
Verify Authenticity of Analog Data
ok?
no
Object is a Forgery

*Figure 2: Block diagram for mode of operation*

digital notation of the fingerprint. This data structure is digitally signed by the creator's private key. A digital signature method like the RSA signature [RSA78] can be used. The private key is kept secret. The signed data is stored on the object. Like the analog information, it may be stored inherent or on a non-detachable label.

Please note that the public key is needed during the authentication. Thus it denotes some kind of a-priori knowledge. However, the public key may also be stored on the component, digitally signed by a master key from a globally-trusted authority.

## 2.2 The Authentication Process

The first step during the authentication is to read out the digital data stored on the component (A1). This data contains the digitalized fingerprint of the object as well as the signature. Further, the fingerprint is extracted with the same method (S2) as during the signing process.

The data is verified using the public key of the creator of the digital label (A2). The public key has to be known a-priori or it can be also safely stored inside the digital data (cf. Section 2.1).

To verify the analog label, the true patterns of the object's fingerprint are compared with the stored patterns from the digital label. The comparison metric is closely-related to the type of pattern extracted in step S2. The object is considered authentic, if the analog label in step A3 as well as the digital label in step A2 are considered authentic.

This combination of analog fingerprint patterns with digitally-signed data enables the authentication of object-specific fingerprints. As a-priori knowledge, only information about reading the data and extracting the fingerprint as well as about a master public key is needed.

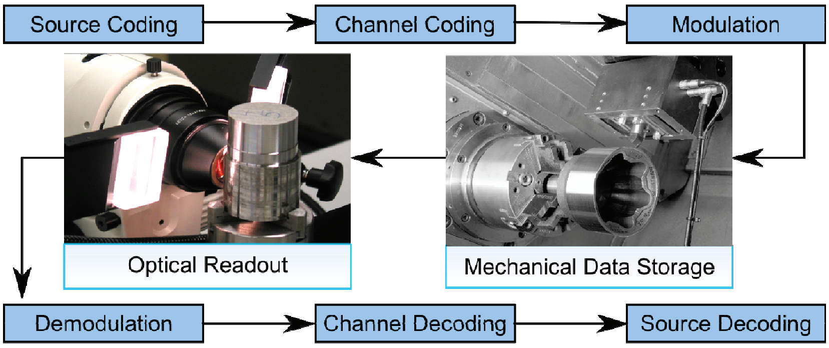


*Figure 3: Transmission principle*

## 3 Self-Authentication in Gentelligent Components

In the following, we demonstrate the work flow for inherently storing data and a fingerprint on the surface of rotational symmetric components. For inherent data storage, the material of the component itself has to be used. However this means that no binary effects can be exploited, like flipping magnetic domains in hard drives or λ/4 pits for destructive interference in CDs. Thus we use the standard model of digital transmission [Sch70]. As displayed in Figure 3, it consists of source coding (efficient representation of information), channel coding (interleaving to avoid burst errors, redundancy for error correction), modulation (conversion from digital frames to an analog signal run), the transmission channel (which usually is the radio link), and vice versa the demodulation, and the decoding. Modulation and channel coding have to be adapted to the characteristics of the channel such that the digital data does not become corrupted, and that the analog signal is transmitted undistorted with satisfactory signal-to-noise-ratio.

In this scenario, the analog signal run is preserved in the form of a groove with varying depth which is located on the surface of the component, similarly to an audio signal on a gramophone record or a PAL signal on a video disc [Isa85]. The reconstruction of the groove for reconstructing the analog signal is performed with nondestructive optical means using a microscope with low magnification. For demonstration purposes and simplicity, we do not apply any channel coding. Further, as modulation we use binary amplitude shift keying (2-ASK) with a pulse width of 50% to ease demodulation. This means, we distinguish two binary states and between two transmitted bits, we always return to the zero state.

### 3.1 Writing

As mentioned in Section 1.1, an essential part of gentelligent components is the ability to permanently and inherently hold data. The research focuses on using the component’s surface as well as the subsurface layers or its volume. Within the CRC 653, a fast-tool-servo was developed to store the data by micro-structuring the work piece surface. This

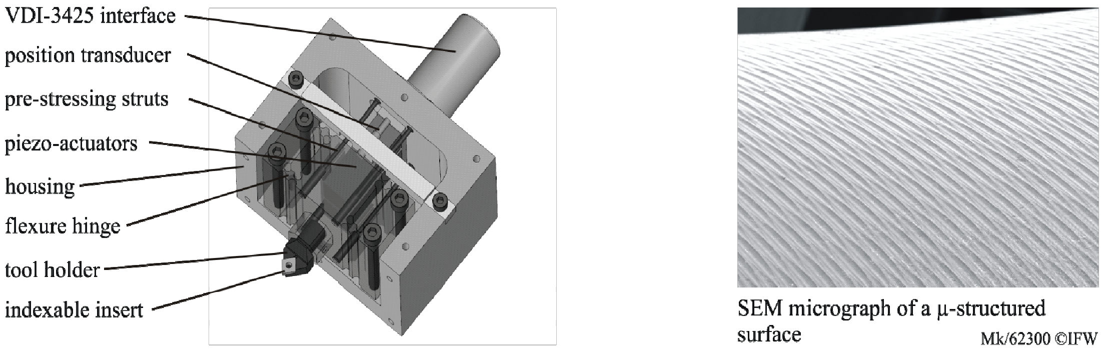


*Figure 4: a) Solid model of the fast-tool-servo. b) SEM micrograph of a micro-structured surface*

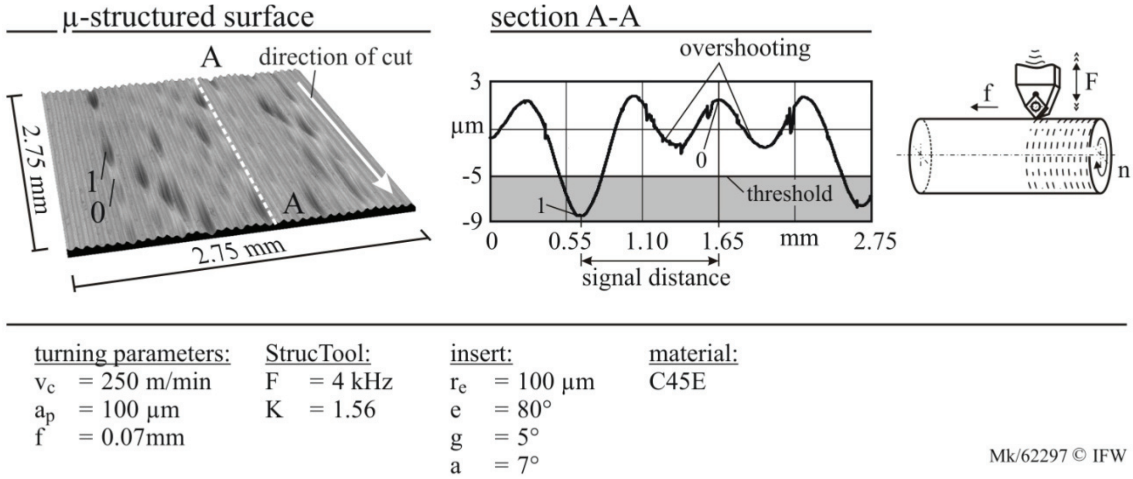
so-called StrucTool is used in a turning process for micro-structuring a component. In fact, the micro-structure consists of only one long groove that is wound around the component and spreads over all the surface.

The piezo-driven tool holder operates and moves perpendicular to the surface. As shown in Figure 4a, the tool is designed with a flexure hinge and a tool holder connected to the rigid body of the tool by piezo-actuators. The considerably small mass of the moving parts of the tool leads to a first natural frequency ω above 6 kHz. Experiments show that the dynamic range of the tool has a major impact on the practical information storage density [DBS+08]. Using the suggested modulation, this provides a theoretical data rate F of up to 6 kbit/s, with an amplitude of max. 8 µm. Hence a cutting speed of $v_c$ = 250 m/min leads to a bit length of l = 0.7 mm. The data density depends on the feed rate f. By applying a feed of f = 0.07 mm, a data density of 2 kbit/cm$^2$ can be realized. Figure 4b shows an SEM micrograph of the micro-structured surface of the outer diameter of a gentelligent component used as a demonstrator in the CRC 653.

The analog signal run created during the modulation (Figure 3) is used as input signal to excite the piezo-driven tool. By the defined tool deflection microstructures can be written onto the surface during the machining process. Figure 5 shows a depth map of a micro-structured surface taken by a confocale microscope and the run of a groove. By the piezo-actuatory movement of the tool, the surface profile is manipulated.

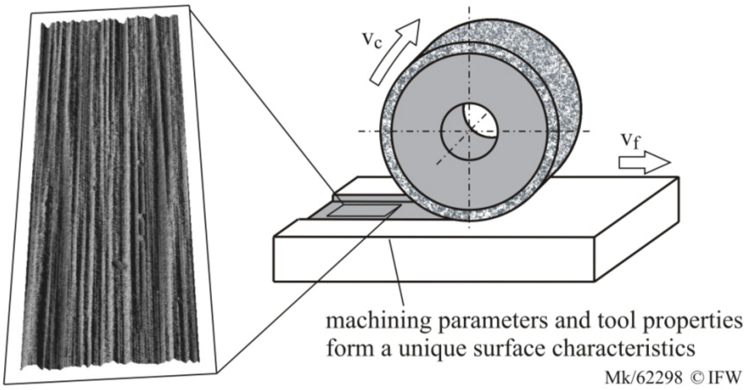
The research project includes the identification of process parameters to achieve the highest surface quality. The quality of the micro-structures and the density of the stored information depend on the feed rate and the cutting speed in combination with the frequency and the magnitude of the fast-tool-servo, the micro geometry of the cutting tool and the properties of the work piece material.

Permanently storing a distinct binary code on the components surface is one part of the self-authentication to prevent plagiarism. The second part is the application of an analog signature. Like a fingerprint embossed to the component, a unique surface structure is generated within the manufacturing process by grinding. Figure 6 shows a depth map from the fingerprint of a gentelligent component.



Mk/62297 © IFW

*Figure 5: Binary data on a gentelligent component with micro-structured surface. Dark colors denote deep positions with binary state 1, light colors denote state 0.*


$v_c$
$v_f$
machining parameters and tool properties
form a unique surface characteristics

Mk/62298 © IFW

*Figure 6: Applying a fingerprint to the surface of a gentelligent component by grinding*

The characteristics of the structure depend on the machining parameters and the properties of the grinding wheel. Because of the statistical arrangement of the abrasive grains and the small dimensions of the structure, it cannot be artificially replicated. The structure is read out and converted into digital data. This data can then be stored on the component's surface and in a database of the manufacturer.

## 3.2 Reading

Reconstructing the run of the groove depth means reconstructing the analog signal run. We use an optical approach as reading out the inherent data should be possible non-destructive and with simple means. There are many well-researched techniques for optical depth estimation like, e.g depth from focus [Gro87] and defocus [NC07], from stereo [Fal94] and from shading [HB89]. However, applications for these techniques like optical gramophone readout [TB06] or visual inspection [Sch02] only are able to reconstruct surfaces which are one magnitude larger (≈ 50 - 100 μm) than the groove variations to be recovered here (± 4 μm). Thus for depth reconstruction, we use directed illumination as measuring principle [DBR+09]. It makes use of reflections and shadows that arise from a directed illumination. As depicted in Figure 7, the edges of reflecting and shadowed areas are both shifted towards the middle of the groove if it becomes

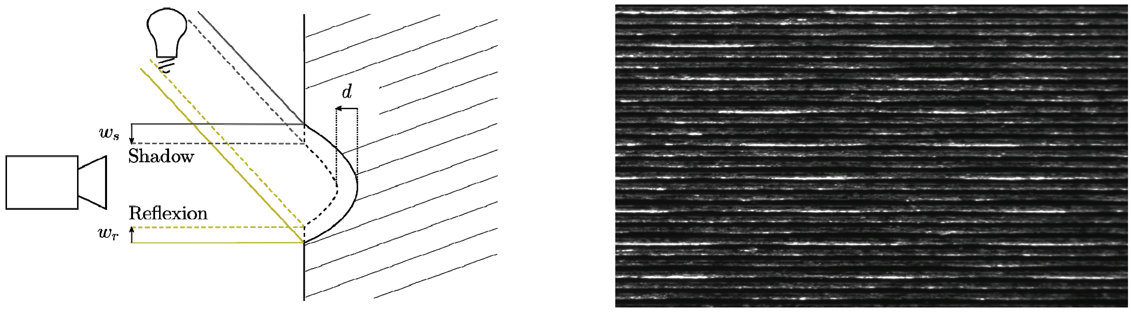


*Figure 7: a) Measuring principle of directed illumination. b) Surface view under directed illumination from the top. In the area of 2x3 mm$^2$, several groove segments running horizontally are visible. Variations in depth result in reflections and shadows.*

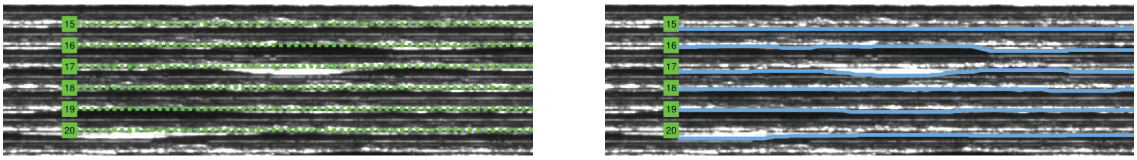


*Figure 8: a) Middles of groove sections found by 1D spectral analyses. b) Tracking result of the HMM tracking*

flatter. As a qualitative estimation of the signal run is sufficient for the demodulation, only the edges of reflection and shadow have to be tracked. In fact, we even only track the reflection edge as it was found to be more stable towards perturbations.

The edge tracking algorithm is split in two steps. First the groove segments, which all run parallel, are separated. We assume that they run approximately horizontal. Several vertical 1D cuts through the surface image are spectrally analyzed [Kay88]. Thus the coarse structure with periodically-occurring groove patterns can be used to find a dominating frequency corresponding to the groove distance. Likewise, the best-fitting phase algorithm from [DBR+09] is used for that frequency to determine the middles of the groove sections and the borders in between them (Figure 8a).

The second step is tracking the groove reflection edge. To find the most probable image interpretation, the Hidden Markov Model (HMM) from Figure 9 is used. It consists of one state per image pixel. To relate the appearance of the reflexion edge with the model, the observation probability of each state $S_{x,y}$ is related to the image deviation in $y$-direction. The movement of the Piezo tool, which cutted in the groove, is related to the transition probabilities. In order to have a continuous connection, only transitions from one column to the next are possible. For each transition, the probability is Gaussian-distributed with highest probability if the edge runs horizontal. For this HMM, the Viterbi algorithm [Vit67] finds the most-probable run of the groove (Figure 8b).

To read out the whole surface, the tracking is performed for all surface views of the object. Next, the extracted groove sections are fused at those positions, where the right border of one view joins the left of the next view. After one rotation, groove section $n$ meets section $n + 1$ such that the whole groove signal can be assembled. As last processing step, the signal is unbiased by subtracting the groove center from the signal.

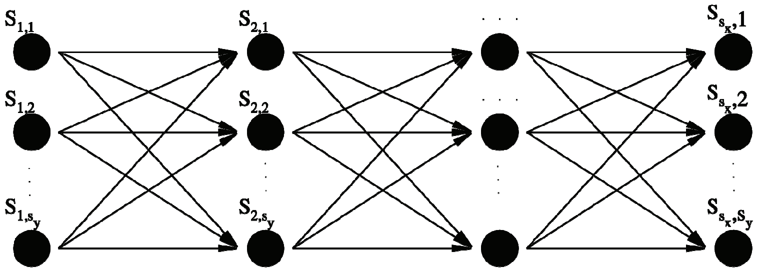


*Figure 9: Hidden Markov Model used for the edge tracking.*

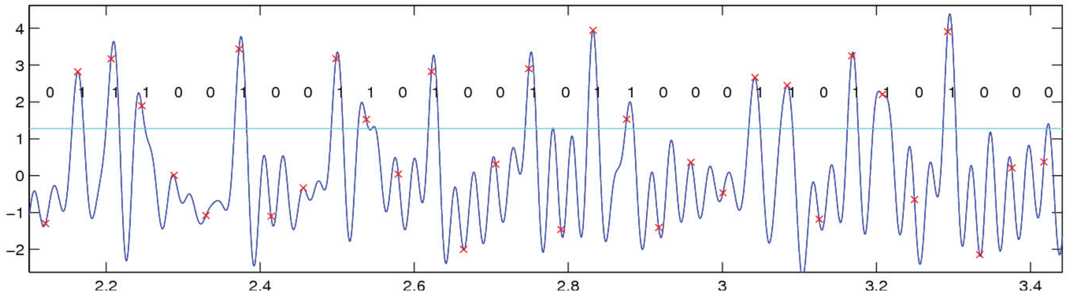


*Figure 10: Reconstructed signal and demodulated data*

For the demodulation, the signal is low-passed and binarized using a threshold found by a statistical signal analysis (Figure 10). Now the signal is ready to be decoded according to the scheme from Figure 3. As shown in [DBR+09], the influence usual of wear and tear as well as local damage is correctable by state-of-the-art channel coders.

Reading out a grinding fingerprint is done by analyzing the intensity profile of reflected light orthogonal to the grinding direction. An intensity run is sampled in equal steps and compared with another using the normalized cross-correlation. By this, matching and non-matching fingerprints can be classified.

## 4 Conclusion and Future Work

In this paper, we described an authentication scheme that combines analog fingerprints and digital authentication. By this, we enable authentication of components without having a-priori knowledge on the analog fingerprint. For gentelligent components this allows verifying the origin for plagiarism protection. Furthermore this could allow e.g., self-authenticating bank notes with stronger individual water marks as fingerprint and signed digital data stored on the surface in the form of an individual bar code. Likewise, a bar code on a letter could be used to verify the hand-written signature of the writer by applying our authentication scheme to signature patterns [KSX04].

Further, we showed the work flow for writing and reading inherent data and fingerprints on rotation-symmetric components. Recently, a fast-tool-servo was developed that allows micro-structuring of planar components during milling processes. This will enlarge the range of application for inherent data storage. In the next step, we research on enabling micro-structuring during the milling of free form surfaces.

## Acknowledgment

This work was funded as part of the Collaborative Research Center (CRC) 653 by the Deutsche Forschungsgemeinschaft (DFG). We would like to thank the DFG for its financial and organizational support of this project.

## References

[DBR+09] Dragon, R., Becker, C., Rosenhahn, B., Ostermann, J. Reading from Scratch - A Vision-System for Reading Data on Micro-Structured Surfaces. 31. DAGM Symposium, LNCS, Springer, Vol. 5748, pp. 402–411, 2009

[DBS+08] Denkena, B., Boehnke, D., Spille, C., Dragon, R. In-process information storage on surfaces by turning operations. CIRP Annals - Manufacturing Technology, Vol. 57(1):85–88, 2008

[Fal94] Falkenhagen, L.: Depth Estimation from Stereoscopic Image Pairs Assuming Piecewise Continuos Surfaces. In: European Workshop on Combined Real and Synthetic Image Processing for Broadcast and Video Productions, 1994

[Gro87] Grossmann, P.: Depth from focus. Pattern Recognition Letters 5(1), 63–69, 1987

[HB89] Horn, B.K.P., Brooks, M.J. (eds.): Shape From Shading. MIT Press, Cambridge, 1989

[Isa85] Isailovic, J.: 2.4: Capacitive Videodiscs. In: Videodisc and Optical Memory Systems. Prentice-Hall, Englewood Cliffs, 1985

[Kay88] Kay, S.M.: Modern Spectral Estimation. Prentice-Hall, Englewood Cliffs, 1988

[KSX04] Kalera, M.K., Srihari, S., Xu, A.: Off-line signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence 18(7), 1339-1360, 2004

[NC07] Namboodiri, V.P., Chaudhuri, S.: On defocus, diffusion and depth estimation. Pattern Recognition Letters 28(3), 311–319, 2007

[RSA78] Rivest, R.L., Shamir, A., Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21:120–126, 1978

[Sch70] Schwartz, M.: 1: Introduction to Information Transmission. In: Information Transmission, Modulation, and Noise. McGraw-Hill, New York, 1970

[Sch02] Schaper, D.: Automated Quality Control for Micro-Technology Components Using a Depth From Focus Approach. In: Fifth IEEE Southwest Symposium on Image Analysis and Interpretation, pp. 50–54, 2002

[TB06] Tian, B., Barron, J.L.: Reproduction of sound signal from gramophone records using 3d scene reconstruction. In: Irish Machine Vision and Image Processing Conference, 2006

[Vit67] Viterbi, A.J.: Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding algorithm. IEEE Transactions on Information Theory 13(2), 260–269, 1967

[Zho09] Zhou, W.: RFID and item-level information visibility. Eur. J. Oper. Res. 198:252–258, 2009

## Authors

**Ralf Dragon** studied Electrical Engineering with a focus on information processing at the Leibniz Universität Hannover (LUH), starting in 2001. In 2005, he wrote his study thesis 'Appearance-Based Facial Motion Analysis for Model-Based Coding' at the Institutionen för Systemteknik, University of Linköping. His diploma thesis 'Camera Calibration with Movable Calibration Patterns' at the Institut für Informationsverarbeitung (TNT) got the VDE study award 2006. Ralf Dragon received his Dipl.-Ing. degree with distinction in 2006. Since 2007 he has been working towards a PhD degree at the TNT. His research interests are image interpretation and computer vision.

**Prof. Dr.-Ing. Jörn Ostermann** studied Electrical Engineering and Communications Engineering at the LUH and Imperial College London, respectively. He received Dipl.-Ing. and Dr.-Ing. from the LUH in 1988 and 1994, respectively. From 1988 till 1994, he worked as a Research Assistant at the Institut für Theoretische Nachrichtentechnik conducting research in low bit-rate and object-based analysis-synthesis video coding. In 1994 and 1995 he worked in the Visual Communications Research Department at AT&T Bell Labs on video coding. He was a member of Image Processing and Technology Research within AT&T Labs - Research from 1996 to 2003. Since 2003 he is Full Professor and Head of the TNT at the LUH, Germany.

**Prof. Dr.-Ing. Berend Denkena** studied Mechanical Engineering at the LUH. He received Dipl.-Ing. and Dr.-Ing. from the LUH in 1987 and 1992, respectively. After working as a Research Engineer at the Institute of Production Engineering and Machine Tools (IFW) conducting research on the wear of ceramic cutting tools (1987 to 1994), he became Head of Standards Engineering and Systems at Thyssen Production Systems in Auburn Hills/USA (1993 to 1995). In 1995 and 1996 he served as Head of Machining Center Development at Thyssen Hüller Hille, Ludwigsburg. From 1996 to 2001 he was Head of Engineering and Turning Machine Development at Gildemeister Turning Machines, Bielefeld. Since 2001 he is Full Professor at the LUH and Head of the IFW.

**Dr. rer. nat. Bernd Breidenstein** studied Mineralogy at the universities of Marburg and Göttingen. He received his Dr. in natural sciences from the Technical University of Clausthal (TUC) in 1989. After working for Röntgenseifert (Seifert X-rays, now GE Sensing and Inspection Technologies) as a leader of the analytical application lab, and Siemens Business Services, he changed to the IFW in 2001. Besides leading the analytics team he is doing research and teaching.

**Tobias Mörke** studied Mechanical Engineering at the LUH, starting in 2004. In 2010, he wrote his diploma thesis on the surface error prediction on peripheral milling of flexible components considering chamfered cutting tools at the IFW. He received his Dipl.-Ing. degree in 2010. Since 2010 he works towards a PhD degree at the IFW. His research interests are micro-structuring and residual stresses in machined components.