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

*Ralf Dragon*¹, Jörn Ostermann¹, Berend Denkena², Bernd Breidenstein², Tobias Mörke²

 ¹ Institut f
ür Informationsverarbeitung (TNT)
 ² Insitut f
ür Fertigungstechnik und Werkzeugmaschinen (IfW) Leibniz Universit
ät Hannover

2010-09-24

This work was funded as part of the Sonderforschungsbereich 653 by the DFG.



Self-Authentication Idea Application Examples

Inherent Data on Gentelligent Components Depth Reconstruction at Scratch Scale Image Partitioning Tracking the Reflexion Edge

Self-Authentication in Gentelligent Components

Conclusion





What is Authentication?

- Verifying genuineness, origin vs. forgery
- Means
 - Historically: Stamps and seals on deeds
 - Handwriting: Signature
 - ► Forensics: *Fingerprint*



Impression of cylinder seal, Mesopotamia, Uruk Period (4100 BC–3000 BC)



Fingerprints, taken since 19th century

Universität

lannove

What is Authentication?

- Verifying genuineness, origin vs. forgery
- Means
 - Historically: Stamps and seals on deeds
 - Handwriting: Signature
 - Forensics: Fingerprint
- Analog Authentication
 - Differences exist
 - Significance to original is detectable



Impression of cylinder seal, Mesopotamia, Uruk Period (4100 BC–3000 BC)



Fingerprints, taken since 19th century

Universität

Institut für Informationsverarbeitung

Digital Authentication

- ► Digital data can be copied exact ⇒ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)





Digital Authentication

- ► Digital data can be copied exact ⇒ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)





Digital Authentication

- ► Digital data can be copied exact ⇒ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)



- Specific to data getting signed
- Specific to authenticating entity

Digital Authentication for Objects

- Digital signature is cryptographically proved to be very strong
- Digital data is not related to real world
- Idea: Sign data describing specific component properties
 - None? Insert a random pattern!
 - Where to store data? Inherent!

Every object/component may have a different pattern for verification





Self-Authentication





Why is this self-authentication?



Prior Information

- Public key of signer needed
- Public key can also be stored in digital data structure
 - Signed by root public key
 - \Rightarrow Only prior knowledge needed: Public root certificate





Self-Authentication

Signature For Documents





Self-Authentication

Individual Bank Notes



Object to be authenticated

Analog label where a fingerprint is situated

Digital label where digital information about the fingerprint is stored





Individual Bank Notes



Object to be authenticated

Analog label where a fingerprint is situated

Digital label where digital information about the fingerprint is stored

- Individual watermarks possible
- (Money is as virtual as information)





Why Inherent?

Fingerprint

- Must be fixed to component
- Not inherent
 - Can get lost
 - Can be mixed up
- Data
 - Centralized from database
 - Accessability
 - Abuse to create forgeries
 - Not inherent
 - Can get lost
 - Can be mixed up



Self-Authentication Idea Application Examples

Inherent Data on Gentelligent Components Depth Reconstruction at Scratch Scale Image Partitioning Tracking the Reflexion Edge

Self-Authentication in Gentelligent Components

Conclusion





Gentelligent Components







Gentelligent Components









Gentelligent Components



Institut für Informationsverarbeitung

Gentelligent Components







- Micro-structured surface for data storage
- Groove wound around component
- Cut in by Piezo tool during a turning process
- Depth is varied







- Micro-structured surface for data storage
- Groove wound around component
- Cut in by Piezo tool during a turning process
- Depth is varied
- No digital structures can be created





Transmission principle

- Groove is imprint of the analog signal run of the Piezo tool
- Recovering the run means reconstructing the analog signal
- Data transmission system
- Depth reconstruction with optical means
- Re-use existing methods
- Only qualitative (no exact scaling) reconstruction needed





Depth from Directed Illumination



- Parallel illumination
- Groove consists of shadow and reflexion region
- Variation of groove depth by *d* shifts
 - shadow border by w_s
 - reflexion border by w_r
- We focus on reflexion
 - Geometry does not allow shadows and reflextions
 - Less image perturbation
- Edge tracking solves depth reconstruction qualitatively



Surface under Directed Illumination







	A REAL PROPERTY AND A REAL		THE REPORT OF A DESCRIPTION OF A DESCRIP	and the second second second
Construction of Construction o		Contraction of the second states of the second states of the		And its state of the second
A DECK OF THE OWNER	and the second	and the second	- AT	Party And Strength Manual
the second second		The second states and the	and the state of the second	
	the second s		and the second	Contraction of the second
Statement of the second se		A REAL PROPERTY OF THE REAL PR	ALL DAY IN CO. P. MICHAELER	Call Roughan Coll Manage
		and the second states of the States of the second		
and a start of the start of the start of the	Carrow Contraction of the	and the second second second	and the state of the second second	and the second second
a state of the second second		and a second	and the state of the	
	Contraction of the second s			Statement of the local division of the local
			as 10796/1437 (0007	
Carrier and a state of the second state of the	1.15 March	and the second second	a second and a second sec	A
The printer and spint the second	1			
and the second		the second second second second second	and the second se	
And the second se	No		14 Contract (11)	
	man in the first of the second	a state of the state	Construction on the Streetweet Construction	
		and the second second second second	Contraction Contractor	A COLORADOR AND
				state
	the second s	and the second second	and the second s	and the second se
And the second se	the second s	the second s		the second se
the state of the s	the second se	and the second se	the second s	and the second se
	· · · · · · · · · · · · · · · · · · ·			



54. APR	-		NUT THAT AND ADD
	2		and the states
R. Co. sect. Ex.	3	an a	Anna Anna
10 18-1	4		
And Annalis	5		
-	6		
	27	a se a construir a constru	
	8		
-	9		1
	10		
-	11		A Drew Street
	12		-
	13		
	14		
	15		- Colores
-	16		-
-	17		
-	18		
	19		
	20		Sec.
	21		Sec. Sec.
	22		and the second second
	23		
	24		
	25		
	26		
	27		
	28		
	29		
	30		
	31		
	32	a de la general de la companya de la	
	33		
and the second			
-			



- Assumption: Groove runs approximately horizontal
- Perform several spectral analyses of the image I(x, y) at column x = x_i in vertical direction
- Filtering: Horizontal moving average (noise), vertical median (cutting artifacts)
- Vertical cut forms the 1D signal f(y) which is analyzed





- Periodic reflexion area: $y = (n + \frac{1}{2})\lambda_0 + \phi_0$
- Distance λ_0 or frequency u_0
- Phase shift $\phi(u_0)$

Spectral Estimation

•
$$p(u) = 1/R \sum_r |F_r(u)|$$

- ► No phase information as φ(u) is not shift-invariant
- Phase estimation extention of average periodogram method^a

mationsverarbeitung

^aDragon et. al., DAGM 2009





14 APR -			NUT SALIDARD SH
	2	an a	and the state of
R. Co. sect	3		Anna Anna
	4		
2-1- Anna	5		
-	6		
-	7		
	8		
	9		and the second second
	10		
	11		A 2
Concession in which the	12		
-	13		
-	14		
			Contract of the local division of the
	15		State of the local division of the local div
	10		
-	17		and the second second
and the second	18		
	19	×	
	= 20		Sec.
	21		
	22		
	23		135-11-11-11-11-11-11-11-11-11-11-11-11-11
	24		
	25		
-	26		
	27		i prosente en en
	28		10 10
	29		
	30		
=2	31		
	32		
	33		
100000	-		
			the station of



Extraction of the Groove Edge

- Model appearance of the groove edge
- Model movement of the Piezo tool
- Robust to perturbations







Extraction of the Groove Edge

- Model appearance of the groove edge
- Model movement of the Piezo tool
- Robust to perturbations







Adapted HMM Model

- Each node $S_{x,y}$ models one image pixel I(x, y)
- Observation probability: $p_o(x_i, y_i|I) \propto c \frac{I(x_i, y_i+1) I(x_i, y_i-1)}{2}$
- Transition probability: $p_t(x_{i+1}, y_{i+1}|y_i) \propto \mathcal{N}(\sigma^2, y_i)$
- Groove edge $Y = (y_1, y_2, \dots, y_{s_x})$ is found with Viterbi algorithm finding maximum of $P = p_o(x_{s_x}, y_{s_x}) \prod_{i=1}^{s_x-1} p_t(x_{i+1}, y_{i+1}|y_i) p_o(x_i, y_i)$

Institut für Informationsverarbeitung



And approximately service and the service of the	AND THE PARTY OF ANY ADDRESS OF ANY	and the Wight Street and	AND A REAL PROPERTY AND A	THE REPORT OF THE PARTY AND ADDRESS OF
Contrast of the Owner of the Ow	the second second second second second	in the second second	the second second second second second	the second s
Including the second state of the second state	No. of Concession, Name of Street, or other	the restaurant water and		Contraction of the local division of the loc
		Service Print, Name Sciences		
		ARA-Administration marries of the second		
			10-01-021 million	a construction of the second sec
		Torra States - March - States	interfactorial train the second	
	white an a serie and	55		
			and the second second	and the table to a firm
and the second	Contraction of the second			and the second because the
Concerning and the second s			Contraction of the second second	
State of the local division in which the local division in the loc	Construction of the other states	Contraction of the local division of the loc		Second statements of the second statements
and designed to a designed of	and the second s			
	and the local distance of the second s		11	
	1010	1.11		
		North La Million II		
and the second s				
	and the second s			and the second
17	A DESCRIPTION OF A DESC	And the other states of the	and the second second second second	the second se
	and the second		Water of the state	And the second se
data and the pattern of the second second second	the second se	and the second se	the second s	the second se
NAMES OF TAXABLE PARTY OF TAXABLE PARTY.	the second s	CARGO AND A DESCRIPTION OF THE OWNER OWNER OF THE OWNER	CONTRACTOR OF THE PARTY OF THE PARTY OF THE	the second s
			• / · · · •	
			3 / ²	۵
			۰. 	



Self-Authentication Idea Application Examples

Inherent Data on Gentelligent Components Depth Reconstruction at Scratch Scale Image Partitioning Tracking the Reflexion Edge

Self-Authentication in Gentelligent Components

Conclusion





Fingerprint

- Imprint of grinding process
- Pseudo-random

- Sample intensity profiles using directed illumination
- Compare using NCC







NCC of Depth Profile

Component 1



	and the second se				
spanses and the second	the second	Cash of the local			
	Contraction of the local division of the loc	1000 CT 1000	Contraction And	Section of the sectio	
		COLUMN TWO IS NOT	A DECEMBER OF	AND COLUMN	
CONTRACTOR OF TAXABLE PARTY.	CT CO. Carl Participation				
- to the start of the	71.0		and the second second		
			The second second	and share the state of the	
Carlos Carlos Company	La Marcalla Contraction	And the second s		the second second	
				And the second second	
-					
and the second se	and the second second	and the second			
And Personal Property lies and the second se	-			a lot of the lot of the	
	-			a contraction of the	
NAMES OF TAXABLE PARTY.				States of Lot of	



Shifted Normalized Profile





Institut für Informationsverarbeitung

Reading out

Proceeding

- Microscope with low magnification (2.6 mm × 2 mm)
- ► Images are stitched together using ≈ 100 views
- ► Overall surface view is partitioned using ≈ 200 cuts
- Groove sections are extracted and connected









Run of the groove over one rotation

- Center of the groove wobbles (mechanical inaccuracies)
- Groove sections n and n + 1 are fused
- Exacly one groove wound around the component
- Groove center is subtracted \Rightarrow signal is available







- Inherent data storage and readout possible
 - Further error-correcting channel-code could be used
- Inherent fingerprint possible
 - Local disruptions can be overcome by using several grinding profiles





Conclusion

Self-Authentication Idea Application Example

Inherent Data on Gentelligent Components Depth Reconstruction at Scratch Scale Image Partitioning Tracking the Reflexion Edge

Self-Authentication in Gentelligent Components

Conclusion





Conclusion



General idea

- Inherently store fingerprint in digital form
- Sign digital data with a public key
- ⇒ No prior information needed besides a root public key

Self-authentication in gentelligent components

- Groove $(6 \, \mu m \pm 3 \, \mu m)$ on surface
- Reading: Directed illumination
- Data density of 1.6 kbit/cm²
- Fingerprint is grinding imprint
- Digital notation by sampled depth profiles



Data Density Calculation

Calculation

- 2-ASK: 1Bit/Symbol
- Data rate: R = 1.1/mm
- Groove distance: $d_f = 0.07 \,\mathrm{mm}$
- Density: $R \times \frac{1}{d_f} \approx 1.6 \, \text{kbit/cm}^2$

Not taken into account

- Simplified demodulation
- Cross talking
- Redundancy for error correction
- Improved modulation scheme with multiple carriers



BER for Turbo Code

2/3 redundancy



Informationsverarbeitung

100



Vertical cut

