

## Digitale Wasserzeichen

Grundlagen, Verfahren, Anwendungsgebiete

Bearbeitet von  
Jana Dittmann

1. Auflage 2000. Taschenbuch. xii, 183 S. Paperback

ISBN 978 3 540 66661 5

Format (B x L): 15,5 x 23,5 cm

Gewicht: 305 g

[Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit, Geschäftsssoftware > Zeichen- und Zahlendarstellungen](#)

schnell und portofrei erhältlich bei

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

# Inhaltsverzeichnis

<b>1</b>	<b>Motivation und Einführung .....</b>	1
1.1	Problembeschreibung .....	3
1.2	Der Ansatz .....	4
1.2.1	Aufstellung eines Klassifikationsschemas .....	4
1.2.2	Erforschung verbesserter Wasserzeichenverfahren auf der Grundlage des Klassifikationsschemas.....	4
1.3	Gliederung des Buches .....	6
1.3.1	Grundlegende Aspekte zur Sicherheit in Multimediaapplikationen .....	6
1.3.2	Grundlagen digitaler Wasserzeichen und das Klassifikationsschema.....	6
1.3.3	Neuartige Wasserzeichenverfahren .....	7
1.3.4	Anwendungen, offene Probleme.....	7
<b>2</b>	<b>Allgemeine Sicherheitsanforderungen in Multimedia-Applikationen.....</b>	9
2.1	Begriff „Multimedia“ .....	9
2.2	Security – Allgemeine Sicherheitsanforderungen.....	10
2.3	Konzepte für das Sicherheitsmanagement.....	12
2.3.1	Kryptographie .....	12
2.3.2	Steganographie.....	14
2.3.3	Digitale Wasserzeichen.....	16
<b>3</b>	<b>Digitale Wasserzeichen .....</b>	19
3.1	Grundlagen digitaler Wasserzeichen.....	19
3.1.1	Definition und Terminologie .....	19
3.1.2	Verfahrensgrundlagen.....	22
3.1.3	Verfahrensparameter.....	24
3.1.4	Durchführung von Qualitätstests zur Robustheit: Benchmarking .....	28
3.2	Klassifizierung der Wasserzeichen.....	29
3.2.1	Klassifikationsmerkmal erste Ebene: Anwendungsgebiet.....	30
3.2.2	Klassifikationsmerkmal zweite Ebene: Verfahrensparameter ..	31
3.2.3	Klassifikationsmerkmal: Resistenz gegen Attacken.....	33

<b>4 Nicht-wahrnehmbare robuste Wasserzeichen zur Urheberidentifizierung .....</b>	43
4.1 Wasserzeichen für Einzelbilder.....	44
4.1.1 Generelle Verfahrensgrundlagen .....	44
4.1.2 Stand der Technik .....	46
4.1.3 Verfahrensentwurf zur Optimierung von Robustheit und Sichtbarkeit .....	52
4.2 Wasserzeichen für Bewegtbilder.....	75
4.2.1 Anforderungen an Bewegtbildwasserzeichen.....	75
4.2.2 Stand der Technik .....	77
4.2.3 Anpassung des Einzelbildverfahrens für Videos .....	78
4.3 Wasserzeichen für Audiodaten.....	88
4.3.1 Anforderungen an Verfahren für Audiodaten.....	88
4.3.2 Stand der Technik .....	89
4.3.3 Entwurf eines Audiowasserzeichenverfahrens für komprimiertes Datenmaterial als Ergänzung zum Videowasserzeichen.....	92
4.4 Wasserzeichen für 3D-Modelle.....	102
4.4.1 Stand der Technik .....	103
4.4.2 3D-Szenen-Markierungen auf Basis von Bild- und Tonwasserzeichen .....	106
4.4.3 Markierungsverfahren von VRML-Knoten .....	107
<b>5 Digitale Fingerabdrücke zur Kundenidentifizierung .....</b>	115
5.1 Lösungsansatz.....	115
5.2 Algorithmus zur Erstellung von kollisionssicheren Fingerabdrücken .....	116
5.2.1 Zwei einfache Beispiele .....	117
5.3 Wasserzeichenverfahren für kollisionssichere Fingerabdrücke für Bilddaten .....	119
5.3.1 Wasserzeichenalgorithmus .....	120
5.3.2 Einbringen des Fingerprints .....	121
5.3.3 Fingerprint-Abfrage .....	124
5.3.4 Testergebnisse .....	128
5.4 Bewertung und Verallgemeinerung des Verfahrens auf andere Medienströme .....	133
<b>6 Nicht-wahrnehmbare fragile Wasserzeichen zur Integritätsprüfung .....</b>	135
6.1 Lösungsansatz.....	136
6.2 Merkmalsvektoren für Bildmaterial zur Integritätsprüfung: der Inhaltsauszug .....	137
6.3 Wasserzeichen zur Integritätsprüfung über die Kantencharakteristik von Bildern.....	140
6.3.1 Die Kantenextraktion: Bildung des Merkmalsvektors.....	141
6.3.2 Erstellung des kantenabhängigen Wasserzeichens .....	141

6.3.3	Toleranz gegen zugelassene Bildverarbeitung.....	142
6.3.4	Sicheres inhaltsbezogenes fragiles Wasserzeichen.....	145
6.3.5	Nachweis der Urheberrechtsverletzung auf Basis doppelter Muster unter Verwendung robuster Wasserzeichen .....	145
6.3.6	Blockbasierte Wasserzeichen zur punktuellen Manipulationsdetektion.....	146
6.3.7	Bewertung der Farbe.....	146
6.3.8	Problem bei vielen Kanten im Bild.....	146
6.4	Verallgemeinerung auf andere Medienströme .....	147
<b>7</b>	<b>Offene Probleme und Herausforderungen.....</b>	<b>149</b>
7.1	Wasserzeichenverfahren mit einem sicheren öffentlichen Detektor....	149
7.2	Laufzeiteffizienz und Robustheit gegen kombinierte Angriffe.....	149
7.3	Security Betrachtungen der Verfahren .....	150
7.4	Wasserzeichen für Audio und 3D-Modelle .....	150
7.5	StirMark für Audio und 3D .....	150
7.6	Evaluierung von fragilen Wasserzeichentechniken .....	150
7.7	Messung des visuellen Qualitätsverlustes .....	151
7.8	Verfahrenstransparenz: Einordnung der Verfahren in das Qualitätsschema .....	151
7.9	Kombination von Medienströmen: Copyright und Integrität.....	151
7.10	Wasserzeichenverfahren als Urheber- und Integritätsnachweis für biometrische Merkmale .....	152
7.11	Notwendigkeit und Umsetzungsmöglichkeiten von Copyrightinfrastrukturen .....	152
7.11.1	Robustheitsgarantien: Zertifizierte Wasserzeichenverfahren .....	152
7.11.2	Schlüsselverwaltung .....	152
7.11.3	Standardisierung der einzubringenden Copyrightinformationen.....	153
<b>8</b>	<b>Anwendungen .....</b>	<b>155</b>
8.1	DVD.....	155
8.2	Security-Gateways.....	159
8.3	MPEG-7-Applikationen .....	160
<b>9</b>	<b>Zusammenfassung und Ausblick .....</b>	<b>163</b>
<b>10</b>	<b>Anhang.....</b>	<b>167</b>
10.1 (1)	VRML IndexedFaceSet Knoten.....	167
10.2 (2)	Details zum mathematischen Modell von Schwenk/Ueberberg.....	167
	<b>Literaturverzeichnis.....</b>	<b>173</b>
	<b>Index .....</b>	<b>181</b>