

Xpert.press

Springer-Verlag Berlin Heidelberg GmbH

Die Reihe Xpert.press des Springer-Verlags vermittelt Professionals in den Bereichen Betriebs- und Informationssysteme, Software Engineering und Programmiersprachen aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Jana Dittmann

Digitale Wasserzeichen

Grundlagen, Verfahren,
Anwendungsgebiete

Mit 38 Abbildungen, 38 Tabellen
und CD-ROM



Springer

Jana Dittmann
GMD-Forschungszentrum Informationstechnik
Institut für Integrierte Publikations-
und Informationssysteme (IPSI)
Dolivostraße 15, 64293 Darmstadt

ISBN 978-3-540-66661-5

Additional material to this book can be downloaded from <http://extras.springer.com>

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Dittmann, Jana: Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete/

Jana Dittmann. - Berlin; Heidelberg; New York; Barcelona; Hongkong; London;

Mailand; Paris; Singapur; Tokio: Springer, 2000

(Xpert.press)

ISBN 978-3-540-66661-5 ISBN 978-3-642-56971-5 (eBook)

DOI 10.1007/978-3-642-56971-5

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

© Springer-Verlag Berlin Heidelberg 2000

Ursprünglich erschienen bei Springer-Verlag Berlin Heidelberg New York 2000

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutzgesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: Künkel + Lopka, Heidelberg

Satz: Datenkonvertierung durch perform, Heidelberg

SPIN: 10737497 33/3142 GF 543210

Vorwort

Digitale Wasserzeichen sind seit Anfang der 90er Jahre verstärkt Thema in der Wissenschaft und Wirtschaft, um die Authentizität von Mediendaten zur Durchsetzung von Urheberrechten zu gewährleisten und die Unversehrtheit (Integrität) der Mediendaten nachweisen zu können. Am Institut für Integrierte Publikations- und Informationssysteme (IPSI) im GMD-Forschungszentrum Informationstechnik GmbH in Darmstadt entstanden (und entstehen) durch die Arbeiten von Frau Dr.-Ing. Jana Dittmann signifikante wissenschaftliche Fortschritte. Wesentliche Ergebnisse werden in diesem Buch vorgestellt:

Die heute existierenden Verfahren sind bisher fast alle sehr anwendungsspezifisch und zeigen in hohem Maße uneinheitliche Verfahrensparameter sowie teilweise sehr geringe „Sicherheitsniveaus“. Es fehlen einheitliche Definitionen von Qualitätsparametern, um u.a. die Verfahren vergleichbar zu machen. An dieser Stelle setzt die Arbeit an: Es wird ein medienunabhängiges Klassifikationsschema für Wasserzeichen vorgestellt, das als Grundlage für die erstmalige breitere Strukturierung des Gebietes dient. Dabei wird in systematischer Weise deutlich herausgearbeitet, welche praktischen Anwendungsgebiete digitale Wasserzeichen belegen und welche Anforderungen sie erfüllen müssen. Dies bildet die Grundlage für eine Qualitätsbewertung von Wasserzeichen.

Aus der Vielzahl der Wasserzeichen des Klassifikationsschemas behandelt Frau Dittmann in diesem Buch im Detail robuste Wasserzeichen zur Urheberidentifizierung und Kundenmarkierung sowie fragile Wasserzeichen zum Integritätsnachweis.

Es werden neue Vorgehensweisen zur zuverlässigen Detektion der Wasserzeichen (auch nach einer Medienverarbeitung) vorgestellt. Die Arbeiten für Bildmaterial auf Basis sogenannter selbst spannender Wasserzeichenmuster (SSP Self Spanning Pattern) zeigen vielversprechende Möglichkeiten. Bisherige Verfahren versuchen Medienoperatoren aufzuspüren und rückgängig zu machen, um das Wasserzeichen korrekt auslesen zu können. Der vorgestellte SSP-Ansatz verfolgt eine gänzlich neue Vorgehensweise. Da auf bild-inhärenten Eigenschaften gearbeitet und das Muster über diese Eigenschaften eingebracht wird, müssen Medienoperatoren nicht mehr erkannt und rückgängig gemacht werden.

Für sogenannte „Kundenmarkierungen“ wird erstmals ein mathematisches Modell in ein Wasserzeichenverfahren für Bilddaten umgesetzt, das es erlaubt, sogar nach Koalitionsangriffen von mehreren Kunden, die das Wasserzeichen zerstören wollen, direkt auf die zusammenarbeitenden Kunden zu schließen.

Im Bereich fragile Wasserzeichen zur Manipulationsdetektion wird ein Verfahren dargestellt, das ein robustes Wasserzeichenverfahren als Träger nutzt und direkt auf dem Inhalt von Bilddaten arbeitet. Dieses Verfahren kann etwa Skalierung und Kompression von direkten Manipulationen, die zu deutlichen Veränderungen im Datenmaterial führen, unterscheiden.

Darmstadt, im April 2000

Ralf Steinmetz

Inhaltsverzeichnis

1	Motivation und Einführung	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
2	Allgemeine Sicherheitsanforderungen in Multimedia-Applikationen	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
3	Digitale Wasserzeichen	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

4	Nicht-wahrnehmbare robuste Wasserzeichen zur Urheberidentifizierung	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
5	Digitale Fingerabdrücke zur Kundenidentifizierung	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
6	Nicht-wahrnehmbare fragile Wasserzeichen zur Integritätsprüfung	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
7	Offene Probleme und Herausforderungen.....	149
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
8	Anwendungen	155
8.1	DVD.....	155
8.2	Security-Gateways.....	159
8.3	MPEG-7-Applikationen	160
9	Zusammenfassung und Ausblick	163
10	Anhang.....	167
10.1	(1) VRML IndexedFaceSet Knoten.....	167
10.2	(2) Details zum mathematischen Modell von Schwenk/Ueberberg.....	167
	Literaturverzeichnis.....	173
	Index	181

Abbildungsverzeichnis

Abbildung 1:	Steganographische Grundprinzipien: Einbetten und Auslesen mit symmetrischem Schlüssel	15
Abbildung 2:	Wasserzeichenmuster in einem Foto	21
Abbildung 3:	A) Genereller Einbettungs- und B) Abfrageprozeß	24
Abbildung 4:	StirMark Angriff auf das Wasserzeichen	35
Abbildung 5:	Mosaikattacke für Bildmaterial	36
Abbildung 6:	Invertierbarkeitsproblem	37
Abbildung 7:	Mustergenerierung	55
Abbildung 8:	Generiertes 8x8 Muster aufgespannt über 64x64 Bildpunkten	55
Abbildung 9:	Markierungspunkte aus dem Kantenbild	57
Abbildung 10:	Beispiel dreier geometrischer Figuren	58
Abbildung 11:	Vierer-Gruppe mit Initial- und PointPattern in der geometrischen Figur	59
Abbildung 12:	Struktur von InitialPattern, PointPattern, WatermarkPattern	59
Abbildung 13:	Eingebrachte Wasserzeichenmuster am Beispiel einer Vierer-Gruppe	64
Abbildung 14:	Wirkung von StirMark	66
Abbildung 15:	Schema: Schutz von Bildbereichen	80
Abbildung 16:	Genereller Ablauf für das Audiowasserzeichen	94
Abbildung 17:	Einbringen eines Informationsbits	96
Abbildung 18:	4 Dreiecksmaschen eines Gittermodells als ein Macro-Embedding-Primitive	104
Abbildung 19:	Polygonales Maschennetz mit Zeigern auf eine Scheitelpunktsliste	108
Abbildung 20:	Beispiel zur Referenzierung der Scheitelpunkte	109
Abbildung 21:	Eine 2-detektierendes Fingerprinting-Schema	118
Abbildung 22:	Ein Tetraeder als ein Beispiel für 3-detektierendes Fingerprinting-Schema	119
Abbildung 23:	Schema Einbringen des Fingerprints	121
Abbildung 24:	Bild mit Markierungsblöcken und Redundanz r_1	122
Abbildung 25:	Einbringen des Informationsbits x_1 in die DCT Koeffizienten für x_{11}	124
Abbildung 26:	Abfrageschema	125
Abbildung 27:	Abfrage aus den DCT-Koeffizienten	127
Abbildung 28:	Berechnung der Differenzansicht von zwei markierten Bildern	131
Abbildung 29:	Manipulationen in der Darstellung	136
Abbildung 30:	Blockstruktur über die Kantencharakteristik EC	143
Abbildung 31:	Erkennen von Manipulationen mit Hilfe des binären Blockschemas	144
Abbildung 32:	Schematische Vorgehensweise bei der Mustererzeugung mit EC	144
Abbildung 33:	Sicheres inhaltsbasiertes fragiles Wasserzeichen	145
Abbildung 34:	Vorgehensweise: Suche nach Veränderungen des Inhalts	146
Abbildung 35:	Ablauf im Gateway in 10 Schritten	160
Abbildung 36:	Das MH-Schema in $PG(2,2)$	170
Abbildung 37:	Anschauliche Darstellung des Schwenk-Ueberberg-Ansatzes im dreidimensionalen Raum	170
Abbildung 38:	Nicht eindeutige Decodierung von Fingerabdrücken	171

Tabellenverzeichnis

Tabelle 1:	Die wichtigsten Sicherheitsanforderungen	11
Tabelle 2:	Wasserzeichenverfahren und ihre Verfahrensanforderungen	32
Tabelle 3:	Wasserzeichenverfahren und ihre Qualitätsparameter.....	40
Tabelle 4:	Grundlegende Medienverarbeitungsoperatoren.....	41
Tabelle 5:	Bewertung der existierenden Einzelbildverfahren	52
Tabelle 6:	Gespannte Muster	68
Tabelle 7:	Fehlerkennungsraten für midgray.ppm.....	70
Tabelle 8:	Fehlerkennungsraten für lena.ppm	71
Tabelle 9:	Fehlerkennungsraten nach der Anwendung von StirMark	72
Tabelle 10:	Bewertung des Einzelbildverfahrens	74
Tabelle 11:	Bewertung der existierenden Videoverfahren	78
Tabelle 12:	Fehlerkennungsraten für midgray.mpg.....	83
Tabelle 13:	Fehlerkennungsraten für org-volvo-12.mpg	84
Tabelle 14:	Fehlerkennungsraten nach der Anwendung von StirMark	85
Tabelle 15:	Bewertung des Videoverfahrens.....	87
Tabelle 16:	Bewertung der existierenden Audioverfahren	92
Tabelle 17:	Skalenfaktoren für eine Gruppe von 8 Frames	97
Tabelle 18:	Differenzenfenster in x- und y-Richtung über die Skalenfaktoren	97
Tabelle 19:	Differenzenfenster	98
Tabelle 20:	Bestimmung eines ähnlichen Musters auf den Skalenfaktordifferenzen	98
Tabelle 21:	Gefundenes Muster.....	99
Tabelle 22:	Differenz.....	99
Tabelle 23:	Geändertes Muster.....	99
Tabelle 24:	Bewertung des Audioverfahrens.....	102
Tabelle 25:	Zusammenfassung der Robustheitsaussagen	105
Tabelle 26:	Bewertung der existierenden 3D-Verfahren	106
Tabelle 27:	Bewertung des VRML-Verfahrens.....	114
Tabelle 28:	$n \times r_1$ Markierungspositionen mit Redundanz r_1	122
Tabelle 29:	Zufallsmarkierungsfolgen $R_{i,j}$	123
Tabelle 30:	Quantisierungsmatrix.....	123
Tabelle 31:	$n \times r_1$ Markierungspositionen mit Redundanz r_1 im Abfrageprozeß	126
Tabelle 32:	Zufallsmarkierungsfolgen $R_{i,j}$	126
Tabelle 33:	Testergebnisse grundlegender Angriffe bzw. Bildtransformationen	130
Tabelle 34:	Testergebnisse der Fingerprint-Angriffe	131
Tabelle 35:	Bewertung des Wasserzeichenverfahrens für Fingerabdrücke	133
Tabelle 36:	Auswahl relevanter Merkmalsvektoren.....	138
Tabelle 37:	Zugelassene und zu erkennende Bildveränderungen und deren Auswirkungen.....	139
Tabelle 38:	VRML IndexedFaceSet Knoten	167