Digitale Wasserzeichen

Bilddaten sicher übertragen

Techniken des „Watermarking“ und die digitale Signatur werden künftig für den Bildtransfer in der Medizin wichtig.

Thomas M. Lehmann

Watermarking bedeutet das Einbringen von Wasserzeichen in Bildern. Mit unsichtbaren Wasserzeichen wird Information versteckt (so genanntes Information Hiding, 7). Bereits aus dem alten China sind Techniken überliefert, um Nachrichten zu verstecken. Sender und Empfänger haben eine spezielle Lochmaske („Cardan-Gitter“), die, über einen Text gelegt, die eigentliche Nachricht aus den darunter liegenden Buchstaben extrahiert. Die Systematisierung des Information Hiding in den Weltkriegen führte zur Kryptologie als Wissenschaft von der Geheimhaltung von Nachrichten (5). Die ersten technischen Prinzipien stellte 1883 Auguste Kerckhoffs auf (8). Er postulierte, dass die Methode, mit der Nachrichten verschlüsselt werden, nicht auf Dauer geheim gehalten werden kann und somit die Sicherheit nicht aus der Methode selbst, sondern nur aus dem Schlüssel abgeleitet werden darf. Dies ist als Kerckhoffssches Prinzip auch heute noch gültig und wird zum Beispiel bei der digitalen Signatur angewendet.

Obwohl in vielen Bereichen der digitalen Medienwelt bereits eingesetzt und perfektioniert, sind Watermarking-Techniken für medizinische Bilder derzeit noch weit von Routineanwendungen entfernt. Dennoch nimmt die Zahl der wissenschaftlichen Fachbeiträge kontinuierlich zu, in denen die Möglichkeiten dieser Technologie systematisch untersucht werden (13, 12, 10, 2).

Medizinische Anwendungsszenarien

Die denkbaren Anwendungen von Watermarking-Techniken in der Medizin decken ein breites Spektrum ab. Hierbei lassen sich zwei Kernszenarien identifizieren, die die Sicherheit der Information betreffen *(Abbildung 1)*. Nach der inter-

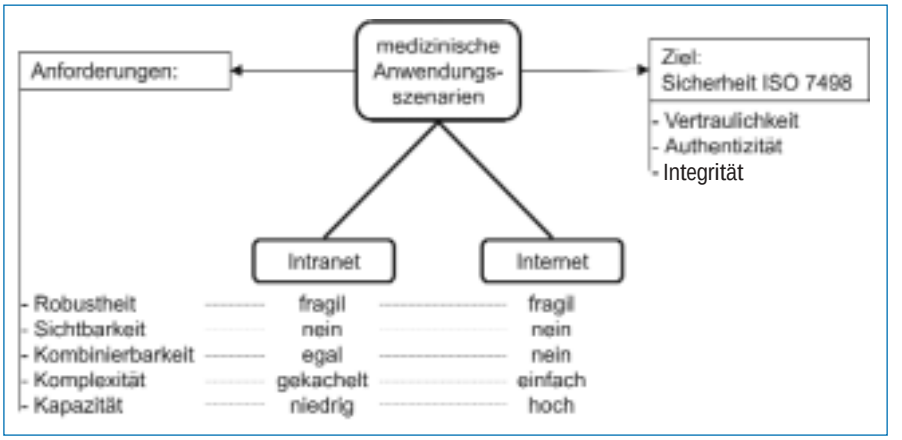

Abbildung 1: Ziele und Anforderungen der medizinischen Anwendungsszenarien für digitale Wasserzeichen

nationalen Norm ISO 7498-2 ist die Sicherheit von digitalen Daten durch drei Komponenten gegeben (6):

1. **Vertraulichkeit** bedeutet, dass die Information nur demjenigen zugänglich wird, für den sie bestimmt ist, aber anderen Individuen, Institutionen oder Prozessen verschlossen bleibt. Damit ist die Gewährleistung von Vertraulichkeit ein Kernelement der Kommunikation patientenbezogener Daten.

2. Die **Authentizität** oder Echtheit gewährleistet, dass die Information tatsächlich von dem in der Nachricht angegebenen Sender stammt. Beispielsweise ist also das Senderfeld, das in den gängigen E-Mail-Programmen als Absender-E-Mail-Adresse angezeigt wird, nicht authentisch im Sinne der ISO-Norm, denn es kann beliebig gesetzt und auch im Nachhinein noch modifiziert werden.

3. Die **Integrität** einer Nachricht sichert die Unversehrtheit oder Unverfälschtheit der beim Empfänger eingegangenen Information. In der Medizin ist Integrität von Bildern vor allem wichtig, um Manipulationen im Bild oder in einzelnen Bildbereichen ausschließen zu können. Dabei spielt es keine Rolle, ob eventuelle Änderungen durch Übertragungsfehler auf dem Transport entstanden sind oder – aus welchen Gründen auch immer – absichtlich eingebracht wurden.

- **Internet:** Die Übertragung von medizinischen Daten über öffentliche Netzwerke stellt eines der Kernszenarien medizinischer Anwendungen des digitalen Wasserzeichens dar. Während im Intranet eines Krankenhauses die Sicherheit der Daten in der Regel durch Abschottung des gesamten Netzes mit einer Firewall gewährleistet wird (1), ist ein medizinischer Datensatz, der über das öffentliche Internet übermittelt wird, fremden Zugriffen ungeschützt zugänglich. Ein solcher Transfer ist in teleradiologischen Anwendungen oder auch im Hinblick auf die elektronische Patientenakte unumgänglich. Nur so können die Daten zum Patienten oder zu einem kooperierenden niedergelassenen Arzt weltweit übertragen werden.

Nach gängigen Standards zum Bildtransfer, wie zum Beispiel dem DICOM(Digital Imaging and Communication in Medicine)-Protokoll (4), werden die patientenbezogenen Daten in Form eines Headers den Bilddaten vorangestellt. Damit können diese auch einfach getrennt oder vertauscht werden. Mit Watermarking-Techniken können diese Informationen hingegen unsichtbar in das Bild selbst eingebracht werden und sind damit nicht mehr vom Bild trennbar. Bei diesem Anwendungsszenario stehen somit die Vertraulichkeit und die Authentizität der Information im Vordergrund. Verletzungen der Integrität müssen lediglich erkannt werden, damit eine erneute Übertragung initiiert werden kann.

- **Intranet:** Innerhalb des Krankenhausnetzwerkes können ganz andere Anforderungen von primärem Interesse sein. Zwar werden Bildtransformationen und Änderungen, die der Arzt während der Diagnose vornimmt, mit DICOM standardisiert protokolliert, aber auch hier ist der Fall denkbar, dass diese Zusatzinformation – da nicht direkt mit dem Bild verknüpft – im Nachhinein verloren gegangen ist. Die Diskussion, ob solche Manipulationen an den Bilddaten mutwillig, zufällig oder durch Fehlbedienung von Software entstanden sein können, ist dabei ohne Belang. Deutlich wird jedoch, dass im internen Bereich eines Krankenhausinformationssystems (KIS) die Integrität der Daten im Vordergrund steht. Neben der Feststellung, dass ein Bild manipuliert wurde, ist unter Umständen auch von Interesse, an welchen Stellen oder wie stark das vorhandene Bild vom originalen abweicht.

Grundlegende Eigenschaften von Wasserzeichen

Anhand dieser beiden generellen Szenarien lässt sich verdeutlichen, dass für die verschiedenen Anwendungen unterschiedliche Eigenschaften von Wasserzeichen erforderlich sind.

- **Robustheit und Sicherheit:** Beim Watermarking bezeichnet „Robustheit“ die Resistenz eines Wasserzeichens gegenüber willkürlichen Änderungen des Bildes, wohingegen „Sicherheit“ die Resistenz gegen gezielte Angriffe auf das Wasserzeichen unter Kenntnis verfahrensspezifischer Eigenschaften meint. Ein Verfahren ist robust, wenn die eingebrachte Information zuverlässig aus dem Bild wieder ausgelesen werden kann, auch wenn dies zwischenzeitlich modifiziert, aber dabei nicht vollständig zerstört wurde. Die betrachteten Bildmodifikationen reichen dabei je nach Anwendung von geometrischen Transformationen, wie zum Beispiel Änderungen der Größe, lineare und nichtlineare Filterung, Kontrastoptimierungen und verlustbehaftete Kompression, bis hin zum Ausdruck eines digitalen Bildes und

dessen Wiedereinscannen. Es gibt heute bereits derart robuste Verfahren, dass diese aufgrund eines daumengroßen Schnipsels beliebiger Form von einem einfachen Tintenstrahlausdruck im A5-Format das Originalbild identifizieren können, selbst wenn dieser Schnipsel zu klein ist, als dass das zugehörige Bild von einem menschlichen Betrachter eindeutig identifiziert werden könnte (3). Neben robusten Wasserzeichen spricht man von fragilen, wenn diese schon bei kleinsten lokalen Änderungen zerstört werden, und von semifragilen, wenn lediglich kleinere Modifikationen des Bildes möglich sind, ohne dass das Wasserzeichen zerstört wird.

- **Sichtbarkeit, Wahrnehmbarkeit und Detektierbarkeit:** Je nach Anwendung können sichtbare oder unsichtbare Wasserzeichen sinnvoll sein. Die unsichtbaren Wasserzeichen können begrifflich weiter abgestuft werden. Man unterscheidet die Wahrnehmbarkeit in Bezug auf das visuelle System des Menschen und die Detektierbarkeit im Hinblick auf die Erkennung der Tatsache, dass ein Wasserzeichen im Bild vorhanden ist. Beispielsweise ist ein nicht wahrnehmbares Wasserzeichen detektierbar, wenn sich durch das Einbringen des Wasserzeichens grundlegende Parameter des Bildrauschens derart ändern, dass dies durch eine statistische Analyse nachweisbar ist.
- **Kombinierbarkeit und Invertierbarkeit:** Die Kombinierbarkeit von Watermarking-Verfahren zielt auf das spezielle Design hybrider Algorithmen ab. So kann es sinnvoll sein, ein fragiles und ein robustes Wasserzeichen miteinander zu kombinieren. Dies ist nur dann möglich, wenn die Verfahren kombinierbar sind, das heißt sich gegenseitig nicht beeinflussen oder gar zerstören. Das Invertierbarkeitsproblem erfasst die detektierbare Reihenfolge von Wasserzeichen. Wird in ein Bild von einer Instanz A das Wasserzeichen A eingebracht und in das so markierte Bild von einer Instanz B das Wasserzeichen B, dann kann bei invertierbaren Verfahren nicht mehr festgestellt werden, in welcher Reihenfolge die Markierung erfolgte, und damit, wer der eigentliche Urheber des Bildes ist. Sind die Wasserzeichen robust und unsichtbar beziehungsweise nicht detektierbar, dann verläuft ein Authentizitätstest des Bildes bezüglich des Urhebers A genauso positiv ab wie bezüglich des Urhebers B. Dies ist ein für viele Anwendungen jedoch unerwünschter Effekt.
- **Komplexität und Kapazität:** Die Parameter Komplexität und Kapazität beschreiben technische und algorithmische Eigenschaften von Watermarking-Verfahren. Die Komplexität beschreibt den Rechenaufwand, der notwendig ist, um das Wasserzeichen einzubetten oder zu extrahieren. Dieser hängt von der jeweiligen Implementierung des Verfahren ab, sollte im Allgemeinen jedoch möglichst niedrig sein. Die Komplexität kann als Anzahl notwendiger Operationen oder auch einfach als Laufzeit einer Implementierung angegeben werden. Die Kapazität eines Verfahrens gibt an, wie komplex das Wasserzeichen selbst sein darf. Sie beschreibt also den Informationsumfang der Marke, die im Bild kodiert wird. Oft besteht eine direkte Abhängigkeit zwischen der Kapazität und der Sichtbarkeit. Je mehr Information im Bild versteckt werden muss, desto eher kann man erkennen, dass überhaupt versteckte Information im Bild enthalten ist.

Mit Blick auf die medizinischen Anwendungsszenarien lässt sich grundsätzlich feststellen, dass unsichtbare und auch nicht wahrnehmbare Wasserzeichen benötigt werden. Schließlich darf das Wasserzeichen die medizinische Information im Bild nicht verfälschen oder gar verdecken.

Im Bereich des Internets, also zum Beispiel für teleradiologische Anwendungen, muss das Wasserzeichen fragil sein, um mögliche Änderungen zu indizieren und eine neue Übertragung des Bildes zu initiieren. Es sollte nicht kombinierbar sein, sodass auch kein Invertierungsproblem entstehen kann. Da unter Umständen viele Bilder transferiert werden müssen, sollte zumindest das Entschlüsselungsverfahren eine geringe Komplexität haben. Außerdem ist eine relativ hohe Kapazität gefordert, wenn umfangreiche Patienteninformationen mit dem Bild verbunden werden sollen *(Abbildung 1)*.

Im Bereich des Intranets sind die Parameter Komplexität und Kapazität nicht von so hoher Relevanz. Als Wasserzeicheninformation mag ein einfacher Bild-Identifier ausreichen, und in der bekannten Umgebung des eigenen Computernetzwerks lassen sich ausreichend Berechnungskapazitäten bereitstellen, die eine

höhere Verfahrenskomplexität auffangen können. Stattdessen möchte man bei möglichen Bildänderungen Rückschlüsse auf den Bereich im Bild ermöglichen, der verändert wurde. Dies kann im einfachsten Fall durch eine Kachelung eines kleinen Basiszeichens erfolgen, das zeilen- und spaltenweise wiederholt in das Bild eingebracht wird. Sind alle fragilen Basiszeichen korrekt, dann wurde das Bild nicht verändert. Können hingegen einige Basiszeichen aus einem vorliegenden Bild nicht mehr extrahiert werden, lässt sich über deren Position auf den Ort der Bildmodifikation oder Bildstörung schließen *(Abbildung 1)*.

Techniken des digitalen Wasserzeichens

Wie kann ein nicht sichtbares fragiles Wasserzeichen technisch generiert werden? Hierzu gibt es in der nichtmedizinischen Literatur viele Verfahrensansätze, die man prinzipiell jedoch in zwei Klassen einteilen kann (7, 5). Eine Gruppe von Verfahren arbeitet im Bildbereich, die andere im Bildfrequenzbereich.

- **Techniken im Ortsbereich:** Zunächst kann man sich die in das Bild einzubringende Information als binäre Bitfolge vorstellen, die auf die Pixelkoordinaten des Bildes verteilt wird. Im Hinblick auf die geforderte Nicht-Sichtbarkeit des Wasserzeichens ist eine gleichmäßige Verteilung vorteilhaft. Zunächst müssen die exakten Koordinaten festgelegt werden, in denen die Wasserzeicheninformationen eingebracht werden sollen. Dies ist beispielsweise durch eine Art Cardan-Gitter möglich. Dann sind dem Sender und Empfänger des Bildes die gleichen Koordinaten a priori bekannt, an denen sich eineWasserzeicheninformation befindet. „Eleganter“ sind Pseudozufallsfolgen, bei denen die tatsächlichen Koordinaten nach einem bestimmten Algorithmus, zum Beispiel aus der Bilddimension, eindeutig generiert werden. Der Least-Significant-Bit(LSB)-Algorithmus ist ein einfaches Beispiel für ein Wasserzeichen im Ortsbereich. Hier wird an den betrachteten Koordinaten das jeweils unbedeutendste Bit des binären Pixelgrauwerts verwendet, um die Wasserzeicheninformation aufzunehmen. Damit wird der tatsächliche Grauwert an der Bildstelle um maximal einen Grauwert verändert. Zum Beispiel wird hierbei aus dem Grauwert 54 der Grauwert 55 oder aus dem Grauwert 255 der Grauwert 254. Die resultierenden Effekte sind kaum wahrnehmbar *(Abbildung 2)*.

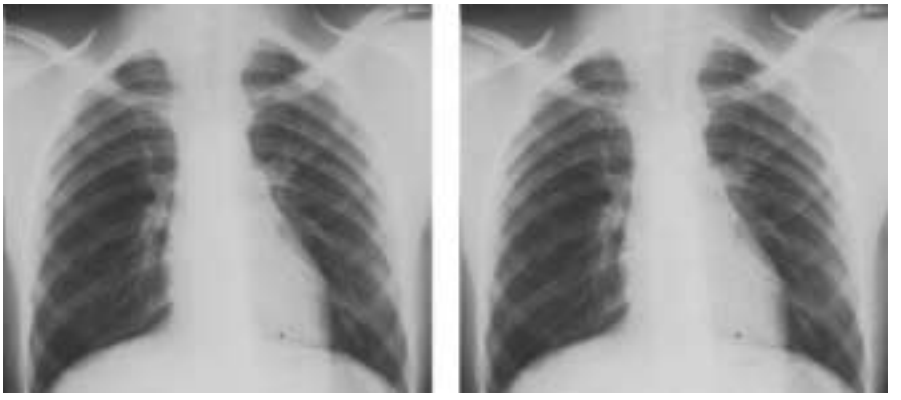

Abbildung 2: LSB-Verfahren. Röntgenbild mit 8-Bit-Quantisierung (256 Graustufen) ohne (links) und mit (rechts) LSB-Modifikationen. In einem Bild mit 512 × 512 Pixeln lassen sich circa 32 000 Textzeichen unterbringen. Dies entspricht 16 Schreibmaschinenseiten. Um den resultierenden Rauscheffekt deutlich zu machen, wurde nicht das letzte Bit, sondern das drittletzte Bit modifiziert.

- **Techniken im Frequenzbereich:** Andere Techniken transformieren das Bild zunächst in den Frequenzbereich, in dem dann Frequenzparameter modifiziert werden. Solche Frequenzverfahren sind in der Regel weniger sichtbar oder erkennbar als Verfahren, die im Ortsbereich arbeiten, denn eine Bitmodifikation eines Frequenzparameters verteilt sich auf das ganze Bild.

- **Adaptive Verfahren:** Diese zwei einfachen Grundkonzepte lassen erahnen, dass es eine Vielzahl von Kombinationen und Koppelungen der verschiedensten Mechanismen gibt. Sind grundlegende Bildbereiche wie Objekt und Hintergrund bekannt oder einfach und automatisiert detektierbar, kann die Einbringung des Wasserzeichens auch lokal adaptiv erfolgen. Zum Beispiel wird die Wasserzeicheninformation nur im Bildhintergrund eingebracht. Das hat insbesondere bei medizinischen Anwendungen den Vorteil, dass die eigentlich wichtige Bildinformation im Objektbereich unverändert bleibt. Bei Bedarf kann ein Bild auch um einen Rahmen erweitert werden, der dann wie ein Hintergrund behandelt wird.

Beispielanwendung: Digital Envelope

Das Kinderkrankenhaus der University of Southern California ist im Bereich der digitalen Bildverarbeitung und der PACS (Picture Archiving and Communication Systems) eines der führenden Institute in der Welt. Hier hat man bereits vor sechs Jahren begonnen, die Anwendung von Wasserzeichen in medizinischen Bildern zu erproben, um die Sicherheit bei teleradiologischen Anwendungen zu optimieren. Das hieraus entstandene Verfahren nennen die Autoren „Digital Envelope“ (2).

Ausgangspunkt ist die Übertragung eines medizinischen Bildes und der zugehörigen Patienteninformation über die das KIS schützende Firewall hinaus zu einem dezidierten Empfänger irgendwo im unsicheren Internet. Nur dieser soll in der Lage sein, die Patienteninformation zum Bild zu entschlüsseln. Außerdem soll er sich sicher sein können, dass das Bild nicht verändert wurde und auch vom Children’s Hospital stammt. Damit muss der „Digital Envelope“ also Vertraulichkeit, Authentizität und Integrität gewährleisten.

Die prinzipielle Idee des Verfahrens modelliert den Versand eines Fotoabzugs im Brief mit der Post. Hierzu muss das Bild unter Umständen erst passend geschnitten werden. Dann werden auf die Rückseite des Fotos zum Beispiel die Namen der aufgenommenen Personen und das Aufnahmedatum geschrieben. Der Absender unterschreibt, das heißt signiert diese Angaben, und dann wird das Foto in einen Briefumschlag gesteckt, und dieser wird versiegelt. Damit ergeben sich die Verfahrensschritte: Vorverarbeitung, Signatur, Zusammenstellung des Digital Envelopes und Versiegelung.

Vertraulichkeit, Authentizität und Integrität werden hierbei mittels einer digitalen Signatur erreicht, die auch aus anderen Bereichen der elektronischen Kommunikation bekannt und in Deutschland bereits gesetzlich geregelt ist (11). Hierzu wird eine Art Prüfsumme aus der zu signierenden Information mit einem bestimmten allgemein bekannten Algorithmus errechnet. Während im normalen E-Mail-Verkehr die Information aus den Buchstaben der Wörter besteht, sind es im Bereich der medizinischen Bildverarbeitung die Pixel des Bildes. Die Prüfsumme, auch Hash oder Digest genannt, ist zwar kleiner als das Bild, ändert sich jedoch mit jeder kleinsten Pixeländerung im Bild. Zusätzlich zum Bild wird dann auch der Digest übertragen. Beim Empfänger kann dieser erneut berechnet werden. Gleichen sich beide, ist die Integrität des Bildes gewährleistet. Damit niemand das Bild und den Digest modifizieren kann, wird der Digest nach einem Public-Key-Verfahren verschlüsselt.

Verfahrensschritte des „Digital Envelopes“ *(Abbildung 3)*

1. Vorverarbeitung: Zunächst wird das Bild vorverarbeitet. Es wird automatisiert bestimmt, in welchen Bildbereichen tatsächliche Bildinformation steckt und in welchen Bereichen eine Shutter-Abschattung oder Hintergrund dargestellt ist. Hierfür gibt es zuverlässige Algorithmen (9). Das Ergebnis dieser Vorverarbeitung ist dann eine so genannte Bounding Box, die das eigentliche Bild von einem Hintergrundbereich trennt.

2. Digest und Signatur: Von dem Bildbereich wird dann ein Digest berechnet. Dabei gewährleistet der Extraktionsalgorithmus, dass sich der Digest ändert, wenn auch nur ein Pixel im Bildbereich modifiziert wurde. Dieser Digest wird dann mit

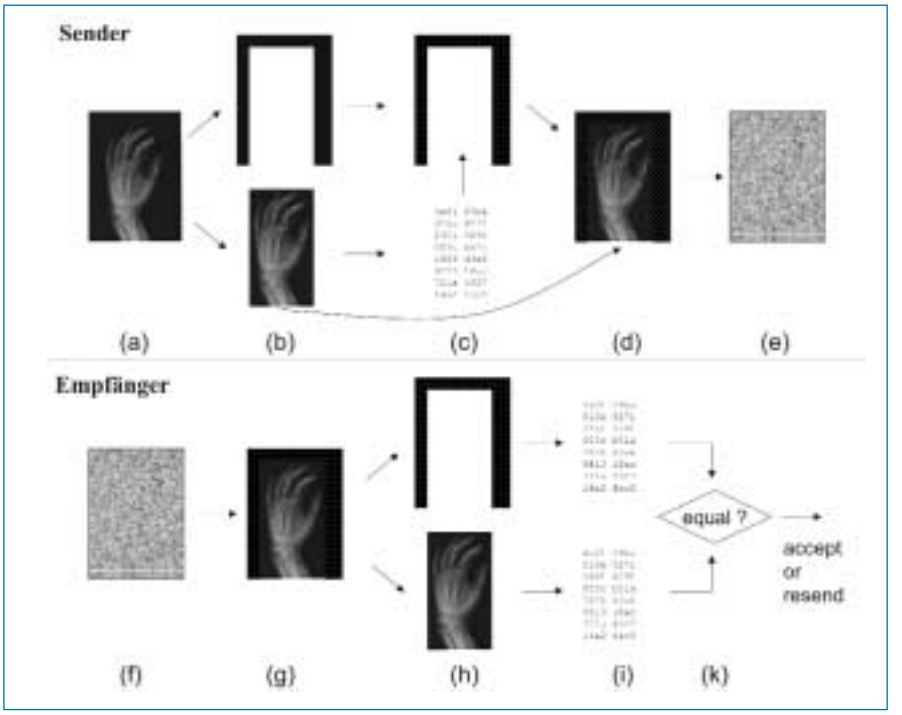

Abbildung 3: Prinzip des Watermarking in medizinischen Bildern. Auf der Senderseite wird im Originalbild (a) zunächst der Bildbereich vom Hintergrundbereich getrennt (b). Aus dem Bildbereich wird ein Digest berechnet und in den Hintergrund eingebettet (c). Dann wird das Bild wieder zusammengesetzt (d) und für die Übertragung im Internet gegebenenfalls komprimiert oder verschlüsselt (e). Auf der Empfängerseite (f) wird das Bild zunächst dekomprimiert (g) und dann mit demselben Algorithmus in Objekt- und Hintergrundbereich zerlegt (h). Die Signatur lässt sich aus dem Bild erneut berechnen und auch aus dem Hintergrund extrahieren (i). Sind beide gleich, wird das Bild akzeptiert, ansonsten wird die Übertragung erneut initiiert (k).

dem privaten Schlüssel des Senders verschlüsselt. Jeder, der Zugriff auf die Komponenten Bild, verschlüsselter Digest und Public Key des Senders hat, kann jetzt die Authentizität und Integrität des Bildes prüfen. Hierzu muss er lediglich mit dem genannten Verfahren den Bildbereich ermitteln, den Digest berechnen, den verschlüsselten Digest dekodieren und beide vergleichen.

3. Digital Envelope und Versiegelung: Im nächsten Schritt wird der verschlüsselte Digest mit den vertraulichen personenbezogenen Daten verbunden und mit dem Public Key des Empfängers verschlüsselt. Werden bei dem asymmetrischen Signaturprinzip Daten mit einem privaten Schlüssel kodiert, wird zur Dekodierung der zugehörige öffentliche Schlüssel benötigt. Genauso kann man die Daten mit einem öffentlichen Schlüssel kodieren – dann ist zur Entschlüsselung der zugehörige private Schlüssel erforderlich. Da mit dem „Digital Envelope" der öffentliche Schlüssel des Empfängers verwendet wird, kann die Nachricht nur vom Empfänger selbst geöffnet werden.

4. Dateneinbettung: Zuletzt wird die Information zum Beispiel mit dem Least-Significant-Bit-Verfahren in den Hintergrundbereich des Bildes integriert. Durch die Trennung zwischen Bild- und Hintergrundbereich wird gewährleistet, dass die medizinisch relevante Information durch das Wasserzeichen selbst nicht verändert wird. Das Bild mit Wasserzeichen kann nun verlustfrei komprimiert oder mit weiteren Verschlüsselungsverfahren kombiniert werden.

5. Dekodierung: Beim Empfänger wird zunächst die Bilddatei dekomprimiert. Dann wird der Hintergrundbereich bestimmt und hieraus das Wasserzeichen extrahiert. Nur der richtige Empfänger kann das Wasserzeichen interpretieren und somit die patientenbezogenen Daten dechiffrieren. Damit ist die Vertraulichkeit gewährleistet. Dann wird die übertragene Prüfsumme mit der des empfangenen Bildes verglichen, was sowohl die Integrität des Bildes als auch die Authentizität des Senders beweist.

Ein Nachteil des beschriebenen Verfahrens ist, dass ein Broadcasting medizinischer Bilder nicht möglich ist. Der „Digital Envelope“ muss für jeden Empfänger neu berechnet werden. Damit hat jeder Empfänger ein eigenes Wasserzeichen, und er muss für jedes Bild die unter Umständen aufwendigen Berechnungen durchführen, die zur Ausbettung und Dekodierung der Information notwendig sind. Um diesen Ansatz zu erweitern, wird daher zurzeit am Children's Hospital eine zentrale Zertifizierungsstelle für medizinische Bilder eingerichtet. Die Wasserzeichen der zu versendenden Bilder werden nicht mehr mit dem öffentlichen Schlüssel des Empfängers, sondern immer mit dem öffentlichen Schlüssel der Verifizierungsstelle verschlossen. Jeder Empfänger kann dann bei Bedarf bei der Zertifizierungsstelle die Authentizität und Integrität der Daten bestätigen lassen. Damit entfallen auch teilweise die aufwendigen Berechnungen auf der Empfängerseite (2).

Fazit

In der Informatik und im Internet sind die Techniken des digitalen Wasserzeichens bereits stark verbreitet, wohingegen die Anwendungen im medizinischen Bereich zurzeit noch spärlich sind. Nicht zuletzt im Hinblick auf die elektronische Patientenakte und den damit verbundenen Transfer sensitiver Patienten-/Bilddatenkombinationen werden diese Techniken jedoch auch hier in naher Zukunft verstärkt eingesetzt werden.

Literatur

1. Blobel B, Pharow P: Datensicherheit in medizinischen Informationssystemen und Gesundheitsnetzen. In: Lehmann TM (Hrsg.): Handbuch der Medizinischen Informatik. Carl Hanser Verlag, München, 2. Aufl. 2005, 713–732.
2. Cao F, Huang HK, Zhou XQ: Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics 2003; 27: 185–96.
3. Deguillaume F, Voloshynovskiy S; Pun T: Secure hybrid robust watermarking resistant against tampering and copy attack. Signal Processing 2003; 83(10): 2133–70.
4. DICOM PS 3.1-2004: Digital imaging and communications in medicine. National Electrical Manufacturers Association (NEMA), Rosslyn, VA, 2004.
5. Dittmann J: Digitale Wasserzeichen. Springer-Verlag Berlin, 2000.
6. ISO 7498-2: Information processing systems/open systems interconnection/basic reference model. Part 2: security architecture. International Organization for Standardization (ISO), Genf, 1989.
7. Katzenbeisser S, Petitcolas FAP (eds): Information hiding techniques for steganography and digital watermarking. Artech House, Boston, MA, 2000.
8. Kerckhoffs A: La Cryptographie Militaire. Journal des Sciences Militaires 1883; 9: 5–38.
9. Lehmann TM, Goudarzi S, Linnenbrügger N, Keysers D, Wein B: Automatic localization and delineation of collimation fields in digital and film-based radiographs. Proceedings SPIE 2002; 4684(2): 1215–23.
10. Rajendra AU, Subbanna BP; Sathish K, Min LC: Transmission and storage of medical images with patient information. Computers in Biology and Medicine 2003; 33(4): 303–10.
11. SigG – Signaturgesetz. Gesetz zur digitalen Signatur in der Fassung des Beschlusses des Deutschen Bundestages vom 13. Juni 1997 (BT-Drs. 13/7934).
12. Tzelepi S, Pangalos G, Nikolacopoulou G: Security of medical multimedia. Medical Informatics and the Internet in Medicine 2002; 27(3): 169–84.
13. Xuan K, Rui F: Watermarking medical signals for telemedicine. IEEE Transactions on Information Technology in Biomedicine 2001; 5(3): 195–201.

Anschrift des Verfassers:
Priv.-Doz. Dr. rer. nat. Dipl.-Ing. Thomas M. Lehmann
Institut für Medizinische Informatik
(Direktor: Univ.-Prof. Dr. med. Dr. rer. nat. Dipl.-Math. Klaus Spitzer)
Universitätsklinikum der RWTH Aachen
Pauwelsstraße 30
52057 Aachen
Telefon: 02 41/8 08 87 93
Fax: 02 41/8 03 38 87 93
E-Mail: lehmann@computer.org