Steganographisches Illustrieren: Neue Perspektiven für Try&Buy

Jana Dittmann[1], Knut Hartmann[2], Henry Sonnet[2]
Felix Ritter[2], Thomas Strothotte[2]

[1]AG Multimedia und Security
Institut für Technische und Betriebliche Informationssysteme

[2]AG Computergraphik und Interaktive Systeme
Institut für Simulation und Graphik

Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2, 39106 Magdeburg

1 Motivation

Die jüngsten Entwicklungen der Computergraphik zeigen, welche effektiven und zugleich intuitiven Möglichkeiten computergenerierte Illustrationen in der Mensch-Computer-Interaktion bieten. Deren Forschungsprototypen basieren auf Modellen, die sowohl geometrische als auch nichtgeometrische Aspekte umfassen. Das vorliegende Papier entwickelt Perspektiven der *steganographischen Illustration*, deren Ausgangspunkt multidimensionale Bildrepräsentationen sind. Hierbei wird das Format zur Repräsentation von Bildern selbst so erweitert, dass zusätzlich zu den Farbwerten der einzelnen Bildpunkte weitere Informationen gespeichert werden. Gegenüber der Einbettung graphischer Informationen in Meta-Formate (XML) oder von Meta-Informationen in Graphikformate (JPEG 2000, MPEG-7) bieten steganographische Verfahren zwei wesentliche Vorteile:

Verschmelzung: Die Information ist untrennbar mit dem Bild selbst verbunden. Damit lassen sich auch herkömmliche Werkzeuge zum Betrachten und Bearbeiten von Bildern uneingeschränkt verwenden.

Lokalität der Codierung: Die zu versteckende Information kann entweder im gesamten Bild oder aber in einzelnen Bildbereichen codiert werden. Eine objektlokale Codierung ermöglicht es, auch nach tiefgreifenden Veränderungen des Bildes, wie beispielsweise dem Ausschneiden des Objektes und dessen Kopieren in ein anderes Bild, auf die den einzelnen Objekten zugeordnete Information zuzugreifen (**Robustheit**).

Die steganographische Encodierung von Zusatzinformationen in das digitale Bildmaterial wirft folgende Fragestellungen auf:

1. Welche **Kapazität** weisen die einzelnen steganographischen Verfahren auf?
2. Welche visuell wahrnehmbaren **Artefakte** bringen diese in das Bildmaterial ein?

Die sicherlich sehr begrenzte Kapazität vom Betrachter nicht wahrnehmbarer objektlokaler Encodierung stellt eine besondere Herausforderung dar, die entweder durch

- eine möglichst effiziente Repräsentation der Zusatzinformation oder aber
- die Ausnutzung der inhärenten Strukturen des Bildes realisiert werden kann.

Der vorliegende Beitrag weist durch steganographisch in Bildern versteckte Zusatzinformationen neue Perspektiven für Try&Buy-Geschäftsmodelle auf. In [DSA00] und [KSD02] wurden fundamentale steganographische Verfahren entwickelt, die neuartige Werbestrategien und Geschäftsmodelle auf Basis digitaler Wasserzeichen ermöglichen. In dieser Arbeit werden steganographische Verfahren zur Entwicklung neuartiger Interaktionsformen mit digitalem Bildmaterial genutzt. Hier eröffnen sich vielfältige Möglichkeiten für Try&Buy-Angebote, wenn sich dieser zusätzliche Nutzen erst nach einer kostenpflichtigen Freischaltung erschließt.

Das Papier ist wie folgt gegliedert: Der Abschnitt 2 stellt im Rahmen einer kurzen Bestandsaufnahme klassische steganographische Verfahren für digitales Bildmaterial vor und zeigt deren Möglichkeiten und Begrenzungen auf. Da in den skizzierten Try&Buy-Ansätzen die Robustheit der encodierten Zusatzinformationen gegenüber Benutzermanipulationen von immenser Bedeutung ist, werden außerdem robuste Annotationswasserzeichen diskutiert. Der Abschnitt 3 zeigt grundlegende Konzepte und Perspektiven des steganographischen Illustrierens auf und stellt den Architekturentwurf eines Systems zum steganographischen Illustrieren vor. Im Abschnitt 4 werden einige vielversprechende Anwendungsfälle für Try&Buy-Mechanismen diskutiert. Im abschließenden Abschnitt 5 werden die erreichten Ergebnisse zusammenfasst.

2 Klassische Steganographie — Bestandsaufnahme

Die Einbettung von Zusatzinformationen in digitales Bildmaterial erfordert steganographische Verfahren, die sowohl eine objektlokale Codierung als auch eine direkte und vom Bildrepräsentationsformat unabhängige Encodierung erlauben. Allerdings erheben klassische steganographische Verfahren zur vertraulichen Kommunikation häufig nicht den Anspruch auf Formatunabhängigkeit. Aus diesem Grund werden in diesem Abschnitt die grundlegenden Konzepte steganographischer Verfahren sowie deren Weiterführung zu digitalen Wasserzeichen diskutiert.

Die *Steganographie*[1] nutzt zur geheimen Kommunikation die Präsenz der Kommunikation. Die Nachricht selbst wird hier zum Träger versteckter Informationen. Historisch gesehen zählen zu den ersten steganographischen Techniken das unsichtbare Schreiben mit spezieller Tinte oder Chemikalien. Es folgten Ansätze, Nachrichten in langen Texten zu verstecken. Bestimmte Buchstaben lassen sich hier zu neuen Wörtern zusammensetzen und formen so eine geheime Nachricht. Heute liegt es nahe, die Irrelevanz bzw. Redundanz binärer Dateien auszunutzen, um Daten zu verstecken. Dabei ist digitales Bild- und Tonmaterial als Träger der geheimen Nachricht ideal geeignet.

Jede steganographische Technik umfasst den *Einbettungsalgorithmus*, der in das Träger-

[1] auch als data hiding oder secure cover communication bezeichnet

material (*Cover*) geheime Daten einbettet und so ein *StegoCover* erzeugt, und den *Abfragealgorithmus*, der aus dem StegoCover die geheime Nachricht extrahiert. Die Sicherheit älterer Verfahren basiert auf der Geheimhaltung der Verfahren selbst. Da steganographische Verfahren jedoch bereits nach kurzer Zeit aufgedeckt werden, verwenden heutige Verfahren als zusätzlicher Sicherheitsparameter geheimer Schlüssel. Wichtige Eigenschaften steganographischer Techniken zur verdeckten Kommunikation sind:

Detektierbarkeit: Die einzubringende Nachricht darf im Trägerdokument nicht aufgespürt, *detektiert*, werden. Im engeren Sinn darf ein Angreifer, bei gleichzeitiger Vorlage des Covers *und* des StegoCovers, diese nicht eindeutig als solche identifizieren können.

Transparenz: Diese Eigenschaft beschreibt, in welchem Grade die Einbettung geheimer Zusatzinformationen akustisch oder optisch wahrnehmbare Veränderungen verursacht.

Kapazität: Diese Eigenschaft beschreibt, wieviel Zusatzinformation in das Trägermaterial eingebracht werden kann.

Klassische steganographische Verfahren sind hinsichtlich einer geringen Detektierbarkeit bei einer hohen Transparenz und Kapazität optimiert und gewährleisten so die Vertraulichkeit der Kommunikation. Sie eignen sich daher hervorragend zur Einbettung großer Informationsmengen in speicherintensive Bildformate, ohne die Qualität des Trägermaterials negativ zu beeinflussen. Einen Überblick über die Vielfalt steganographischer Techniken für Bild- und Tonmaterial findet sich in [JDJ00] und [KP00].

Robustheit

Ein Einbettungsalgorithmus ist *robust*, wenn der Abfragealgorithmus die eingebrachte Information zuverlässig aus dem StegoCover extrahieren kann, auch wenn dieses modifiziert, wohl aber nicht vollständig zerstört wurde. *Robustheit* bezeichnet somit die Widerstandsfähigkeit der in ein Trägermaterial eingebrachten Daten gegenüber Veränderungen durch Weiterverarbeitung. Im anvisierten Try&Buy-Anwendungsszenarium wird eine robuste, da formatunabhängige Encodierung angestrebt, da erst dies dem Anwender einen nachhaltigen Nutzen garantiert. Ein potentieller Verlust der eingebetteten Informationen allein durch zufällige Konvertierungen würde kaum akzeptiert, die Motivation zum Kauf also gering ausfallen. Darüber hinaus bilden objektlokale Codierungen, die hinsichtlich Skalierung des Bildes oder Ausschnittbildung robust sind, zusätzliche Kaufanreize.

Klassische steganographische Verfahren weisen zwar eine hohe Transparenz und Kapazität auf, sind aber selten robust. Digitale Wasserzeichenverfahren, und hier insbesondere Annotationswasserzeichen, basieren auf steganographischen Techniken, sind aber gerade hinsichtlich hoher Kapazität und Robustheit optimiert. In der Literatur sind sehr unterschiedliche Ansätze digitaler Wasserzeichen zu finden. Für die Vielzahl existierender Wasserzeichenverfahren können folgende Anwendungsgebiete identifiziert werden:

Authentifizierung des Urhebers: Robust Authentication Watermark,

Authentifizierung des Kunden: Fingerprint Watermark,

Durchsetzung des Kopierschutzes oder der Übertragungskontrolle: Copy Control Watermark, Broadcast Watermark,

Nachweis der Unversehrtheit: Integrity Watermark oder Verification Watermark,

Annotation des Datenmaterials: Caption Watermark, Annotation Watermark.

Jede Wasserzeichentechnik ist auf eines der genannten Anwendungsgebiete optimiert, die unterschiedliche Ansprüche hinsichtlich der geforderten Robustheit, Kapazität sowie Transparenz spezifizieren. Weitere wichtige Eigenschaften wie Komplexität und Sicherheit werden in [Dit00] diskutiert. Für Try&Buy-Anwendungen erscheinen digitale Annotationswasserzeichen besonders interessant. Mit diesen Markierungen werden Beschreibungen zum Datenmaterial, wie Szenen- und Verwendungsbeschreibungen, aber auch Lizenzhinweise in das Datenmaterial eingebracht. Annotationswasserzeichen bieten eine grundlegende Robustheit und sind auf eine hohe Kapazität optimiert. Anwendungsbeispiele für Bildmaterial finden sich in [Ala00a] und [Ala00b]. Die existierenden Annotationswasserzeichen sind jeweils auf bestimmte Anwendungen optimiert und garantieren deren Ansprüche an Robustheit und Kapazität. Bei wechselnden Anforderungen müssen diese aber angepasst werden. Es zeigte sich auch, dass die Kapazität und Robustheit bezüglich Lokalität bisher nur ungenügend Berücksichtigung finden. Formatkonvertierungen hingegen stellen keine Probleme dar.

3 Perspektiven Steganographischen Illustrierens

Dieser Abschnitt stellt das Konzept des steganographischen Illustrierens, die im skizzierten Anwendungsszenarium vielversprechende steganographische Verfahren und ihre Umsetzung in einer Systemarchitektur vor, wobei stets die im Projekt zu lösenden offenen Fragestellungen herausgearbeitet werden.

3.1 Generelles Konzept

In dieser Arbeit wird davon ausgegangen, dass die von steganographischen Browsern darzustellenden Illustrationen interaktiv durch Methoden der Computergraphik erzeugt werden und sich somit zumindest ein Teil der Funktionalität interaktiver Computergraphiken durch Erweiterung statischer Illustrationen realisiert lässt. Es werden zuerst die Forschungsergebnisse der Computergraphik vorgestellt, die den Ansatz des steganographischen Illustrierens motivierten. Anschließend wird dargestellt, welche Funktionalitäten steganographische Try&Buy-Browser aufweisen könnten.

In jüngster Zeit wurden in der Computergraphik eine ganze Reihe von Techniken entwickelt, die eine effektive Exploration umfangreicher Informationsräume durch Anwendung graphischer Abstraktionstechniken [S+98] und nichtphotorealistischer Illustrationstechniken [SS02] ermöglichen. Diese Arbeiten zielen auf die enge Integration sprachlicher und visueller Informationen und die Koordination der Inhalte beider Medien. So integrierte Preim im System ZoomIllustrator [PRS97] sprachliche Annotationen variabler Länge in interaktive graphische Lernumgebungen. Schlechtweg [SS99] entwickelte mit dem System TextIllustrator das Konzept des illustrativen Navigierens (*illustrative browsing*) in umfangreichen Texten, welches durch Hervorhebung der im Text benannten

Objekte den schnellen Zugriff auf interessante Passagen in umfangreichen Dokumenten ermöglicht. Diese Methode setzt voraus, dass sich die Referenzidentität graphischer und sprachlicher Einheiten automatisch bestimmen lässt. Hartmann [HSHS02] wendete daher Methoden der automatischen Textanalyse zur Extraktion solcher koreferentiellen Beziehungen mit dem Ziel der automatischen Illustration von Fachtexten an. Im von ihm entwickelten System AGILE werden außerdem die Assoziationen zwischen den extrahierten Begriffen berücksichtigt.

Die vorgestellten Systeme benötigen über rein geometrische Repräsentationen hinaus weitere Informationen, wie beispielsweise Angaben zur Klassifikation geometrischer Objekte, deren semantische Relationen oder deren sprachliche Realisierungsmöglichkeiten. Diese Informationen sind entweder Bestandteil der geometrischen Repräsentation (strukturierte geometrische Modelle) oder können über Verknüpfungen mit formalen Wissensrepräsentationen und mehrsprachigen phrasalen Lexika dynamisch bestimmt werden. Des Weiteren werden sowohl Benutzerinteraktionen als auch formale Beschreibungen von Systemreaktionen in Benutzermodellen repräsentiert. Nichtphotorealistische Hervorhebungstechniken können so Visualisierungen erzeugen, die den aktuellen Interaktionszustand berücksichtigen.

Während in allen bisherigen Verfahren die Adaption der Visualisierung an externe Anforderungen durch eine geeignete Wahl der Parameter des Renderingprozesses umgesetzt wurden und somit bei sich ändernden externen Anforderungen stets neue Projektionen zu generieren sind, zielt der vom steganographischen Illustrieren verfolgte Ansatz auf die Einbettung zusätzlicher Information in *eine* Projektion.

Im Folgenden werden eine Reihe möglicher Anwendungen hinsichtlich ihrer Anforderungen zur Repräsentation zusätzlicher Informationen untersucht:

1. Erweiterung um sprachliche Annotationen zu graphischen Objekten,
2. das illustrative Navigieren,
3. die semantische Auszeichnung graphischer Objekte,
4. die Darstellung verdeckter Objekte und
5. die dreidimensionale Darstellung ausgewählter Objekte.

1. Im vorliegenden Ansatz werden **Annotationen**, wie sie in wissenschaftlich-technischen Illustrationen eingesetzt werden, nicht als integraler Bestandteil eines statischen Bildes, sondern als ein zusätzliches Mittel des Informationszugriffs aufgefasst. Der Designer Tufte [Tuf97] bemisst bei einer Analyse visueller Erklärungen die Qualität informativer Bilder an einer geringst möglichen Überlappung der visuellen Mittel zur Umsetzung illustrativer Techniken und denen zur Objektdarstellung (*smallest effective difference*). Im aktuellen Kontext nicht benötigte Annotationen verdecken möglicherweise wichtige Objekte und schränken den Platz zur Darstellung anderer Annotationen ein. Weiterhin nutzen Ankerlinien, die Text und sprachliche Annotation verbinden sowie die Silhouettenlinien graphischer Objekte den gleichen visuellen Code. Eine sorgsame Adaption der Anzahl und des Inhaltes der Annotationen, die das darzustellende Objekt begleiten, ist daher ein nicht zu unterschätzender Mehrwert.

Die Darstellung einer variablen Anzahl von Annotationen durch den steganographischen Browser benötigt folgende zusätzlichen Informationen:

- die Kennzeichnung des Bildes mit einer eindeutigen Referenz, was eine Integration extern gespeicherter Informationen ermöglicht,
- die Kennzeichnung graphischer Elemente mit einer eindeutigen Referenz,
- die Angabe alternativer sprachlicher Realisierungen und
- Positionsangaben zur Darstellung.

Die hier angegebenen Zusatzinformationen sind auch von zentraler Bedeutung für die weiteren Anwendungsfälle und werden daher dort nicht gesondert aufgeführt.

2. Zur Anwendung des Konzeptes des **illustrativen Navigierens** in einem steganographischen Browser werden die im aktuell sichtbaren Text benannten Objekte auch in der Illustration hervorgehoben. Dazu ist die eindeutige Diskrimierbarkeit der einzelnen graphischen Objekte, aber auch die Differenzierung zwischen relevanten und irrelevanten graphischen Objekten notwendig. Der steganographische Browser stellt relevante Objekte normal dar, während alle anderen Objekte in einer einheitlichen Farbe dargestellt werden, die sich vom Hintergrund unterscheidet.

3. Der Zugriff auf externe formale Wissensrepräsentationen ermöglicht die **semantische Auszeichnung** graphischer Objekte. Anhand der eindeutigen Referenz des Bildes und der ausgewählten graphischen Objekte können anwendungsspezifische Zusatzinformationen, z.B. als kontextsensitive Menüstrukturen angeboten werden.

4. Verdeckungen: Die zu visualisierenden Objekte in wissenschaftlich-technischen Illustrationen weisen häufig eine komplexe räumliche Struktur auf. Da aus jeder möglichen Sichtrichtung stets eine große Anzahl von Objekten verdeckt werden, reicht eine Visualisierung allein zumeist nicht aus. Wissenschaftlich-technische Illustratoren nutzen eine Reihe von Illustrationstechniken (Insets, Cutaways, transparente Darstellung, Weglassen oberflächlicher Schichten), um unerwünschte Verdeckungen zu vermeiden. Können Farbwerte verdeckter Strukturen versteckt gespeichert werden, ermöglicht dies die dynamische Erstellung semitransparenter Darstellungen. Hierzu werden die Farbwerte überlagernder transparenter Objekte mit denen opaker Hintergrundobjekte gemischt.

5. Gu u.a. [GGH02] zeigen Möglichkeiten auf, geometrische Modelle bildhaft zu codieren. Diese Repräsentationen können verlustbehaftet komprimiert werden und ermöglichen somit eine skalierbare Approximation dreidimensionaler geometrischer Modelle. Ein steganographischer Browser kann dies zur **dreidimensionalen Darstellung** ausgewählter Objekte vor einem festen Hintergrund nutzen.

Weitere interessante Anwendungen des Try&Buy-Konzeptes für steganographische Bildbrowser sind die bildhafte Codierung von Lösungen in Online-Lehrmaterialien und die stufenweise Bereitstellung von Bildern unterschiedlicher Qualität.

Zusammenfassung: Die hier vorgeschlagenen Anwendungsfälle eines steganographischen Bildbrowsers nutzen **globale Informationen** zur Codierung des aktuellen Anwendungskontextes (z.B. einen eindeutigen Bezeichner des Bildes), die einen Zugriff auf

externe Ressourcen ermöglichen und sicher encodiert werden müssen. Darüber hinaus werden eine Vielzahl **objektlokaler Informationen** benötigt (z.B. zur Kennzeichnung der Bildelemente mit einer eindeutigen Referenz, für dreidimensionale geometrische Repräsentationen, zur Repräsentation der Farbwerte verdeckter Objekte). Zur Codierung ist stets zwischen der benötigten Kapazität und der angestrebten Transparenz stenographischer Verfahren abzuwägen.

3.2 Kapazität und Transparenz objektlokaler steganographischer Verfahren

Die 5 Interaktionsformen des vorigen Abschnitts beanspruchen höchst unterschiedliche Kapazitäten zur Codierung der benötigten Zusatzinformationen. Sie reichen von kurzen sprachlichen Annotationen, die mit wenigen Bits auskommen, bis hin zur Repräsentation ausgewählter dreidimensionaler geometrischer Modelle, die mehrere kByte beanspruchen. Für deren Codierung sollen steganographische Verfahren bzw. digitale Annotationswasserzeichen benutzt werden. Wie bereits in Abschnitt 2 deutlich gemacht, stellen die Parameter Kapazität und Transparenz eine wesentliche Herausforderung für steganographische Methoden und Annotationswasserzeichen dar.

Darüber hinaus betten sowohl steganographische Verfahren als auch Annotationswasserzeichen die Information entweder linear zu einem festen Startpunkt ein oder verstreuen diese über den gesamten Bildraum. Erweitert man die steganographischen Techniken und Annotationswasserzeichen auf objektlokale Codierungen, müssen zudem Synchronisierungsinformationen in die Codierung aufgenommen werden. Darüber hinaus ist die Kapazität nicht mehr nur vom Speicherbedarf des Gesamtbildes, sondern auch von der Größe der einzelnen geometrischen Objekte abhängig. Beide Faktoren reduzieren die bisher erreichbaren Kapazität, was neue Kapazitätsabschätzungen notwendig macht. In weiteren Arbeiten sind bekannte Techniken, wie sie beispielsweise in [Dit00] oder [Ala00a] beschrieben werden, diesbezüglich zu untersuchen. Neben einer direkten Einbettung der zusätzlichen Informationen sollen des Weiteren auch indirekte Verfahren wie die Codierung von Links betrachtet werden.

Ebenso ungelöste Probleme wirft die Transparenz objektlokaler Codierungen auf. Einfarbige Objekte erlauben nur sehr geringe Kapazitäten, da sonst die Transparenz der Codierung bzw. bei steganographischen Methoden auch deren Detektierbarkeit nicht gewährleistet werden kann. Daher müssen Verfahren entwickelt werden, die Abstriche hinsichtlich Transparenz oder Detektierbarkeit in Kauf nehmen oder dynamisch zwischen verschiedenen Einbettungstechniken auswählen.

3.3 Robustheit und Security

Das skizzierte Try&Buy-Szenarium erfordert neben einer hohen Transparenz und Kapazität auch die Robustheit hinsichtlich Formatkonvertierungen, Ausschnittbildungen und Skalierungen. Die Einbettung dreidimensionaler Objekte legt es nahe, auch Robustheit gegenüber Rotationen einzubeziehen, da Objekte ausgeschnitten und in andere Bilder leicht rotiert eingefügt werden könnten.

Die bisher bekannten steganographischen Verfahren sind allerdings nicht robust.[2] Die Diskussion macht deutlich, dass bezüglich der Robustheit weiterer Forschungsbedarf besteht. Hier kann aber auf Erfahrungen aus dem digitalen Wasserzeichenbereich ([Dit00, Ala00a, Ala00b]) zurückgegriffen werden. Diese Arbeiten zeigen, dass Anforderungen an die Robustheit auch die Kapazität und Transparenz beeinflussen. Um zusätzlich auch Sicherheit — in unserem Fall Zugriffsschutz für Try&Buy — zu erreichen, muss die einzubettende Information verschlüsselt werden; ein Vorgehen, was bisher vor allem bei steganographischer Kommunikation genutzt wird.

3.4 Kryptographische Protokolle und Schlüssel

Um für Try&Buy-Mechanismen einen ausreichenden Zugriffsschutz zu realisieren, sind die steganographisch einzubettenden Zusatzinformationen zu verschlüsseln. Die Zusatzinformationen lassen sich somit nur durch den Erwerb zusätzlicher Schlüsselinformationen freischalten. Zur Freischaltung sollen verschiedene Alternativen unterstützen werden:

1. der Kunde erhält erst nach Erwerb der Schlüsselinformation Zugang zu den Annotationen;
2. der Kunde hat auf eine begrenzte Auswahl von Bildobjekten und deren Annotationen freien Zugang. Der Zugriff auf weitere Einzelbildannotationen erfordert den Erwerb von Schlüsseln;
3. der Kunde sieht alle potentiellen Annotationen (z.B. nur in unvollständigen Ansichten oder in begrenzter Auflösung), kann aber auf die Annotationen in voller Qualität nach Erwerb der Schlüsselinformationen zugreifen.

Um den Zugriff bzw. den Zugang zu den Annotationen zu schützen, soll ein symmetrisches Kryptosystem (z.B. AES) benutzt werden. Hier werden die Annotationen für jeden i-ten Kunden mit einem Schlüssel k_i verschlüsselt. Diese lassen sich anschließend ausschließlich durch den i-ten Kunden freischalten. Die Verschlüsselung kann pro Bild für alle m enthaltenen Annotationen einen identischen k_i oder einen separaten Schlüssel k_{ij} nutzen. Um eine Zuordnung und die Freischaltung von Bild, Kunde und Annotation sowie benötigter Schlüssel k_i bzw. k_{ij} zu erreichen, bietet es sich an, eine Datenbank zu führen.

Für verschlüsselte Annotationen sind außerdem Protokolle der Schlüsselverteilung an die Kunden zu entwickeln. Es ist denkbar, den bzw. die Schlüssel k_i bzw. k_{ij} über ein asymmetrisches Kryptosystem [Sch95] zu verteilen: Der Kunde stellt seinen öffentlichen Schlüssel zur Verfügung und erhält anschließend den Freischaltschlüssel k_i bzw. k_{ij} mit seinem öffentlichen Schlüssel verschlüsselt zurück. Erst das Vorliegen des zugehörigen geheimen Schlüssel erlaubt das Entschlüsseln. Solche Verfahren sind auch als Hybride Kryptosysteme bekannt.

Hat der Kunde den Zugangscode entschlüsselt, kann er auf die Annotationen mit dem erhaltenen symmetrischen Schlüssel zugreifen. Um Angreifer zu demotivieren, die Bil-

[2] In der Praxis erweist es sich als sehr schwierig, die in der Literatur vorgestellten Verfahren auf ihre Robustheit zu testen und zu vergleichen, da sie meist nur informal beschrieben sind und nicht als frei verfügbare Testversionen vorliegen. Außerdem besitzen die Verfahren bisher kaum Möglichkeiten, objektlokale Codierungen vorzunehmen.

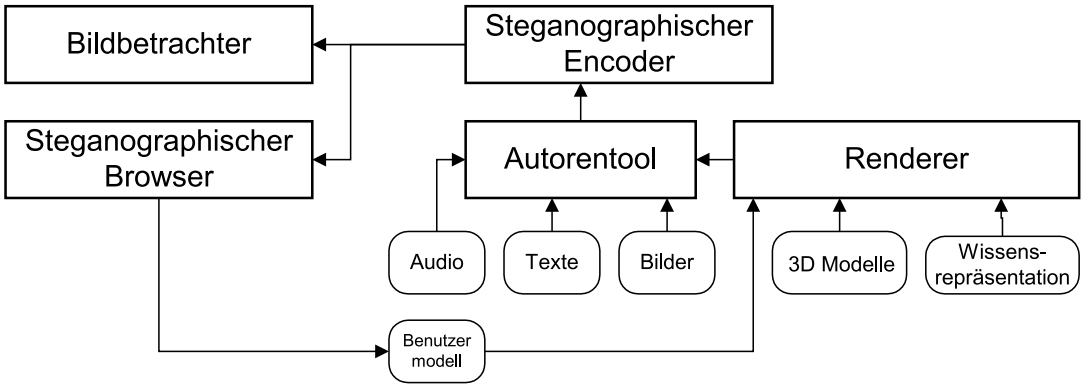

Abbildung 1: Architektur eines steganographischen Try&Buy-Systems, das sowohl ein Autorentool zum steganographischen Anreichern von Illustrationen als auch kostenfreie und kostenpflichtige Zugriffsmechanismen umfasst.

der und die gekauften Annotationen sowie deren Schlüssel weiterzugeben, bieten sich die bekannten robusten digitalen Wasserzeichen zur Kundenidentifzierung an, die in das Datenmaterial beim ersten Laden des Bildes eingebettet werden. Ein direkter Schutz ist damit zwar nicht zu erreichen, es kann aber die Weitergabe verfolgt werden, was sich als stark demotivierend erwies. An dieser Stelle sei aber auf die Probleme von Koalitionsangriffen auf Kundenmarkierungen hingewiesen (siehe [Dit00]).

3.5 Architekturentwurf

Der im vorliegenden Papier skizzierte Ansatz zum steganographischen Illustrieren umfasst sowohl Mechanismen des Encodierens multidimensionaler Informationen in Bildern als auch deren Ausnutzung innerhalb eines steganographischen Browsers mit dem Ziel, potentiellen Kunden umfassendere Interaktionsmöglichkeiten anzubieten. Im Architekturentwurf der Abbildung 1 stellen der steganographischen Encoder (rechts) und der steganographische Browser (links) unabhängige Komponenten dar, die sich durch in einem Benutzermodell gespeicherte Informationen gegenseitig beeinflussen können. Ist eine solche Kommunikation für den Nutzer aus Sicherheits- oder Vertrauensgründen nicht akzeptabel, kann der steganographische Browser nur die innerhalb des Bildes gespeicherten Informationen ausnutzen. Anderenfalls können über im Bild codierte Referenzen weitere Zusatzinformationen abgerufen werden. Hier sind Mechanismen zu entwickeln, die es Nutzern erlauben, vertrauenswürdige Dienste zu spezifizieren, deren Arbeitsweise zu kontrollieren, aber kostenlose Ausnutzung der offerierten Zusatzleistungen durch Angriffe zu verhindern. Darüber hinaus müssen Protokolle und Softwarekomponenten des steganographischen Autorentools, das einen entsprechenden Encoder umfasst und des steganographischen Browsers entwickelt werden.

4 Anwendungsbeispiele steganographischer Browser

Im Folgenden werden fiktive Anwendungsbeispiele für einige der oben skizzierten Szenarien präsentiert. Dazu werden in einer Reihe von Fallstudien die in herkömmlichen

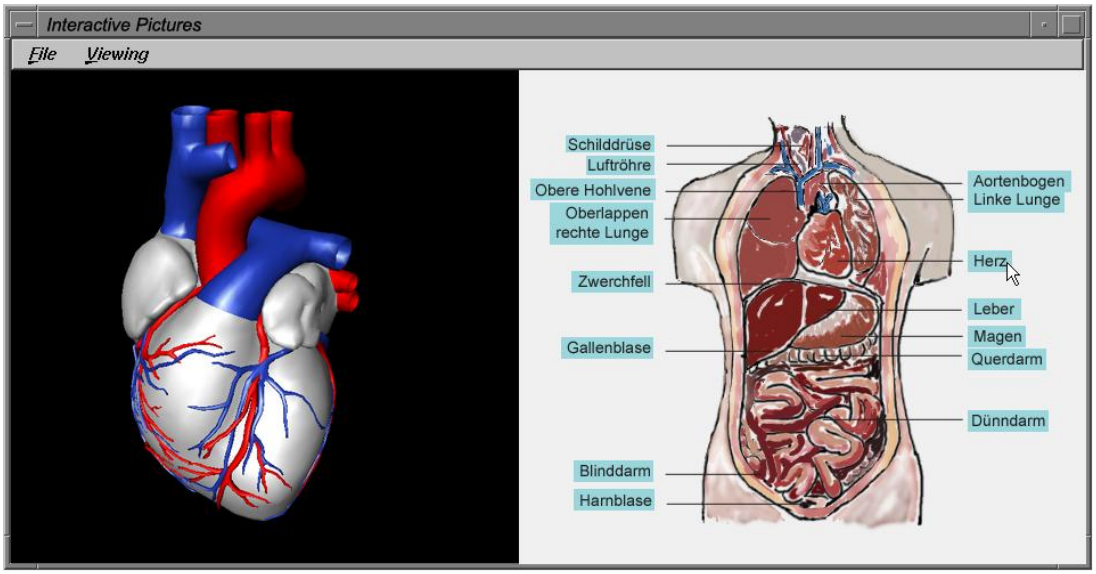

Abbildung 2: Darstellung der inneren Organe, die Illustrationen in anatomischen Lehrbüchern nachempfunden wurde (rechts) und die um interaktiv explorierbare dreidimensionale Modelle erweitert werden können (links).

Lernszenarien verwendete Illustrationen den durch Zusatzinformationen erweiterten steganographischen Illustrationen gegenübergestellt.

4.1 Interaktive Exploration komplexer räumlicher Verhältnisse

Illustrationen, wie sie häufig in Lehrbüchern zu finden sind, bieten dem Betrachter im Vergleich zu Photographien verschiedene Vorteile: sie sind übersichtlich, leicht verständlich und lassen für den aktuellen Kontext Unwesentliches weg. Allerdings bedingt die Darstellung aus nur einer Sichtrichtung, dass auch wichtige Objekte im Bild partiell verdeckt sind und so nur teilweise dargestellt werden können. Interaktiv explorierbare dreidimensionalen Darstellungen bieten Möglichkeiten, die räumliche Konfiguration der dargestellten Objekte und deren tatsächliche Form besser einschätzen zu können. Abbildung 2 zeigt auf der rechten Seite eine schematische Illustration, wie sie in vielen anatomischen Lehrbüchern vorkommt. Sie stellt den menschliche Körper mit Fokus auf die inneren Organe dar und kann als Bilddatei mit herkömmlichen Browsern betrachtet werden. Solche zweidimensionalen Projektionen können aber die zu visualisierenden komplexen räumlichen Konfigurationen nur ungenügend vermitteln. Mit Hilfe des steganographischen Browsers können räumliche Verhältnisse auch interaktiv erkundet werden. Hierzu werden sowohl in der Darstellung des menschlichen Körpers als auch in den dazugehörigen Annotationen Verweise auf dreidimensionale geometrische Modelle versteckt, die bei Aktivierung interaktiv erkundet werden können. Wird wie in Abbildung 2 beispielsweise das Herz in der Illustration selektiert, erscheint daraufhin das auf der linken Seite dargestellte dreidimensionalen Modell des Herzens. Auf diese zusätzlichen Informationen kann der Nutzer allerdings erst zugreifen, wenn das ebenfalls in das Bild codierte Passwort eingegeben wurde.

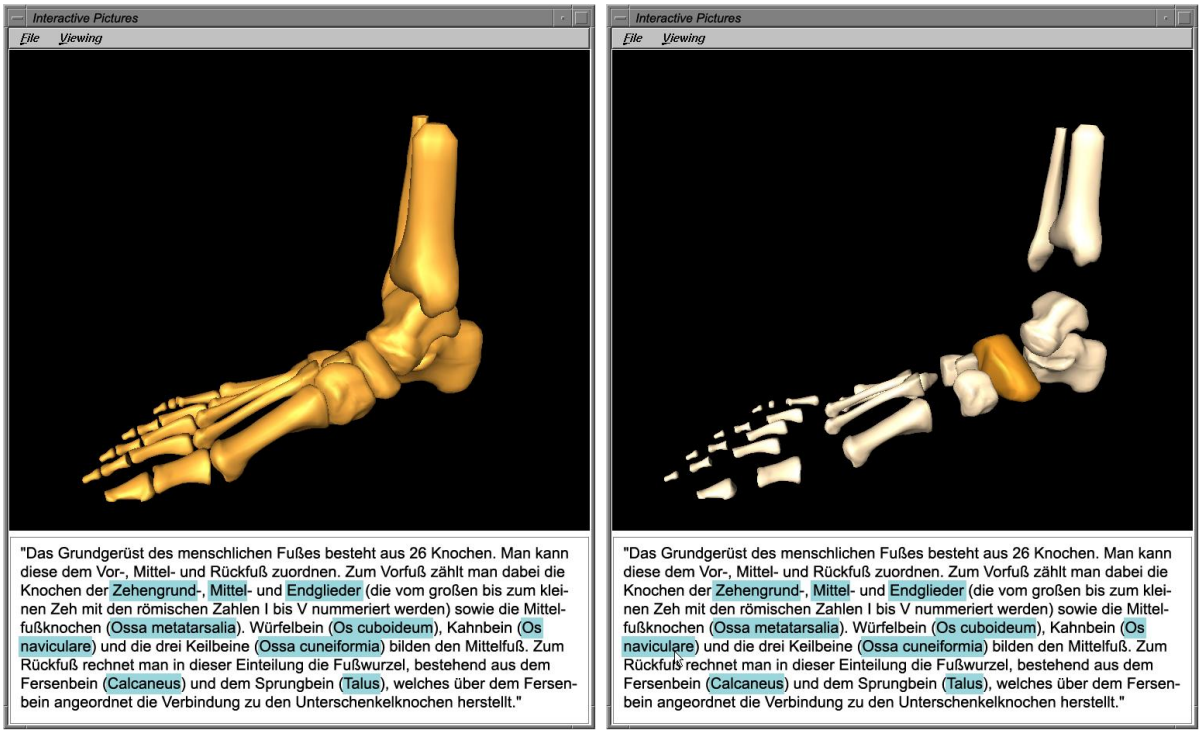

Abbildung 3: Illustratives (links) und steganographisches Navigieren (rechts). Beide Darstellungen sind an das System TextIllustrator [SS99] angelehnt.

4.2 Illustratives Navigieren

Ein weiteres Anwendungsbeispiel demonstriert die Möglichkeiten des illustrativen Navigierens in einem steganographischen Browser. Nachdem der Nutzer ein hervorgehobenes Textfragment selektiert, wird das entsprechende graphische Objekt des Modells hervorgehoben, indem die Farbe aller anderen Objekte verblasst und sie zugleich auch verkleinert werden. Außerdem können Explosionsdarstellungen abgerufen werden, die nicht-fokussierte Objekte verkleinern, so dass Objekte, die sich im Inneren des Modells befinden oder sich auf der aus Sicht des Betrachters abgewandten Seite befinden, besser zu erkennen sind. Sobald die sensitiven Textbereiche verlassen werden, kehrt die steganographische Illustration wieder in den Ausgangszustand zurück, der alle Objekte in ihrer tatsächlichen Größe, Farbe und Position darstellt.

In vielen Fällen ist es wünschenswert, weitere Darstellungsparameter zu beeinflussen. Ein steganographischer Browser kann es nach einer entsprechenden Freischaltung ermöglichen, verdeckte Objekte sichtbar zu machen oder die Farbgebung graphischer Objektes zu verändern. Solche Adaptionen erfordern in herkömmlichen Bildbearbeitungsprogrammen einen großen Aufwand und fundierte Kenntnisse, da Beleuchtungsverhältnisse zu berücksichtigen sind. In einer allein durch die Farbwerte ihrer Bildpunkte definierten Illustration können außerdem weder Verdeckungen aufgehoben noch kann die Sichtrichtung modifiziert werden. Liegen den einzelnen Bildobjekten jedoch geometrische Modelle zugrunde, ist nicht nur die Veränderung deren Farbgebung problemlos möglich — durch Adaption der Sichtrichtung oder der Reihenfolge der Objekte beim Berechnen der Projektion können verdeckte Objekte im Vordergrund sichtbar werden. Die Bereiche zur Darstel-

Abbildung 4: Ein steganographisches Bildwörterbuch, indem die selektierten Objekte durch fremdsprachige Termini überlagert werden.

lung der einzelnen Bildobjekte encodieren zusätzlich Referenzen auf die entsprechenden geometrischen Modelle. Aufgrund dieser objektlokalen Encodierung besteht weiterhin die Möglichkeit, Bildobjekte auszuschneiden und sie anschließend in ein anderes Bild einzufügen ohne das dabei die referentielle Beziehung zwischen Bildobjekt und geometrischem Modell aufgehoben wird.

4.3 Steganographische Bildwörterbücher

In Lernszenarien sind häufig visuell wahrnehmbare Objekte mit ihrer sprachlichen Bezeichnung in Verbindung zu setzen. Dafür eignen sich Bilder in besonderem Maße, was die große Zahl von Bildlexika und der große Anteil mit sprachlichen Annotationen versehener Illustrationen in wissenschaftlich-technischen Lehrmaterialien belegen. Die Strukturen des menschlichen Gehirns speichern einen großen Teil der wahrgenommenen Informationen bildhaft. Daher können Vokabeln in Kombination mit Bildern besser erlernt werden als in reiner textueller Form. Ein vielversprechendes Anwendungsgebiet steganographischer Illustrationen sind daher interaktive Vokabeltrainer (siehe Abbildung 4). Hier encodieren Bildsets, die das Alter der intendierten Zielgruppe berücksichtigen, deren sprachliche Bezeichnungen objektlokal. Selektiert der Nutzer diese Bereiche, wird die Objektdarstellung mit deren Bezeichnung in einer Fremdsprache überlagert. Da beim Erlernen einer Fremdsprache zudem die Aussprache dieser Termini wesentlich ist, sind auch Verweise auf Audiodateien zu encodieren.

5 Zusammenfassung

Das vorliegende Papier entwickelt das Konzept des steganographischen Illustrierens, das die in der Computergraphik entwickelten Interaktionsmöglichkeiten in begrenzten Maße auch für steganographische Bildbetrachter zugänglich macht. Die im Papier skizzierten Try&Buy-Anwendungen machen eine objektlokale Encodierung der benötigten Zusatzinformationen und deren Robustheit gegenüber Formatkonvertierungen, Ausschnittbildungen und Skalierungen notwendig. Da herkömmliche steganographische Verfahren diesen Anforderungen nicht genügen, wird skizziert, welche in Annotationswasserzeichen und der Kryptographie entwickelten Techniken zu adaptieren sind. Dieser Ansatz wirft eine ganze Reihe offener Fragestellungen hinsichtlich der benötigten Kapazität, Transparenz und Robustheit auf. Außerdem wird ein Protokoll für steganographische Try&Buy-Anwendungen vorgestellt, das — kombiniert mit kryptographischen Ansätzen aus dem Bereich Shared Keys und Public-Key-Verfahren — in einem Try&Buy-Szenarium wichtige Aspekte des Schlüsselmanagements anspricht.

Literatur

[Ala00a] Adnan M. Alattar. Bridging Printed Media and the Internet via Digimarc's Watermarking Technology. In *Electronic Proceedings ACM Multimedia 2000 Workshops*, 2000.

[Ala00b] Adnan M. Alattar. Smart Images Using Digimarc's Watermarking Technology. In *Proceedings of SPIE Security and Watermarking of Multimedia Contents II*, volume 3971, pages 264–273, 2000.

[Dit00] Jana Dittmann. *Digitale Wasserzeichen*. Springer Verlag, Berlin, 2000.

[DSA00] Jana Dittmann, Petra Steinebach, Martin Wohlmacher, and Ralf Ackermann. Digital Watermarks Enabling E-Commerce Strategies: Conditional and User Specific Access to Services and Resources. *EURASIP Journal on Applied Signal Processing*, 2002(2):174–184, February 2000. (Special Issue on Emerging Applications of Multimedia Data Hiding).

[GGH02] Xianfeng Gu, Steven J. Gortler, and Hugues Hoppe. Geometry Images. In John Hughes, editor, *SIGGRAPH 2002 Conference Proceedings*, Annual Conference Series, pages 335–361. ACM Press/ACM SIGGRAPH, 2002.

[HSHS02] Knut Hartmann, Stefan Schlechtweg, Ralf Helbing, and Thomas Strothotte. Knowledge-Supported Graphical Illustration of Texts. In Maria De Marsico, Stefano Levialdi, and Emanuele Panizzi, editors, *Proc. of the Working Conference on Advanced Visual Interfaces (AVI 2002)*, pages 300–307, Trento, Italy, May, 22–24 2002. ACM Press, New York.

[JDJ00] Neil F. Johnson, Zoran Duric, and Sushil Jajodia. *Information Hiding Steganography and Watermarking-Attacks and Countermeasures*. Kluwer Academic Pub Books, 2000.

[KP00] Stefan Katzenbeisser and Fabien A.P. Petitcolas, editors. *Information Hiding*

Techniques for Steganography and Digital Watermarking. (computer security series). Artech House Books, 2000.

[KSD02] Guido Kratz, Martin Steinebach, and Jana Dittmann. Innovative Geschäftsmodelle auf der Basis digitaler Wasserzeichen — Werbenetze von Affiliates. In Patrick Horster, editor, *Sichere Geschäftsprozesse*, pages 43–54. it Verlag, 2002.

[PRS97] Bernhard Preim, Andreas Raab, and Thomas Strothotte. Coherent Zooming of Illustrations with 3D-Graphics and Text. In W.E. Davis, M. Mantei, and V. Klassen, editors, *Proc. of Graphics Interface '97*, pages 105–113, Kelowna, BC, Canada, May, 19–23 1997. Canadian Human-Computer Communications Society.

[S+98] Thomas Strothotte et al. *Computational Visualization: Graphics, Abstraction, and Interactivity*. Springer Verlag, Berlin, 1998.

[Sch95] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 2nd edition edition, 1995.

[SS99] Stefan Schlechtweg and Thomas Strothotte. Illustrative Browsing: A New Method of Browsing in Long On-line Texts. In M.A. Sasse and C. Johnson, editors, *Computer Human Interaction. Proc. of INTERACT-99*, pages 466–473, Edinburgh, September 1999. IOS Press. Amsterdam.

[SS02] Thomas Strothotte and Stefan Schlechtweg. *Non-Photorealistic Computer Graphics: Modeling, Rendering and Animation*. Morgan Kaufmann Publishers, Los Altos, 2002.

[Tuf97] Edward R. Tufte. *Visual Explanations: Images and Quantaties, Evidence and Narrative*. Graphics Press, Cheshire, 1997.