Fachseminar
Graphische Datenverarbeitung SS99

Prof. M. Gross

Robust Mesh Watermarking

Emil Praun, Hugues Hoppe, Adam Finkelstein

Seminararbeit von Donat Hauser

Inhaltsverzeichnis

EINLEITUNG....2
ANSATZ....2
BASISFUNKTIONEN....3
Konstruktion des progressiven Meshes....3
Identifikation der signifikanten Bereiche....4
Wahl der Basisfunktionen....4
WATERMARKING-PROZESS....5
Erzeugen der Watermark....5
Einfügen der Watermark....6
Auslesen der Watermark....6
Analyse....7
RESULTATE....7
Angriffsarten....7
Reveiver Operating Characteristic....9
AUSSICHTEN....10
ANHANG: OPTISCHE AUSWIRKUNGEN DER ANGRIFFE....11

Einleitung

Watermarking ist ein Mechanismus, der erlaubt, digitale Daten mit einem unsichtbaren Muster zu versehen, um sie vor unerlaubter Vervielfältigung zu schützen. Durch „Aufdecken“ des Musters kann das Eigentum an einem digitalen Dokument nachgewiesen werden.
Die zunehmenden Bedeutung der elektronischen Medien und die Möglichkeit, digitales Material einfach zu vervielfältigen, haben bereits zur Entwicklung diverser kommerzieller Watermarking-Verfahren geführt. Diese Verfahren sind fast ausschliesslich nur auf Bild-, Video- und Audiodaten anwendbar. Dem Watermarking von 3D-Modellen wurde bisher nur wenig Aufmerksamkeit geschenkt. Die für Bild-, Video- und Audiodaten entwickelte Technik ist nicht analog für beliebige 3D-Geometrie-Daten anwendbar.

Die Anforderungen an ein Watermarking-Verfahren zum Schutz von Urheberrechten sind :

Robustheit: Die Watermark muss Angriffen möglichst gut standhalten. Das Auslöschen einer Watermark durch besonders starke Angriffe soll zu einem erheblichen Qualitätsverlust des Dokuments führen.

Unsichtbarkeit: Die Watermark soll statistisch und visuell unsichtbar sein.

Eindeutigkeit: Die Watermark eines Dokuments muss den Besitzer eindeutig identifizieren.

Ansatz

Das verbreitetste Watermarking-Verfahren für Bilder-, Video- und Audiodaten ist die Spread-Spectrum-Methode. Die Daten werden mittels DCT (Diskrete Cosinus Transformation) oder Wavelet-Transformation in den Frequenzbereich transformiert, wo die Koeffizienten der Basisfunktion mit grösster Energie identifiziert werden. Das Einfügen einer Watermark $w = \{w_1 \dots w_m\}$ erfolgt durch Skalierung der m grössten Koeffizienten mit einem Faktor $(1+\alpha w_i)$.
Anschliessend wird das Dokument zurück in den Zeit-/Bildraum transformiert.
Die Watermark w^* eines verdächtigen Dokumentes lässt sich leicht extrahieren, indem man die Differenzen der Frequenz-Koeffizienten des verdächtigen und des Originaldokuments bildet. Aufgrund der statistischen Korrelation zwischen w und w^* entscheidet man über das Vorhandensein der gesuchten Watermark im verdächtigen Dokument. Die Spread-Spectrum-Methode hat sich als sehr robust erwiesen.
Für 3D-Flächenmodelle gibt es eine Vielzahl von Repräsentationsmöglichkeiten. Das hier vorgestellte Watermarking-Verfahren operiert auf Dreieckmeshes, da sie den „kleinsten gemeinsamen Nenner“ aller Flächenrepräsentationen darstellen. Es ist leicht möglich, andere Repräsentationen in Dreieckmeshes zu konvertieren.

Bei der Anwendung des Spread-Spectrum Ansatzes auf ein Watermarkingverfahren für Dreieckmeshes gibt es folgende zwei Probleme:

- Es gibt für Dreieckmeshes keine natürliche Frequenzraumtransformation.
  Dreieckmeshes lassen sich in progressive Meshes konvertieren, die ähnliche Eigenschaften aufweisen wie traditionelle

Wavelet-Transformationen. Diese neue Meshdarstellung erlaubt die Identifikation von signifikanten Oberflächenausprägungen. Mit einem geeigneten Verfahren konstruiert man eine Menge von Basisfunktionen $\Phi = (\phi^1 \ldots \phi^m)$ über das Mesh und perturbiert die Knoten, ohne die Meshverbindungsstruktur zu verändern.

- Angriffe können die Verbindungsstruktur eines Meshes beliebig verändern. Auf einem Dreieckmesh ist keine Ordnung definiert, wie dies bei Audio (Zeit) oder Bilddaten (Raster) der Fall ist.
  Ein geeignetes Resamplingverfahren ist in der Lage, das angegriffene Mesh unter Verwendung des Originalmeshes abzutasten und für die Extraktion der Watermark geeignet zu rekonstruieren.

Der Ablauf des Verfahrens: In einem ersten Schritt wird eine Menge von skalaren Basisfunktionen über dem Mesh erstellt. Danach wird analog zur Spread-Spectrum-Methode die Watermark mit Hilfe der Basisfunktionen in das Mesh eingebettet. Bevor eine Watermark aus einem verdächtigen Mesh ausgelesen werden kann, muss zunächst eine Registration und ein Resampling durchgeführt werden. Diese Verfahren sorgen dafür, dass die Meshstruktur dem Originalmesh angepasst wird und erlauben die anschliessende Extraktion der Watermark.

Basisfunktionen

Für jeden Koeffizienten w_i des Wasserzeichens konstruiert man eine skalare Basisfunktion ϕ_j^i über die Meshknoten und bestimmt eine globale Verschiebungsrichtung $\mathbf{d}_i$. Für jeden Koeffizienten w_i wird jeder Knoten v_i um einen Vektor proportional zu $w_i \phi_j^i \mathbf{d}_i$ perturbiert.
Um die Robustheit zu gewährleisten, müssen die Basisfunktionen über einem grossen, visuell signifikanten Bereich des Meshes definiert werden. Zu diesem Zweck wird das Mesh in ein progressives Mesh konvertiert, bestehend aus einem groben Basismesh und einer Sequenz von Verfeinerungsoperationen. Davon wählt man die *m* Verfeinerungsoperationen, welche die grösste geometrische Änderung im Modell bewirken. Für jede der *m* Verfeinerungsoperationen konstruiert man eine skalare Basisfunktion über einem bestimmten Nachbarschaftsbereich des Meshes. Die *m* Basisfunktionen bilden Φ und werdet für das Einfügen der Watermark verwendet. Später benutzt man die gleichen über dem Originalmesh definierten Basisfunktionen, um die Watermark eines verdächtigen Meshes zu extrahieren.

Konstruktion des progressiven Meshes

Für die Konstruktion eines progressiven Meshes werden folgende zwei Operationen verwendet:
restricted edge collapse: Ein Knoten wird mit seinem Nachbarknoten vereinigt, wodurch im allgemeinen eine Kante und die zwei daran anliegenden Dreiecke verschwinden.
vertex split: Die zur *restricted edge collapse* Operation inverse Transformation.
Das Mesh wird durch sequentielle Anwendung von *restricted edge collapse* Operationen in ein vereinfachtes Mesh konvertiert. Das so erhaltene grobe Basismesh lässt sich durch eine Sequenz von *vertex split* Operationen wieder mit beliebiger Genauigkeit in das Originalmesh zurückverwandeln.
Die einzelnen *restricted edge collapse* Operationen werden so gewählt, dass die geometrische Gestalt des Originalmeshes möglichst erhalten bleibt. Dazu schätzt man die Position eines neu einzufügenden Knotens, indem man mit Hilfe der unmittelbaren Nachbarknoten den Schwerpunkt und darauf die Flächennormale berechnet. Als Mass für die geometrische

Auswirkung einer *restricted edge collapse* Operation bildet man nun die Distanz h als Differenz zwischen den Normalen des geschätzten und des effektiven Punktes.

Identifikation der signifikanten Bereiche

Nach beendigter Konstruktion des progressiven Meshes werden die *m vertex split* Operationen mit grösster geometrischer Auswirkung h ausgewählt und mit einer Basisfunktion ϕ_i assoziiert. Die h_i dienen später als Skalierungsfaktoren für die Watermark-Koeffizienten w_i. Jeder *vertex split* i eines Knotens v_i identifiziert eine Nachbarschaft, die durch den Ring von Kanten um den Knoten v_i begrenzt ist. Durch progressive Verfeinerung des Meshes mittels der *vertex split* Operationen, lässt sich dieser Ring von Kanten bis in das Originalmesh zurückverfolgen und definiert dort die Nachbarschaft B_i (Abb.1). Für die Nachbarschaft B_i im Originalmesh konstruiert man eine Radius-Funktion r_j^i über den Knoten v_j mit folgender Eigenschaft: $r_j^i = 0$ für den Zentrumsknoten c_i und $r_j^i = 1$ für Knoten an der Grenze oder ausserhalb des Nachbarschaftsbereiches. Für alle übrigen Knoten innerhalb des Nachbarschaftsbereiches gilt:

$$r_j^i = \frac{d(v_j, \{c_i\})}{d(v_j, \{c_i\}) + d(v_j, B_i)}$$

Dabei ist $d(v,S)$ die Länge des kürzesten Pfades zwischen v und einem beliebigen Knoten aus der Menge S. Die Distanzen $d(v_j,\{c_i\})$ und $d(v_j,B_i)$ lassen sich mittels des Dijkstra Algorithmus berechnen, wobei man die Suche auf den Nachbarschaftsbereicht B_i beschränkt. Das Gewicht einer Kante entspricht ihrer Länge.

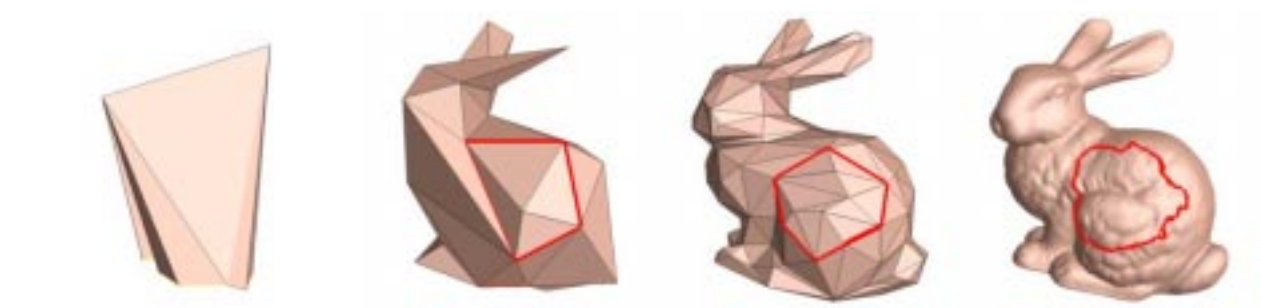


Abb. 1: Progressives Mesh in verschiedenen Auflösungsstufen mit markiertem Nachbarschaftsbereich

Wahl der Basisfunktionen

Bei der Wahl der Basisfunktionen sind zwei wichtige Punkte zu beachten:

- Die durch die Basis Funktionen hervorgerufenen geometrischen Veränderungen des Meshes sollen für einen menschlichen Beobachter möglichst unsichtbar sein.
- Die Basisfunktionen sollen möglichst orthogonal zueinander sein und bei der Registrierung keine einseitigen Translations- oder Skalierungstendenzen aufweisen.

Folgende drei Basisfunktionen wurden für das Watermarking-Verfahren untersucht:

Hut: Die einfache lineare Abbildung $\phi_j^i = 1 - r$ ergibt die Hut-Funktion.

Derby: Aufgrund der C^0 Stetigkeit des Meshes nimmt das menschliche Auge sehr leicht Unstetigkeiten wahr. Es macht deshalb Sinn, eine Basisfunktion höherer Stetigkeit zu benutzen. Die Verwendung einer Polynomialfunktion dritten Grades eliminiert die Unstetigkeiten, die bei der Hut-Funktion an den Grenzen und der Spitze vorhanden sind. Die verwendete Funktion $\phi_j^i = 2r^3 - 3r^2 + 1$ über einem Kreis gleicht einem Derby-Hut.

Sombrero: Es ist schwierig, zueinander orthogonale Basen zu bilden. Die folgende Basisfunktion hat aber die Eigenschaft, dass sie bei der Registrierung keine Translationsverschiebungen bewirkt. Zusätzlich ist das Integral der Funktion über dem Einheitskreis gleich 0. Die resultierende Sombrero-ähnliche Funktion ist $\phi_j^i = 21r^5 + 45r^4 - 25r^3 + 1$.

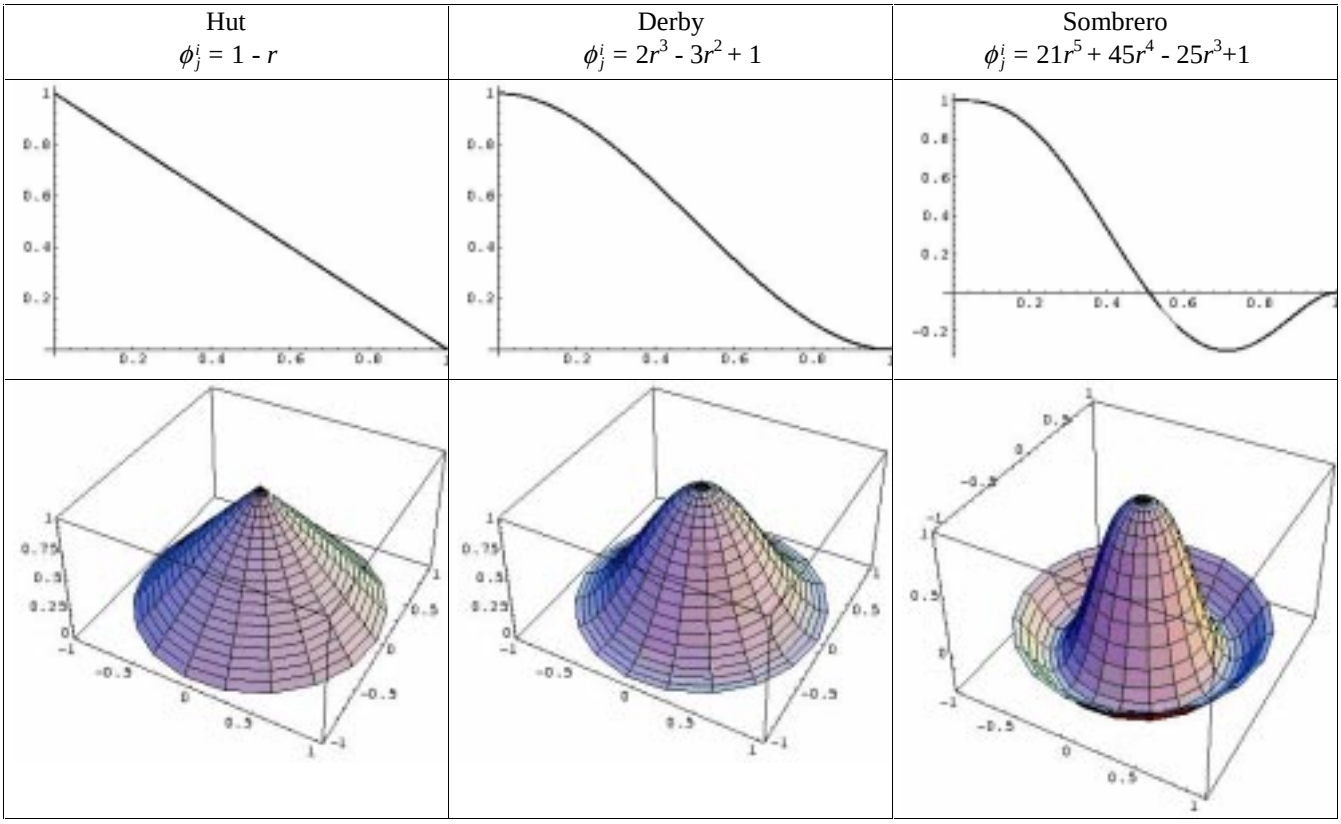


Abb. 2: Basisfunktionen

Watermarking-Prozess

Erzeugen der Watermark

In einem ersten Schritt wird ein Watermark-Vektor $w = (w_1 \ldots w_m)^T$ gebildet. Die Koeffizienten w_i sind reelle Zahlen aus einer Normalverteilung mit Mittelwert 0 und Varianz 1. Um die Watermark zu einer nicht invertierbaren Funktion des Originaldokumentes zu machen, bildet man davon einen Hashwert mittels einer kryptographischen Hashfunktion. Das Resultat dient als Initialwert eines kryptographischen Zufallsgenerators, der die Watermark der gewünschten Länge erzeugt.

Einfügen der Watermark

Das Einfügen der Watermark in das Dokument geschieht folgendermassen. Jede Basisfunktion wird mit einem Koeffizienten multipliziert und zu den 3D-Koordinaten der Mesh-Knoten hinzu addiert. Jede Basisfunktion hat einen skalaren Effekt ϕ_j^i an jedem Knoten und eine globale Verschiebungsrichtung $\mathbf{d}_i$.
Als Matrix Multiplikation sieht dieser Vorgang für jede der 3 Koordinaten X,Y und Z wie folgt aus:

$$\begin{bmatrix} \\ v'_X \\ \\ \end{bmatrix} = \begin{bmatrix} \\ v_X \\ \\ \end{bmatrix} + \varepsilon * \begin{bmatrix} \\ \Phi \\ \\ \end{bmatrix} * \begin{bmatrix} h_1 d_{1x} & & 0 \\ & \ddots & \\ 0 & & h_m d_{mx} \end{bmatrix} * \begin{bmatrix} \\ w \\ \\ \end{bmatrix}$$

v'_X : Kolonnenvektor, der die X-Koordinaten der mit der Watermark versehenen Meshknoten enthält

v_X : Kolonnenvektor, der die X-Koordinaten der Original-Meshknoten enthält

ε : globaler Skalierungsparameter für die Energie der Watermark

Φ : n × m Matrix, dessen Kolonnen die skalaren Basisfunktionen ϕ^i enthalten

hd_x : m × m Diagonalmatrix, die Einträge stellen die X Komponenten der Veschiebungsrichtung skaliert mit der Basisfunktionshöhe h_i dar

w : Watermark

Zusammenfassen der Matrixzeilen und der Vektoren, die den drei Koordinatenkomponenten (X,Y,Z) entsprechen, führt zu folgender vereinfachter Gleichung:

$$\mathbf{v'} = \mathbf{v} + \mathbf{B} * w$$

Das Originaldokument **v** zusammen mit der Watermark wird gespeichert und geheimgehalten. Das mit der Watermark versehene Dokument **v´** wird veröffentlicht.

Auslesen der Watermark

Bevor man das Vorhandensein einer Watermark in einem verdächtigen Mesh überprüfen kann, muss zunächst ein Registrierungs- und danach ein Resampling-Prozess durchgeführt werden. Die Registrierung sorgt dafür, dass das verdächtige Mesh durch geeignete Transformationen (Translation, Rotation und uniforme Skalierung) in das gleiche Koordinaten-Frame wie das Originalmesh gebracht wird.
Das Ziel des Resamplings besteht darin, ein Mesh mit der Topologie des Originalmeshes und der Geometrie des verdächtigen Meshes zu erhalten. Das verwendete Resampling-Verfahren basiert auf der Minimierung einer Energiefunktion, die Distanzdifferenzen, Deformierung und das Kippen von Flächen berücksichtigt.
Nun wird die Differenz der 3D-Koordinaten zwischen den Knoten des vorverarbeiteten verdächtigen Meshes und des Originalmeshes gebildet. Mittels des 3D-Residuenvektor erhält man nun die Watermark durch Lösen des folgenden Gleichungssystems mit der Methode der kleinsten Quadrate:

$$\mathbf{B}\, w^* = (\mathbf{v}^* - \mathbf{v})$$

w^* : die extrahierte Watermark

$\mathbf{v}^*$: Knoten-Koordinaten des vorverarbeiteten, verdächtigen Meshes

$\mathbf{v}$: Knoten-Koordinaten des Originalmeshes

Analyse

Für den Vergleich der eingefügten und extrahierten Watermark dient eine statistische Analyse. In einem ersten Schritt werden die extrahierten Watermark-Koeffizienten gefiltert. Da man erwartet, dass diese normalverteilt mit Mittelwert 0 und Varianz 1 sind, verwirft man Koeffizienten, welche einen gewissen Schwellwert überschreiten. Eine kleine Anzahl verworfener Elemente der Watermark hat nur geringe Auswirkung auf die Analyse. In einem zweiten Schritt wird aus den verbleibenden Koeffizienten und den entsprechenden Werten der eingefügten Watermark ein linearer Korrelationsfaktor ρ berechnet.

$$\rho = \frac{\sum_i (w_i^* - \overline{w^*})(w_i - \overline{w})}{\sqrt{\sum_i (w_i^* - \overline{w^*})^2 \times \sum_i (w_i - \overline{w})^2}} \quad , -1 \le \rho \le 1$$

$\overline{w}$: Mittelwert aller Vektorelemente der Watermark

Zum Schluss berechnet man aus ρ mittels Student-Verteilung die Wahrscheinlichkeit P_{fp}, ob die Korrelation einer zufällig generierten Watermark w^* so gross ist wie das beobachtete ρ. P_{fp} ist die falsch positive Wahrscheinlichkeit und stellt das Risiko dar, eine Watermark als vorhanden zu erklären obwohl sie es gar nicht ist.
Ist eine binäre Antwort für das Akzeptieren der Watermark erwünscht, so vergleicht man P_{fp} mit einem Schwellwert P_{krit}. Für $P_{fp} < P_{krit}$ lautet die Antwort ja. Diese Antwort ist probabilistisch, d.h. es besteht eine gewisseWahrscheinlichkeit, dass das Ergebnis falsch ist.
Das Risiko für ein falsch negatives Ergebnis (die Watermark ist vorhanden, aber wir können sie nicht identifizieren) kann im allgemeinen nicht analytisch berechnet werden, da es von der Art des Angriffs abhängig ist. Durch Verändern des Schwellwertes kann allerdings die Wahrscheinlichkeit von falsch positiven Ergebnissen auf Kosten von falsch negativen verringert werden.

Resultate

Angriffsarten

Im folgenden werden die Resultate verschiedener Angriffe auf vier Meshmodelle erläutert. Jeder Test wurde 5 mal wiederholt unter Verwendung verschiedener Initialwerte für den Zufallsgenerator. Die Einträge der Tabelle sind Mittelwerte der 5 Tests. Als Basisfunktion wurde die Sombrero-Funktion gewählt. Die Watermark umfasst 50 Koeffizienten und der Skalierungsfaktor ε= 0.01.
Die Einträge haben folgendes Format: ρ (nn)P_{fp}
ρ: linearer Korrelationsfaktor
(nn): Anzahl Koeffizienten für die Berechnung von ρ
P_{fp}: falsch positive Wahrscheinlichkeit
fettgedruckten Resultate: Bilder der angegriffenen Meshmodelle sind im Anhang aufgeführt

Angriffsart	Reg.	Res.	Fandisk	Kopf	Drache	Hase
A. Kein Angriff			1.00(50) 0	1.00(50) 0	1.00(50) 0	1.00(50) 0
B. Knoten Umordnung		✓	0.85(49) 10^{-14}	0.87(48) 10^{-15}	0.88(49) 10^{-16}	0.93(50) 10^{-21}
C. Noise .2%			0.86(48) 10^{-14}	0.82(48) 10^{-12}	0.90(47) 10^{-17}	0.98(50) 10^{-35}
D. Noise .45%			0.65(42) 10^{-5}	0.67(42) **10^{-6}**	0.75(47) 10^{-9}	0.93(48) 10^{-21}
E. Noise .7%			0.49(41) 10^{-3}	0.62(39) 10^{-5}	0.60(43) 10^{-5}	0.87(48) 10^{-15}
F. Taubin Glättung			0.83(47) **10^{-12}**	0.99(48) 10^{-38}	0.98(50) 10^{-32}	1.00(50) 0
G. Ähnlichkeitstransformation	✓		0.98(50) 10^{-33}	0.95(46) 10^{-24}	0.96(50) **10^{-29}**	0.97(50) 10^{-29}
H. Vereinfachung 1/2 #Dreiecke		✓	0.82(50) 10^{-12}	0.74(48) 10^{-9}	0.67(48) **10^{-7}**	0.89(50) 10^{-17}
I. Vereinfachung 1/8 #Dreiecke		✓	0.80(48) 10^{-11}	0.47(43) 10^{-3}	0.39(48) 10^{-2}	0.84(48) **10^{-13}**
J. Zweite Watermark			0.71(47) 10^{-8}	0.70(43) **10^{-7}**	0.89(49) 10^{-17}	0.64(46) 10^{-6}
K. Crop			1.00(43) 0	1.00(48) 0	1.00(43) 0	1.00(44) **0**
L =B+C		✓	0.81(49) 10^{-12}	0.65(44) 10^{-6}	0.80(48) 10^{-11}	0.96(50) 10^{-28}
M =B+G *p*	✓	✓	0.81(50) 10^{-12}	0.82(48) 10^{-12}	0.86(50) 10^{-15}	0.93(48) 10^{-20}
N =C+G	✓		0.82(46) 10^{-11}	0.83(45) 10^{-12}	0.86(49) 10^{-15}	0.95(50) 10^{-24}
O =G+L	✓	✓	0.96(41) 10^{-22}	0.76(45) 10^{-9}	0.94(42) 10^{-20}	0.93(42) 10^{-18}
P=B +C +G	✓	✓	0.83(47) 10^{-12}	0.57(47) 10^{-4}	0.85(50) 10^{-14}	0.93(50) 10^{-22}
Q =B+G+H	✓	✓	0.83(50) 10^{-13}	0.74(48) 10^{-9}	0.62(50) 10^{-6}	0.88(50) 10^{-17}
R = Alle (B,C,F,G,H,J,K)	✓	✓	0.36(46) **10^{-2}**	0.35(42) 10^{-2}	0.36(49) 10^{-2}	0.58(49) 10^{-5}

Tabelle 1: Resultate von spezifischen Angriffen auf verschiedene Modelle

Bemerkungen zu den spezifischen Angriffsarten:

B Die Resultate zeigen die Auswirkungen des Resamplings auf das Detektionsverfahren. Obwohl die Geometrie des Modells durch den Angriff nicht verändert wurde, sind die falsch positiven Wahrscheinlichkeiten grösser null. Für das Resampling verwendet man das unveränderte Originalmesh, um zu vermeiden, dass bei diesem Vorgang Informationen der Watermark in das verdächtige Mesh einfliessen. Aus gleichem Grund sind auch die Wahrscheinlichkeiten von (G) grösser null.

C,D,E Beim Noise-Angriff werden alle Knotenvektoren mit einen zufälligen Richtungsvektor perturbiert. Der Noise-Faktor entspricht der Länge des Richtungsvektors relativ zum Durchmesser des Objekts.

F Dieser Angriff zeigt die Auswirkungen von 10 Iteration eines Taubin-Glättungsfilters auf die Knotenkoordinaten. Das Filter glättet im Speziellen eckige Kanten und hat nur beschränkte Wirkung auf Modelle, die bereits relativ glatt sind.

H, I Die Vereinfachungen dieses Angriffs beruhen auf *full edge collapse* Operationen, welche an ausgesuchten Stellen eine Kante durch einen Knoten ersetzen. Bei starken Vereinfachungen behalten nur wenige Knoten ihre ursprüngliche Position. Dieser Angriff kann deshalb als Remeshing betrachtet werden. Es ist zu beachten, dass aggressive Vereinfachungen Teile der Watermark an ausgeprägten Stellen eliminieren können (z.B. im Schwanz oder Kopf des Drachens). Darunter leidet aber die visuelle Qualität des Modells.

J Da sich die Geometrie des Meshes vom Originalmesh unterscheidet, unterscheidet sich auch die Sequenz der restricted edge collapse Operationen, die beim Einfügen einer zweiten Watermark verwendet wird.

K Dieser Crop-Angriff besteht aus der Elimination aller Knoten im rechten Drittel der Bounding-Box des Objektes. Das Resampling Verfahren identifiziert alle Knoten, die im verdächtigten Mesh fehlen und die entsprechenden Watermark-Koeffizienten werden bei der Extraktion der Watermark aus dem Gleichungssystem entfernt. Da gewisse Kolonnen linear abhängig werden können, löst man das Gleichungssystem mittels

Singulärwertzerlegung. Weil alle überlebenden Watermark Koeffizienten extrahiert werden können, ergibt sich bei diesem Angriff eine falsch positiv Wahrscheinlichkeit von null.

Reveiver Operating Characteristic

Eine Standardmethode für die Visualisierung von probabilistischen Detektionsverfahren sind die ROC (receiver operating characteristic) Kurven. Im Falle von Watermarking-Verfahren stellt man die Wahrscheinlichkeit von falsch positiven Ergebnissen der Wahrscheinlichkeit von falsch negativen gegenüber. Eine ideale Kurve verläuft so nah wie möglich am Ursprung unten links, wo die Wahrscheinlichkeiten von falsch negativen und falsch positiven Ergebnissen gleichzeitig klein sind.

In der Praxis ist man primär an der Grösse der falsch positiv Wahrscheinlichkeit interessiert, die besagt, wie wahrscheinlich man eine unschuldige Person fälschlicherweise beschuldigt, ein Modell mit einer eigener Watermark zu besitzen. Für jede falsch positive Wahrscheinlichkeit lässt sich die entsprechende falsch negative Wahrscheinlichkeit ablesen, die der Wahrscheinlichkeit entspricht, dass wir eine schuldige Person nicht anklagen.

Die drei Kurven von Abb. 3 entsprechen Noise-Angriffen von verschiedener Stärke (Angriffe C, D und E in Tabelle 1). Jede ROC Kurve wurde durch 200 Tests mit randomisierten Noise-Angriffen ermittelt. In jedem Test k wurde eine andere Watermark und ein anderes Noise-Muster verwendet. Als Ergebnis jedes Tests erhält man die falsch positive Wahrscheinlichkeit P_{fp}^k. Wählt man P_{fp}^k als Entscheidungsschwellwert für die Präsenz einer Watermark, dann würden alle Tests mit grösseren Wahrscheinlichkeitswerten falsch negative Ergebnisse darstellen. Die falsch negative Wahrscheinlichkeit P_{fn}^k, die P_{fp}^k entspricht, berechnet sich aus dem Anteil der 200 Tests, der eine falsch positive Wahrscheinlichkeit grösser als P_{fp}^k aufweist. Die ROC Kurve besteht aus 200 Punkten mit Koordinaten (P_{fp}^k, P_{fn}^k).

Will man nun beispielsweise 99.9% sicher gehen, keine unschuldigen Personen anzuklagen (falsch-positiv-Schwellwert von 0.001), so wird man im Falle des worst-case Noise-Angriffs (0.7%) mit 37% Risiko die Watermark nicht finden. Bei schwächeren Angriffen ist es bei gleicher falsch-positiv-Wahrscheinlichkeit noch sicherer, keine unschuldige Personen anzuklagen.

Damit eine Watermark robust ist, muss sie Angriffen widerstehen können, die ein Modell nicht visuell gravierend verändern. Die präsentierten Resultate sind in dieser Hinsicht sehr gut, wenn man berücksichtigt, dass die Modelle einen beträchtlichen optischen Qualitätsverlust erlitten haben.

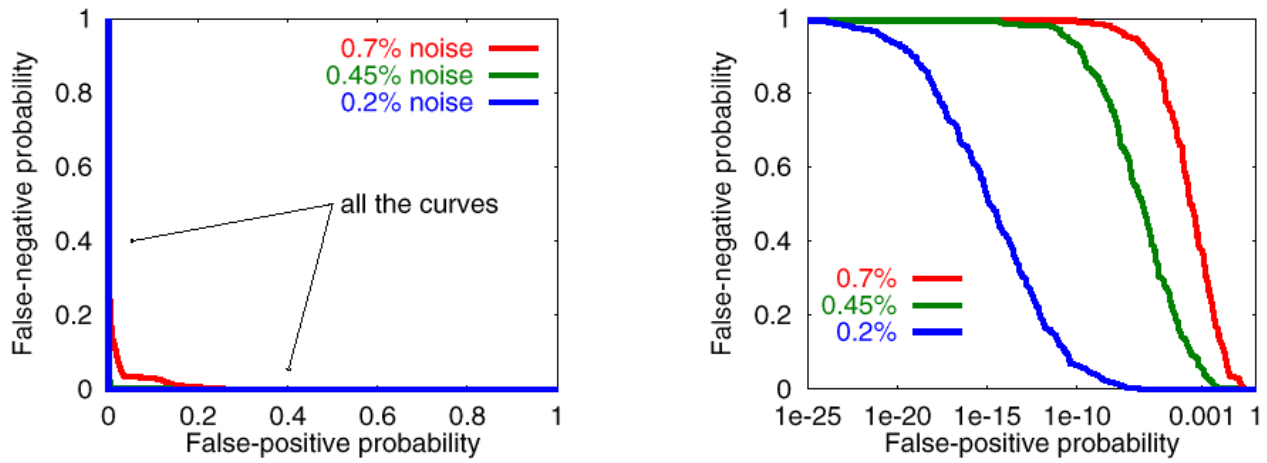


Abb. 3: ROC Kurven für verschiedene Noise-Angriffe auf das Fandisk Modell

Aussichten

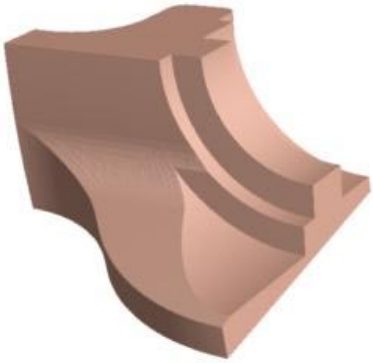
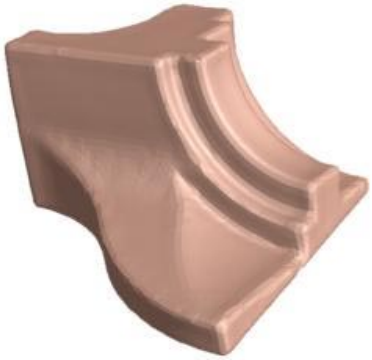
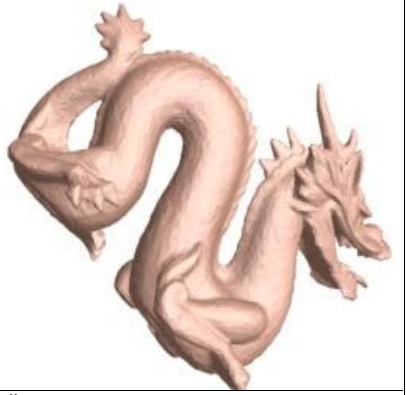
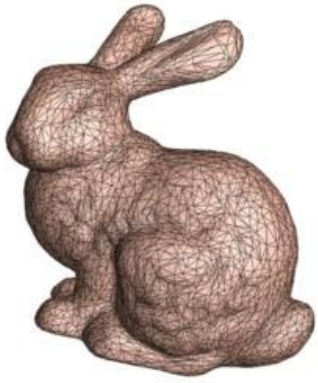
Aussichten auf zukünftige Projekte:

Schnelle Verwerfung: Es ist wünschenswert, ein verdächtiges Modell schneller auf das Vorhandensein einer bestimmten Watermark überprüfen zu können. Dies würde den Einsatz von automatisierten Agenten ermöglichen, mit der Aufgabe nach gestohlenen Dokumenten zu suchen. Die Entwicklung schneller Verwerfungsverfahren ist geplant.

Alternative Flächenrepräsentationen: Von Interesse sind Watermarking-Verfahren für andere Flächenrepräsentationen wie Subdivisionsflächen, CSG Modelle und Bezier/B-Spline Patches. Da diese Repräsentationen oft weniger Parameter verwenden, stellt die Entwicklung eines Watermarking-Verfahrens eine spezielle Herausforderung dar.

Andere Angriffe: Es ist unmöglich, alle möglichen Angriffe auf ein 3D-Modell vorauszusehen. Es ist ebenfalls schwierig, das Ausmass des Schadens eines bestimmten Angriffes abzuschätzen. Es gibt zahlreiche Angriffe, die bei dem vorgestellten Watermarking-Verfahren nicht berücksichtigt wurden, im speziellen affine, projektive und beliebig freie Transformationen. Die affinen und projektiven Transformationen können durch Erweiterung des Registrierungs-Algorithmus behandelt werden. Ein grösseres Problem stellen allerdings die Transformationen mit beliebiger Anzahl Freiheitsgraden dar, sog. FFDs (Free Formed Deformation).

Anhang: Optische Auswirkungen der Angriffe

		
Fandisk (12,946 Dreiecke)	Geglättet	Alle Angriffe
		
Kopf (13,408 Dreiecke)	0.45% noise	Zweite Watermark
		
Drache (30,000 Dreiecke)	1/2 # Dreiecke	Ähnlichkeitstransformation
		
Hase (69,473 Dreiecke)	1/8 #Dreiecke	abgeschnitten