

روشی مقاوم در نهان‌نگاری مدل‌های سه‌بعدی مثلثی مبتنی بر میانه

رضا فرید^{*}، نصرا... مقدم چرکری[†]

چکیده

در این نوشتار، روشی در خصوص نهان‌نگاری اطلاعات در مدل‌های سه‌بعدی مثلثی معرفی می‌گردد. ایده اصلی این روش افزودن مثلث‌هایی به مدل است؛ به نحوی که این افزایش بتواند اطلاعات مورد نظر برای گنجاندن را نمایندگی کند. روش ساخت مثلث‌ها نیز بر اساس انتخاب مجموعه‌ای از مثلث‌ها بر حسب مساحت آن‌ها و انتخاب یکی از میانه‌های مثلث بر حسب رشته پیامی که هدف اصلی، گنجاندن آن در مدل است؛ استوار می‌باشد. می‌دانیم که میانه مثلث در برابر تغییر مقیاس یکنواخت و انتقال مقاوم است. همچنین برای مقاومت در برابر چرخش، ترتیب خاصی را در انتخاب میانه و مثلثی که به مدل افزوده می‌شود، در نظر گرفته‌ایم. افزون بر این موارد، گنجاندن بر حسب ترتیب خاصی از مثلث‌ها صورت می‌گیرد تا در استخراج از همین ترتیب استفاده گردد. در آزمون‌های صورت گرفته مشخص گردید که روش پیشنهادی در برابر مجموعه حمله‌های چرخش، تغییر مقیاس و انتقال، که به حمله مشابهت نیز موسوم است، مقاوم می‌باشد.

کلمات کلیدی

نهان‌نگاری مدل‌های سه‌بعدی، مدل‌های زبان مدل‌سازی واقعیت مجازی، مقاومت، حمله مشابهت، عدم نیاز به مدل اصلی.

A Robust Median-Based Digital Watermarking for Triangular 3D Models

Reza Farid, Nasrollah Moghaddam Charkari

Abstract

In this paper, a blind robust median-based method for embedding and extracting a data stream in a triangular 3D model is introduced. The basic idea is based on adding some new triangles to the model based on a message. Some triangles of the model will be selected according to their areas, and for each selected triangle, one of its three medians will be chosen. Furthermore, based on the chosen median, two triangles will appear. Choosing and adding one of these triangles will be held up to the embedding code. Since median is resistant to translation and uniform scaling, being robust against these two attacks is expected. Also, according to use a specific order in choosing a median and new triangle, this method is supposed to be robust against rotation. The experiments show that the proposed method is robust against all the mentioned attacks; it means it is robust against similarity transformation.

Keywords

3D Digital Watermarking, VRML (Virtual Reality Modeling Language), Robustness, Similarity transformation, Blind Detection.

* دانشجوی کارشناسی ارشد، دانشگاه تربیت مدرس، دانشکده فنی و مهندسی، بخش مهندسی برق، ۰۹۱۲۲۵۴۴۷۴۳، reza_farid@modares.ac.ir

† استادیار، دانشگاه تربیت مدرس، دانشکده فنی و مهندسی، بخش مهندسی برق، ۸۸۰۱۱۰۰۱ داخلی ۳۳۰۱، charkari@modares.ac.ir

۱- مقدمه

روشنایی و کنتراست قابل توجه است [۲۰]. لذا توجه به وجود نمونه آزمون نیز مدنظر قرار می‌گیرد.

به ازای حملات قابل طرح، روش‌های مقابله نیز مورد توجه قرار گرفته‌اند. یکی از مهمترین نتایجی که در این مسیر بدست می‌آید، این موضوع است که از آن‌جا که حملات، کلیت رسانه را خدشه‌دار نمی‌سازند؛ نهان‌نگاری مبتنی بر محتوای رسانه می‌تواند به عنوان شیوه‌ای کارآمد در افزایش مقاومت نهان‌نگاری تلقی گردد. این نوع نهان‌نگاری سعی دارد با یافتن نقاط مشخصه‌ای از رسانه که در برابر حملات گوناگون مقاوم هستند، کار گنجاندن اطلاعات را به انجام برساند [۶، ۱۲ و ۲۶]. بررسی اجمالی تخریب نهان‌نگاری داده در تصویر و چند روش مقابله با آن را در مرجع [۱] می‌توانید مشاهده کنید.

تمرکز این نوشتار بر رسانه‌ای از نوعی دیگر و در بُعدی جدید یعنی مدل‌های سه‌بعدی است. مدلهایی که اصولاً شرحی از مدل را مبتنی بر نقاطی سه‌بعدی و مجموعه‌ای از سطوح مطرح می‌سازند. اهمیت این مدل‌ها در مواردی چون هنر فیلمبرداری، واقعیت مجازی، مدل‌های تجاری و صنعتی است که محصول اولیه توسط فردی خلق و توسط افراد دیگری مورد استفاده قرار می‌گیرد [۱۸].

نخستین گام در این خصوص در سال ۱۹۹۷ شکل گرفت. در تلاش‌های صورت گرفته از آن زمان تاکنون، عمدتاً سعی بر شناسایی مشخصاتی از مدل شده است که در برابر حملات تغییر نکند یا با انجام برخی تبدیلات بتوان بعد از حمله، باز همان مشخصات را یافت. این مشخصات به عنوان مقصد گنجاندن نهان‌نگاری برگزیده شده‌اند. در مرحله استخراج نیز عمده کار در همین شناسایی مشخصات پایه نهان‌نگاری است. مثلاً اگر مدل مثلث‌بندی شود، دو مقداری که یک مثلث یکتا را تعریف می‌کنند، در برابر چرخش، تغییرمقیاس یک‌نواخت و انتقال مقاوم خواهد بود [۱۳].

در تکنیک‌های گنجاندن داده در مدل‌های سه‌بعدی نیز مصالحه‌ای میان خصوصیات زیر باید در نظر گرفت: نامحسوس بودن (یا بسته به کاربرد آشکار بودن)، مقاومت و ظرفیت. این که در برابر چه تغییراتی نیز مقاومت مدنظر است، قابل دسته‌بندی است که تبدیل قالب داده، خطاهای نمایش اعداد ممیزشناور، تبدیلات چرخش، تغییرمقیاس، انتقال و تبدیل خطی انتقال یافته، شکل‌دهی مجدد مدل، تکه کردن مدل، ساده‌سازی چندضلعی‌ها در مدل نمونه‌هایی از این دست هستند.

همچنین مهم است دانسته شود در یک مدل، اجزای هندسی اولیه توصیف‌کننده مدل مورد نظر کدامند. نقاط، خطوط، چندضلعی‌ها، چندضلعی‌های متصل، چندوجهی‌ها و چندوجهی‌های متصل نمونه‌هایی از این اجزای توصیف‌کننده مدل محسوب می‌شوند.

به‌علاوه، طرز بیان مدل سه‌بعدی برای کار اهمیت دارد. مثلاً در یک مدل مثلث‌بندی‌شده می‌توان چیدمان را به صورت یک ترتیب یک بعدی از مثلث‌ها بر اساس مساحت‌شان یا ترتیبی دوبعدی از اتصال مثلث‌ها به یکدیگر بیان کرد. بیان این اجزای اولیه به دو شیوه

در دهه اخیر، با تسهیل و تسریع توزیع داده‌های رقمی توسط کامپیوترهای شخصی و ارتباطات اینترنتی، استفاده و توزیع داده‌های چندرسانه‌ای رشد چشمگیری داشته است. به تبع، مسایلی مانند حفاظت از حق‌نشر در این خصوص مطرح و به دو شکل کلی رمزنگاری و نهان‌نگاری ظاهر شده است. در نهان‌نگاری، اطلاعات در نوع مشخصی از داده رقمی، اصولاً به صورت نامحسوس، گنجانده می‌شود تا در کاربردهای گوناگونی مانند اثبات مالکیت رسانه مورد نظر، انتقال پنهان اطلاعات، تصدیق هویت، نظارت بر پخش و بانک‌های اطلاعاتی بتوان از آن بهره جست. یک نهان‌نگاری اصولاً دارای دو مرحله اصلی است: گنجاندن و استخراج. همچنین با توجه به نوع کاربردی که مدنظر است، تکنیک مورد استفاده در نهان‌نگاری و رسانه نهان‌نگاری شده باید در برابر دست‌کاری‌های سه‌وی و عمدی که می‌تواند موجب تخریب داده نهان‌شده گردد، مقاوم یا شکننده باشد. به‌علاوه نهان‌نگاری در مرحله استخراج می‌تواند نسبت به وجود رسانه اولیه، که فاقد نهان‌نگاری است، وابسته یا مستقل باشد [۲].

در نهان‌نگاری‌های انجام شده، رسانه‌های مختلفی (و در ابعاد گوناگونی) مطرح بوده‌اند. صوت به‌عنوان رسانه‌ای تک‌بعدی (در طول زمان)، تصویر به‌عنوان نگاشتی از فضای دوبعدی و تصاویر ویدئویی متحرک در نهان‌نگاری به‌صورت وسیعی مورد توجه بوده‌اند [۱۸].

در بسیاری از کاربردها، اطلاعات نهان‌نگاری شده قبل از رسیدن به گیرنده می‌تواند دستخوش پردازش‌های سه‌وی و یا عمدی گردد. این پردازش‌ها در خصوص تصاویر می‌تواند شامل مواردی مانند فشرده‌سازی با تلافی، بهسازی سیگنال، تبدیلات رقمی به قیاسی و قیاسی به رقمی، تغییر اندازه، چاپ، پیمایش [۱۹، ۲۹] و سایر اعمال پردازش تصویر باشد که منجر به دستکاری سه‌وی یا عمدی نهان‌نگاری گردد. به هر حال هر پردازشی که منجر به خنثی کردن هدف نهان‌نگاری (و نه لزوماً حذف آن) شود (و اصولاً کیفیت نهان‌نگاری منتج از آن کاهش چشمگیری نداشته باشد)؛ دستکاری، خراب‌کاری و یا حمله محسوب می‌شود [۴، ۵ و ۱۰]. حمله‌ها را می‌توان بر حسب اثر حمله روی نهان‌نگاری و شیوه‌های تفسیر نهان‌نگاری توسط شناسایی‌کننده دسته‌بندی کرد. در دسته‌بندی حملات می‌توان سلسله مراتبی بدین نحو در نظر گرفت: گروه‌های حمله، انواع حمله، کلاس‌های حمله و حملات منفرد یا نمونه حملات که در یک دسته‌بندی به چهار گروه حمله حذفی و دخل‌وتصرف، هندسی، پنهان‌نگاری و تفسیر و پروتکل می‌توان اشاره کرد [۱۱].

در حالت عمومی، ابزارهای سنجش باید حمله و سنجش خود را بر روی انواع مختلفی از رسانه مورد نظر انجام دهند. مثلاً در خصوص رسانه تصویر، هر تصویر از منظر پردازش به دلیلی مانند بافت، مناطق یکدست، حجم، ترکیب، وضعیت لبه‌ها، میزان محو بودن، میزان

[۱۶] و روش‌هایی که در دامنه تغییر شکل یافته، به گنجانند اطلاعات می‌پردازند. مثلاً روش‌های دسته دوم از تکنیک‌های طیف گسترده، تجزیه مش تحلیل چندگانه، دامنه موجک، تبدیل به تصویر و استفاده از روش‌های نهان‌نگاری تصاویر [۲۳]، تبدیل گسسته کسینوس [۲۷]، تبدیل فوریه [۱۷]، تحلیل مولفه پایه‌ای [۸، ۱۴]، بهره گرفته‌اند. مقایسه‌ای از روش‌های هر دو دسته را در مرجع [۸] می‌توانید مشاهده نمایید.

آنچه در این مقاله مورد توجه قرار گرفته است، نتایج کلی در خصوص روش‌هاست که با مطالعه روش‌های تاکنون مطرح شده، قابل جمع‌بندی است. به عنوان نمونه، روش‌های مبتنی بر دامنه تبدیل، در خصوص کیفیت بصری مدل پس از نهان‌نگاری، بر دسته دیگر برتری دارند [۲۸]. همچنین انتخاب مدل توری مثلثی به عنوان پایه مدل، کارآمد است؛ چرا که تبدیل هر مدلی به مدل توری مثلثی میسر و ممکن است [۹]. در خصوص مقاومت نیز می‌توان گفت:

- برای مقاومت در برابر حمله‌ای خاص، باید ویژگی‌ای از مدل را مدنظر داشت که در برابر آن حمله مقاوم باشد.
 - برای مقابله با حمله درهم‌سازی ترتیب رئوس، استفاده از نوع خاصی ترتیب می‌تواند مفید باشد.
 - با گنجانند تکراری پیام، مقاومت در برابر حمله برش را می‌توان انتظار داشت. همچنین بخش‌بندی مدل می‌تواند در این میان نقش مثبتی ایفاء نماید [۱۶].
 - با استفاده از تکرار هر بیت پیام با نرخ مشخصی، مقاومت در برابر اعوجاج حاصل می‌گردد.
- به طور خلاصه می‌توان گفت یک روش خوب نهان‌نگاری به این موارد پاسخ می‌دهد [۹]: (۱) گنجانند در کجا انجام شود تا مقاومت در برابر برخی حملات حاصل گردد؟ (۲) نهان‌نگاری چگونه نامحسوس و با بالاترین استحکام گنجانده شود؟ (۳) نحوه استخراج نهان‌نگاری چگونه است؟

ادامه مقاله، در قالب بخش‌های زیر ارائه شده است. در بخش ۲، کلیاتی در خصوص روش پیشنهادی مطرح می‌گردد. روش گنجانند داده‌ها در مدل و استخراج داده‌ها از مدل، موضوع مورد توجه در بخش‌های ۳ و ۴ می‌باشند. در بخش ۵، به پیاده‌سازی و آزمون روش پیشنهادی پرداخته شده است و در بخش پایانی، جمع‌بندی کار و زمینه کارهای آتی مطرح شده است.

۲- روش پیشنهادی

روش‌های نمایش گوناگونی برای مدل‌های سه بعدی ارائه شده است. در این نوشتار، تمرکز شیوه نمایش مدل بر روی فایل‌های زبان مدل-سازی واقعیت مجازی می‌باشد. برای کسب اطلاع بیشتر از این نوع فایل‌ها می‌توانید به مرجع [۳۲] مراجعه نمایید. در این شیوه نمایش، مدل توسط مجموعه‌ای از نقاط و سطوح ناشی از اتصال این نقاط به یکدیگر توصیف می‌شود. یعنی برای توصیف مثلث ABC باید

کلی همسایگی و مقداری می‌تواند صورت پذیرد. شیوه همسایگی غالباً در برابر تبدیلات هندسی مقاوم است. در شیوه مقداری، تفاوت مقداری از مدل مانند مساحت مدنظر قرار می‌گیرد. ضمناً یافتن جزء اولیه آغازین می‌تواند نقطه حساسی در بیان چیدمان مدل باشد؛ چرا که باید در برابر دستکاری‌ها کاملاً مقاوم باشد.

چیدمان اجزاء اولیه بر اساس همسایگی آن‌ها نیز در سه دسته عمومی، محلی و زیرنویسی قابل انجام است. همان‌طور که در شکل (۱) دیده می‌شود؛ در حالت عمومی، چیدمان بر تمامی اجزاء اعمال می‌شود. در حالت محلی، اجزاء به مجموعه‌های مجزا تقسیم شده و چیدمان بر هر زیرمجموعه انجام می‌گیرد. در حالت زیرنویسی، زیرمجموعه‌ها بسیار کوچک می‌شوند و شامل علامت زیرنویس و سمبل داده خواهند بود [۷].

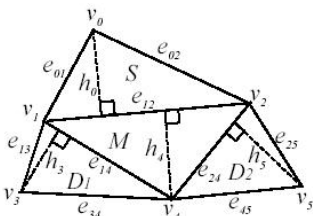


شکل (۱): سه دسته چیدمان اجزاء [۷]

هر یک از الگوریتم‌های مطرح شده، در برابر ترکیبی از حملات یا حمله خاصی با مشکل مواجه می‌شوند. در برخی نمی‌توان بدون پرداخت هزینه استخراج گفت که آیا مدل مورد نظر حاوی نهان‌نگاری هست یا خیر، یا به عبارت دیگر نمی‌توان سریعاً وجود نهان‌نگاری را رد کرد. برخی مدل‌های سه‌بعدی مانند گد نیز، به دلیل تولید محصول از روی مدل، هیچ تهملی در برابر کوچک‌ترین تغییرات در مدل خود را ندارند. همچنین افزودنی‌هایی در این نوع مدل وجود دارد که باید به آن‌ها توجه کرد [۲۱].

به طور خلاصه می‌توان گفت موارد زیر به عنوان برخی چالش‌ها قابل طرح هستند [۲۵]:

- گستردگی حملات و مقاومت در برابر آن‌ها
 - کاهش زمان محاسبات به ویژه در در مدل‌هایی با اجزای پایه زیاد مثلاً یک گیگا نقطه یا گره
 - نیاز یا عدم نیاز به مدل اصلی
 - دشواری مقایسه روش‌های نهان‌نگاری در مدل‌های سه‌بعدی توری به دلیل فقدان شیوه نمایش استاندارد، فقدان مجموعه داده سه‌بعدی استاندارد برای محک، فقدان مجموعه استاندارد حملات و فقدان ابزار سنجش موثر تخریب شکل
 - بهبود امنیت، قابلیت اطمینان، مقاومت و الگوریتم پیچیده‌تر برای گنجانند
 - تعیین شیوه نمایش مدل سه‌بعدی (گد، توری، هندسی و...)
 - تحمیل شرایط کاربرد دنیای واقعی بر الگوریتم‌های پیشنهادی
- در حالت کلی، روش‌های نهان‌نگاری مدل‌های سه بعدی در دو دسته قرار می‌گیرند؛ روش‌هایی که گنجانند خود را در دامنه فضایی صورت می‌دهند و مستقیماً روی اطلاعات موقعیت رئوس کار می‌کنند



شکل (۲): چهارتایی پایه گنجاندن در روش TSQ [۱۳]

در این مرحله، باید ویژگی‌ای در مدل را به‌عنوان مقصد نهان-نگاری معرفی کنیم که در برابر حملات، تغییرناپذیر باشد. در روش پیشنهادی در این مقاله، میانه مثلث به عنوان این ویژگی مطرح شده است. چرا که خاصیت میانه بودن در برابر انتقال مدل، چرخش، تغییر مقیاس و هر تغییری که نسبت بین دو ناحیه ناشی از رسم میانه را تغییر ندهد، معتبر خواهد بود. در هر مثلث، یکی از سه میانه مثلث بر اساس پیامی که قصد گنجاندن آن را داریم، انتخاب می‌شود. به واسطه انتخاب هر میانه نیز دو مثلث جدید متولد می‌شود که یکی از این دو مثلث، بر اساس پیام مورد نظر، انتخاب شده و به مجموعه سطوح مدل افزوده می‌گردد.

در قدم نخست فرض می‌کنیم هر مثلث ABC به نحوی است که ضلع مقابل راس A بیشترین طول و ضلع مقابل راس C کمترین طول را داشته باشد. این فرض ترتیب رئوس و اضلاع در کلیه شکل‌ها و به جهت امکان مقاومت در برابر چرخش مدنظر قرار گرفته است. به همین جهت، مثلث‌های متساوی‌الاضلاع و متساوی‌الساقین در فرآیند گنجاندن مدنظر قرار نمی‌گیرند.

در ادامه کار کمترین، بیشترین و میانگین مقدار مساحت مثلث‌ها محاسبه می‌شود که از این پس به ترتیب تحت مقادیر μ و M بیان می‌شوند. از میان مثلث‌ها، مثلث‌هایی را که مساحت آن‌ها در بازه (۲) باشد، جهت گنجاندن نهان‌نگاری انتخاب می‌کنیم:

$$\mu - \alpha \times (\mu - m) < Ar < \mu + \alpha \times (M - \mu) \quad (2)$$

که در این فرمول، $0 < \alpha < 1$ ضریبی به انتخاب کاربر است که توسط آن میزان تخریب در مدل کنترل خواهد شد. عبارت Ar ، بیانگر مساحت مثلث مورد بررسی است. (البته می‌توان حد بالای بازه را برابر M نیز قرارداد.)

مثلث‌های انتخاب شده را بر حسب مساحت که در فرمول (۳) آمده است [۳]، به صورت صعودی مرتب می‌کنیم. (در صورت مساوی بودن دو مساحت، به مقایسه اضلاع به ترتیب بزرگ‌ترین به کوچک-ترین می‌پردازیم و در صورت تساوی همه موارد، از افزودن مثلث مزبور به مجموعه مرتب شده مثلث‌ها صرفنظر می‌کنیم.)

$$Ar = \sqrt{S(S-a)(S-b)(S-c)} \quad (3)$$

$$S = \frac{1}{2}(a+b+c) \quad \text{که در آن}$$

و مقادیر a ، b و c طول اضلاع مثلث را نشان می‌دهند.

مختصات رئوس مثلث در بخش نقاط تعریف شده باشد و در بخش سطوح نیز ارتباط داشتن سه راس A ، B و C تصریح شده باشد. در این نوع فایل‌ها، مختصات نقاط و نحوه اتصال‌ها در قالب ساختار (۱) ارائه شده‌اند. در این ساختار، هر نقطه توسط مجموعه مختصات سه-مقداری (X_i, Y_i, Z_i) معرفی می‌شود. هر سطح (چندضلعی) نیز با دنباله‌ای از اندیس نقاط (V_i, V_j, V_k, \dots) مشخص می‌شود که با اندیس ۱- پایان آن مشخص می‌گردد. در این مقاله، سطوح مثلثی در فرآیند گنجاندن، مدنظر قرار گرفته‌اند.

```
IndexedFaceSet {
  coord Coordinate {
    point [
      X0 Y0 Z0,
      X1 Y1 Z1,
      ...
    ]
  }
  coordIndex [
    V_i, V_j, V_k, -1,
    ...
  ]
}
```

(۱) ساختار بیانگر مختصات نقاط و نحوه اتصال‌ها

در مرجع [۱۳] نیز این مدل‌ها مدنظر قرار گرفته‌اند. در مرجع مورد اشاره، پس از تعریف مفاهیم اولیه، روشی بنام TSQ مطرح شده است. در این روش، مجموعه مثلث‌های مشابه توسط دو زاویه مثلث یعنی $\{\theta_1, \theta_2\}$ و یا زوج مقادیر فاقد بُعد نسبت اضلاع-ارتفاع یعنی $\left\{\frac{b}{a}, \frac{h}{c}\right\}$ شناسایی می‌شوند که a ، b ، c و h به ترتیب سه ضلع مثلث و عمود بر ضلع سوم هستند. سپس مجموعه‌های چهارمثلثی‌ای مطابق شکل (۲) در مدل شناسایی می‌شوند؛ به نحوی که این هیچ چهارمثلثی با چهارمثلث دیگر لبه مشترک نداشته باشد. در این شکل، e بیانگر طول اضلاع است.

با تغییر جزئی زوج نسبت اضلاع-ارتفاع در مثلث M ، مقدار خاص مشخص‌کننده مجموعه‌های چهارمثلثی، نهان‌نگاری می‌شود. همین کار در خصوص مثلث S با مقدار زیرنویس (که ترتیب چهارمثلثی‌ها را مشخص می‌کند) و مثلث‌های D_1 و D_2 که مقادیر داده‌های نهان‌نگاری (که بخشی از رشته پیام نهان‌نگاری می‌باشند)، انجام می‌گیرد. نتیجه تغییر این زوج مقادیر، جابجایی اندکی در رئوس مثلث‌ها است.

در روش ارائه شده در مقاله حاضر، انتخاب مثلث‌ها بر اساس شرطی روی مساحت مثلث‌ها صورت می‌گیرد. این شرط به کمک ضریبی قابل تغییر توسط کاربر، شکل می‌یابد. هدف این شرط، کنترل میزان دستکاری قابل مشاهده در مدل به واسطه گنجاندن اطلاعات است. در مجموعه مثلث‌های انتخاب شده، ترتیب اجرای روش گنجاندن نیز مبتنی بر مساحت مثلث‌هاست.

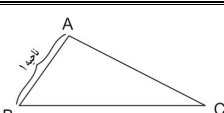
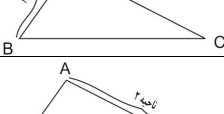
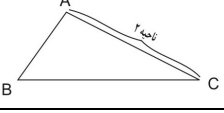
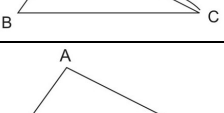
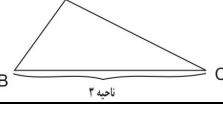
۴- روش استخراج داده‌ها از مدل

این روش، در مرحله استخراج نیازی به مدل اصلی ندارد. مراحل کار به ترتیب زیر خواهد بود:

- ۱) کلیه مثلث‌های مدل را دو بدو با یکدیگر مقایسه می‌کنیم. هدف این مقایسه یافتن دو مثلثی است که مساحت مثلث بزرگ‌تر تقریباً دو برابر مثلث کوچک‌تر باشد و دو مثلث در دو راس مشترک باشند و هرکدام یک راس غیرمشترک نیز داشته باشند.
- ۲) با یافتن چنین زوج مثلثی، بررسی می‌شود که آیا راس غیرمشترک یکی از دو مثلث می‌تواند میانه در مثلث دیگر باشد یا خیر. در صورتی که چنین حالتی بدست آمد، می‌توان گفت که دو مثلث بیانگر دوبیت نهان‌نگاری شده هستند.

برای هر مثلث سه ناحیه در نظر گرفته می‌شود که ناحیه ۱ بیانگر کوچک‌ترین ضلع مثلث و ناحیه ۳ برابر بزرگ‌ترین ضلع مثلث باشد. این که راس غیرمشترک در مثلث کوچک‌تر، میانه کدام ضلع مثلث بزرگ‌تر تشخیص داده می‌شود (که آن را ناحیه میانه می‌توان نامید) و این که کدام ضلع مثلث بزرگ‌تر در ساخت مثلث کوچک‌تر وارد شده است (که آن را ناحیه ضلع مشترک می‌توان نامید)، دوبیت نهان‌نگاری شده را بیان می‌کند. سپس دوبیت استخراج شده بر اساس جدول (۲)، به مثلث بزرگ‌تر انتساب داده می‌شود و دو مثلث مزبور از لیست مثلث‌های مورد بررسی خارج می‌شوند تا دیگر در مقایسه‌ای شرکت نکنند.

جدول (۲)، نحوه استخراج کد ذخیره شده بر اساس میانه و مثلث

شکل نواحی	ناحیه میانه	ناحیه ضلع مشترک	دوبیت کد
	۱	۲	"۰۰"
	۱	۳	"۰۱"
	۲	۱	"۱۰"
	۲	۳	"۱۱"
	۳	۱	شروع رشته

۳) پس از پایان کلیه مقایسه‌ها، مثلث‌هایی که از لیست مورد بررسی خارج شده‌اند و پیام‌های استخراج شده به آن‌ها منتسب شده‌اند؛ بر اساس مساحت، مرتب می‌شوند تا مجموعه گدهای دوبیتی استخراج شده، رشته پیام نهان‌نگاری شده را به صورت تکرار شده ارائه دهند. هر تکرار با "کد شروع" از تکرار بعدی قابل تفکیک خواهد بود.

۴) در پایان همان‌گونه که در فرمول‌های (۴) و (۵) آمده است، محاسبه نسبت تعداد بیت‌های صحیح استخراج شده به بیت‌های پیام اصلی و مقایسه نسبت شناسایی با یک حدآستانه می‌تواند در اثبات مالکیت موثر واقع شود. [۱۴، ۸، ۱۵] در این دو فرمول،

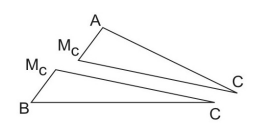
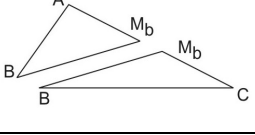

در خصوص پیامی که هدف، گنجاندن آن در مدل است، لازم است به این نکته توجه شود که یک کد دودویی هفتاد بیتی (یا ۱۰ کاراکتری) برای اثبات مالکیت و حفظ حق نشر کافی است [۲۴]. در این مقاله نیز یک پیام هفتاد بیتی به‌عنوان نهان‌نگاره در نظر گرفته شده است که با به‌کارگیری ۳۶ مثلث (یک مثلث جهت مشخص کردن شروع رشته و ۳۵ مثلث جهت گنجاندن ۷۰ بیت اطلاعات) می‌توان نهان‌نگاره را برای یک‌بار در مدل گنجاند. واضح است با توجه به تعداد مثلث‌های لیست مرتب شده، می‌توان گنجاندن را تکرار کرد.

۳- روش گنجاندن داده‌ها در مدل

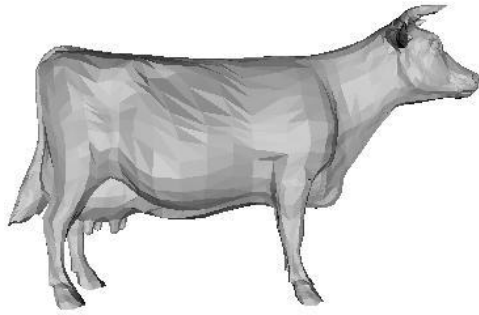
به ازای هر مثلث در لیست مرتب شده به شیوه زیر عمل می‌کنیم:

- ۱) مثلث مورد نظر (ABC) را به نحوی نامگذاری می‌کنیم که A، راس مقابل بزرگ‌ترین ضلع (a) و C، راس مقابل کوچک‌ترین ضلع (c) باشد.
- ۲) دوبیت بعدی از رشته نهان‌نگاره را جهت گنجاندن انتخاب می‌کنیم.
- ۳) برای مثلث ABC، سه میانه M_a ، M_b و M_c می‌توان در نظر گرفت. همچنین به ازای هر میانه دو مثلث جدید (مثلاً به ازای میانه M_a دو مثلث ABM_a و ACM_a) می‌توان تعریف کرد. در این مرحله بر اساس دوبیتی که قرار است در مثلث گنجاندن شود، میانه و مثلث مربوطه را مطابق جدول (۱) انتخاب می‌کنیم.

جدول (۱)، نحوه انتخاب راس و مثلث جهت افزودن به مدل

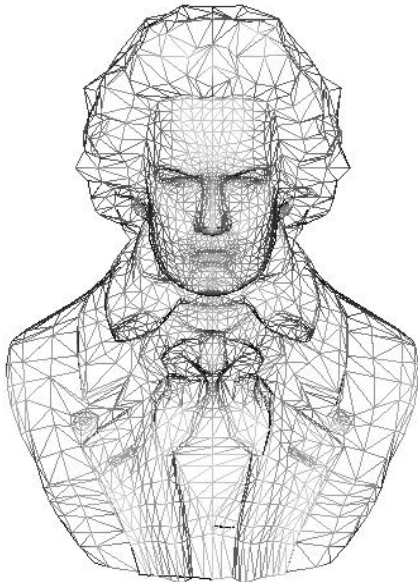
کد	راس	مثلث	شکل
"۰۰"	M_c	ACM_c	
"۰۱"	M_c	BCM_c	
"۱۰"	M_b	ABM_b	
"۱۱"	M_b	CBM_b	
شروع رشته	M_a	ABM_a	

در این جدول، ستون کد، بیانگر دو بیت رشته نهان‌نگاره است؛ ستون راس، بیانگر راسی است که به مدل افزوده می‌شود؛ ستون مثلث، بیانگر مثلثی است که باید به مدل افزوده شود و در ستون شکل نیز شکل مثلث‌ها برای فهم بهتر موضوع ارائه شده است. ترتیب این انتخاب‌ها بر اساس طول اضلاع مثلث از کوچک به بزرگ بوده است. یعنی ابتدا میانه متناظر با کوچک‌ترین ضلع مثلث مدنظر قرار گرفته است. در انتخاب دو مثلث ناشی از میانه انتخاب شده نیز مثلثی مقدم فرض شده است که از دو ضلع ممکن، ضلع کوچک‌تر در ساخت آن ظاهر شده است.



شکل (۴): مدل دوم قبل از نهان‌نگاری و حمله

از آن‌جا که میانه مثلث در برابر انتقال و تغییر مقیاس یکنواخت مقاوم است، انتظار می‌رود در برابر این دو حمله، استخراج بدون مشکل صورت گیرد. همچنین با توجه به این‌که ترتیب انتخاب میانه اضافه شده به هر مثلث بر اساس ترتیب بزرگی اضلاع آن مثلث صورت گرفته است و ترتیب طول اضلاع نیز در برابر چرخش مقاوم است، توقع است، روش در برابر حمله چرخش نیز مقاوم باشد. در مجموع، مقاومت روش در برابر حمله مشابهت مورد انتظار است.



شکل (۵): نمای مثلثی مدل نخست قبل از نهان‌نگاری و حمله

برای آزمون این موارد، مدل نهان‌نگاری شده تحت حملات انتقال، تغییر مقیاس یکنواخت، چرخش و ترکیب این سه حمله قرار گرفته است. فرمول کلی این تبدیلات در مرجع [۳] ارائه شده است. هفت حالت برای حمله چرخش، چهار حالت برای حمله تغییر مقیاس، پنج حالت برای حمله انتقال در نظر گرفته می‌شود. چرخش در درجه‌های ۵، ۱۰، ۳۰، ۴۵، ۶۰، ۹۰ و ۱۸۰ درجه صورت داده شده است که دامنه وسیعی از این حمله را پوشش می‌دهد. تغییر مقیاس با فاکتورهای ۰/۲۵، ۰/۵، ۱/۵ و ۲ صورت گرفته است که اثر کوچک-نمایی و بزرگ‌نمایی مدل حتی با نسبت اعشاری نیز مدنظر قرار گیرد. بردارهای انتقال نیز مطابق بردارهای $T1=(0.03,-0.04,0.08)$ ، $T2=(1.6,2.8,-3.2)$ ، $T3=(-1.8,-3.1,4.0)$ ، $T4=(3.0,-4.0,2.6)$ و $T5=(5.0,2.0,-8.0)$ انتخاب شده‌اند؛ به نحوی که انتقال در حالت

$d(\theta)$ بیانگر رشته استخراج شده، $w(\theta)$ همان رشته پیام اصلی (گنجانده شده)، فرمول (۴) بیانگر مقدار شناسایی غلط و فرمول (۵) بیانگر مقدار نسبت شناسایی است.

$$e_w(\theta) = \begin{cases} 1 & \text{if } (w(\theta) \neq d(\theta)) \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

$$D_w = 1 - \frac{\text{card}\{e_w(\theta)\}}{\text{card}\{w(\theta)\}} \quad (5)$$

۵- پیاده‌سازی و آزمایش روش

آزمون بر روی دو مدل معروف در زبان مدل‌سازی واقعیت مجازی انجام شده است. مدل نخست، مدل Beethoven با تعداد ۲۵۲۱ راس و ۵۰۲۸ سطح (مثلث) و مدل دوم، مدل Cow با تعداد ۲۹۰۳ راس و ۵۸۰۴ مثلث، انتخاب شده‌اند که به ترتیب در شکل (۳-الف) و شکل (۴) ارائه شده‌اند. همچنین در شکل (۵)، نمای سطوح مثلثی مدل نخست قبل از نهان‌نگاری ارائه شده است. پیاده‌سازی در محیط ویژوال سی ++ نسخه ۶ انجام گرفته است و در پیمایش مدل‌های مزبور از کتابخانه مربوطه [۳۰] استفاده شده است. همچنین برای نمایش مدل‌ها، از یکی از مرورگرهای خاص این مدل‌ها [۳۱] استفاده شده است.



شکل (۳-الف): مدل نخست قبل از نهان‌نگاری
شکل (۳-ب): مدل نخست بعد از نهان‌نگاری

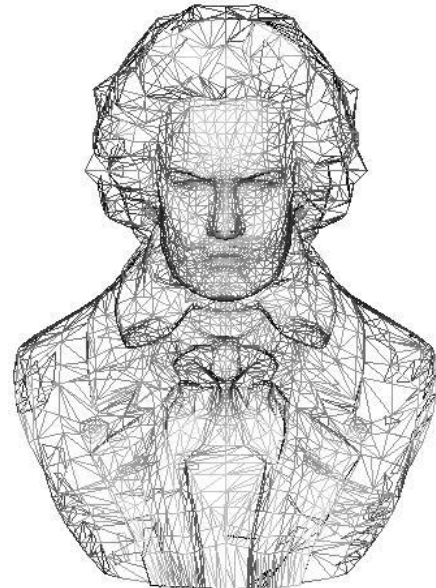
در مرحله گنجاندن، مدل نخست با ضریب ۰/۳ و مدل بعدی با ضریب ۰/۴ مورد توجه قرار گرفته‌اند. در شکل (۳-ب)، مدل نخست پس از گنجاندن و در شکل (۶)، نمای مثلثی مدل نخست پس از گنجاندن ارائه شده است. تقسیم برخی مثلث‌ها بر اساس افزودن یکی از میانه‌هایشان باعث شده است تا تعداد مثلث‌ها به ۶۶۲۱ مثلث افزایش یابد که این موضوع نشان می‌دهد ۱۵۹۳ مثلث به مدل اضافه شده است. با توجه به این‌که به کمک هر مثلث، دوبیت اطلاع نهان-نگاری شده است و یک مثلث جهت مشخص کردن شروع هر تکرار نیاز است؛ می‌توان نتیجه گرفت با هر ۳۶ مثلث، یک بار تکرار نهان-نگاری صورت گرفته است و این بدین معنی است که حداقل ۴۴ بار رشته پیام در مدل مزبور نهان‌نگاری شده است. به همین ترتیب، در مدل دیگر نیز بیش از ۷۶ بار، رشته پیام در مدل گنجانده شده است.

کوچک و بزرگ نسبت به دامنه تغییرات مختصات رئوس مدل‌ها، صورت گیرد. پس از اعمال حمله‌های منفرد، ترکیب حمله مشابهت یا RST اعمال شده است. برای این حمله نیز شش حالت ترکیب چرخش ۴۵ درجه، تغییر مقیاس ۰/۵ و ۲ و انتقال تحت T1، T4 و T5 را در نظر گرفته شده است. دو شکل (۷) و (۸)، دو مدل را بعد از اعمال حالت ششم ترکیب، نمایش می‌دهند.

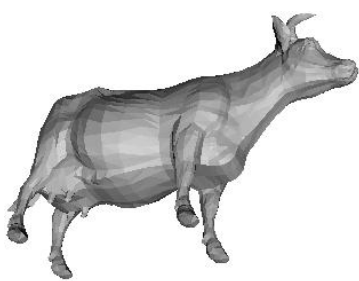
سپس روش استخراج روی مدل‌های مورد حمله واقع شده، اعمال شد. نتیجه این اعمال، بازیابی کلیه تکرارهای کل رشته پیام گنجانده شده را بیان نمود. اگرچه در بازیابی مشخص گردید که در مواردی، ترتیب بیت‌های استخراج شده مطابق انتظار نبوده است. این امر به دلیل خطای محاسبات ممیزشناور ناشی از اعمال تبدیلات فوق و وابستگی مساحت مثلث به عنوان عامل ترتیب‌دهی بروز نموده است و موجب شده است که با وجود بازیابی کلیه بیت‌های گنجانده شده، نسبت شناسایی در برخی تکرارها برابر "۱" نگردد. در جدول (۳)، نتایج استخراج پس از حمله ترکیبی مشابهت ارایه شده است.

انتخاب ضریب در انتخاب مثلث‌ها، قابلیت بهبود یافتن و خودکار شدن را داراست. همچنین می‌توان شرط انتخاب مثلث‌ها را (که اکنون برحسب مساحت است)، نیز بهبود داد. به‌علاوه، با توجه به وجود تکرار در مدل، می‌توان انتظار داشت با تغییراتی در پیاده‌سازی و بررسی رشته استخراج شده با طول‌های متفاوت در تکرارهای گوناگون، مدل در برابر حمله برش نیز مقاوم باشد. از آن‌جا که نسبت طول اضلاع در حمله کشیدن و در نتیجه در تبدیل خطی انتقال‌یافته تغییر می‌کند، در برابر این حمله نیز می‌توان توقع داشت که روش مقاوم نباشد و نیاز به بهبودی در این حالت را می‌توان برای روش مطرح کرد. بررسی دقیق‌تر، پیاده‌سازی و آزمون مواردی از این دست، به عنوان قدم‌های بعدی قابل توجه خواهد بود.

شکل (۷): مدل نخست بعد از نهان‌نگاری و حمله



شکل (۶): نمای مثلثی مدل نخست بعد از نهان‌نگاری



شکل (۸): مدل دوم بعد از نهان‌نگاری و حمله

شکل (۷): مدل نخست بعد از نهان‌نگاری و حمله

جدول (۳)، نتایج استخراج پس از حمله ترکیبی مشابهت (تحت درجه چرخش ۴۵ درجه)

فاکتور تغییر مقیاس						مدل	بردار انتقال
۲	۲	۲	۰/۵	۰/۵	۰/۵		
T ₅	T ₄	T ₁	T ₅	T ₄	T ₁	نسبت شناسایی	۱
۰/۹۷۴	۰/۹۶۹	۰/۹۶۹	۰/۹۶۳	۰/۹۶۶	۰/۹۶۸	نسبت شناسایی	۲
۰/۷۹۴	۰/۹۱۶	۰/۹۰۳	۰/۷۴۴	۰/۷۴۸	۰/۷۳۳		

۶- جمع‌بندی و کارهای آتی

در این مقاله، روشی جهت نهان‌نگاری مدل‌های سه‌بعدی مثلثی مبتنی بر افزودن مثلثی حاوی میانه مثلث‌ها ارایه شد. در مقایسه با روش‌های دیگر، ایده این مقاله، به‌کارگیری میانه به عنوان یک ویژگی مقاوم، در کنار سایر ویژگی‌های تاکنون معرفی شده، در برابر برخی حملات بوده است. انتخاب مثلث‌ها جهت گنجاندن یک رشته پیام، مبتنی بر مساحت آن‌ها و ضریبی انتخاب شده توسط کاربر فرض شد. دو بیت پیام در هر مثلث انتخاب شده، در انتخاب یک میانه از سه میانه مثلث مزبور و انتخاب یک مثلث از دو مثلث ناشی از آن میانه، نقش ایفاء نمود تا بدین صورت، مثلث افزوده شده به مدل، دوبیت مزبور را نمایندگی کند. در ترتیب گنجاندن اطلاعات پیام نیز مجدداً

سیاسگزاری

نویسندگان مقاله از مرکز تحقیقات مخابرات ایران به جهت پشتیبانی مالی این پژوهش کمال سیاسگزاری را دارند.

مراجع

- [۱] فرید، رضا، بررسی اجمالی تخریب در نهان‌نگاری داده در تصویر و چند روش مقابله با آن، گزارش درس سمینار، دانشگاه تربیت مدرس، تهران، ۸۷ صفحه، اسفند ۸۳.
- [2] Cox, Ingemar J., Miller, M. L., Bloom, J. A., "Digital Watermarking", Morgan Kaufman Publishers, 2002.
- [3] Vince, John, "Geometry for Computer Graphics, Formulae, Examples & Proofs", Springer, 2005.
- [4] Wu, Min, "Multimedia Data Hiding", a dissertation presented to the faculty of Princeton University in candidacy for the degree of doctor of philosophy, Chapter 9, pp. 190-223, June 2001.
- [5] Voloshynovskiy, S., Pereira, Sh., Pun, Th., Eggers J. J., K. Su, Jonathan, "Attacks on Digital Watermarks: Classification, Estimation-based Attacks, and Benchmarks", IEEE Comm. Magazine, August 2001.
- [6] Kim, Bum-Soo, Choi, Jae-Gark, Park, Chul-Hyun, Won, Jong-Un, Kwak, Dong-Min, Oh, Sang-Keun, Koh, Chang-Rim, Park, Kil-Houm, "Robust digital image watermarking method against geometrical attacks", Real-Time Imaging 9 (2003) 139-149 (Elsevier).
- [7] Ohbuchi, R., Masuda, H., Aono, M., "Geometrical and Non-geometrical Targets for Data Embedding in Three-Dimensional Polygonal Models", Computer Comm., Vol. 21, pp. 1344-1354, Elsevier (1998).
- [8] Zafeiriou, S., Tefas, A., Pitas, I., "Blind Robust Watermarking Schemes for Copyright Protection of 3D Mesh Objects", IEEE Transactions on Visualization and Computer Graphics, Vol.11 No.5, p.596-607, Sep. 2005.
- [9] Zhiqiang Yu, Horace H.S. Ip, L.F. Kwok, "A robust watermarking scheme for 3D triangular mesh models", Pattern Recognition, Vol.36, Issue.11, (2003) 2603-2614 (Elsevier).
- [10] Nikolaidis, A., Tsekeridou, S., Tefas A., Solachidis, V., "A survey on watermarking application scenarios and related attacks", IEEE International Conf. on Image Processing (ICIP 2001), Greece, 7-10 October 2001.
- [11] Meerwald, Peter, Pereira, Shelby, "Attacks, applications and evaluation of known watermarking algorithms with Checkmark", SPIE Symposium, Electronic Imaging, Conference on Security and Watermarking of Multimedia Contents IV Proceedings of SPIE, Volume 4675, San Jose, CA, USA, January 21 - 24, 2002.
- [12] Kutter, M., Bhattacharjee, S. K., Ebrahimi, T., "Towards Second Generation Watermarking Schemes", in IEEE-ICIP'99, p320-323, vol. 1, 1999, Kobe (Japan).
- [13] Ohbuchi, R., Masuda, H., Aono, M., "Watermarking three-dimensional polygonal models", Proc. of the ACM Multimedia'97 Seattle, Washington, USA, Addison-Wesley Publishing, Reading, WA, pp.261-272.
- [14] Kalivas, A., Tefas, A. and Pitas, I., "Watermarking of 3D Models Using Principal Component Analysis", Proc. IEEE Int'l Conf. Acoustics, Speech, and Signal Processing, vol. 5, pp. 676-679, In ICME, 2003.
- [15] Tefas, A., Louizis, G., Pitas, I., Nikolaidis, N., Lyroutdia, K., "Robust spatial 3D image watermarking", Proc. of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2001), pp. 229-232.
- [16] Cotting, Daniel, Weyrich, Tim, Pauly, Mark, Gross, Markus, "Robust Watermarking of Point-Sampled Geometry", International Conference on Shape Modeling and Applications 2004 (SMI'04) pp. 233-242.
- [17] Solachidis, Vassilios, Pitas, I., "Watermarking digital 3D volumes in the Discrete Fourier Transform domain", IEEE International Conference on Multimedia & Expo (ICME 2005), Amsterdam, The Netherlands, July 2005.
- [18] Harte, T., Bors, A.G., "Watermarking 3D Models", Proc. IEEE Intern. Conf. on Image Processing, Rochester, NY, USA, 22-25 Sep. 2002, vol. III, pp. 661-664.
- [19] Wolthusen, Stephen, "On the Limitations of Digital Watermarks: A Cautionary Note", Proc. of the 4th International Conference of Information Systems Analysis and Synthesis, International Institute of Informatics and Systemics, 1998.
- [20] Petitcolas, Fabien A. P., Anderson, Ross J., "Evaluation of copyright marking systems", Proceedings of IEEE Multimedia Systems'99, vol. 1, pp. 574-579, Italy.
- [21] Ohbuchi, R., Masuda, H., Aono, M., "A Shape-Preserving Data Embedding Algorithm for NURBS Curves and Surfaces", Proc. of the Computer Graphics International (CGI) 1999, Canmore, Canada, June 7-11.
- [22] Ohbuchi, R., Mukaiyama, A., Takahashi, Sh., "Watermarking a 3D shape defined as a point set", Proceedings of the 2004 International Conference on Cyberworlds, pp. 392-399, Tokyo, Japan, 2004.
- [23] Song, Han Sae; Cho, Nam Ik, "Digital watermarking of 3D geometry", Proceedings of International Intelligent Symposium on Signal Processing and Communication Systems, 2004. ISPACS 2004, Page(s):272 - 277.
- [24] Ashourian, M., Enteshari, R., Jeon, J., "Digital Watermarking of Three-dimensional Polygonal Models in the Spherical Coordinate System", Proc. of the IEEE Computer Graphics International (CGI'04), 2004.
- [25] Ohbuchi, R., Mukaiyama, A., Takahashi, Sh., "A Frequency-Domain Approach to Watermarking 3D Shapes", Proc. EUROGRAPHICS 2002, Saarbrücken, Germany in September 2-6, 2002 (also as Computer Graphics Forum 21(3), pp. 373-382, 2002.
- [26] Lee, Hae-Yeoun, Kim, Jong-Tae, Lee, Heung-Kyu, Suh, Young-Ho, "Content-Based Synchronization Using the Local Invariant Feature for Robust Watermarking", WISA 2004, LNCS 3325, pp. 122-134, Springer-Verlag.
- [27] Jeon, Jeonghee; Lee, Sang-Kwang; Ho, Yo-Sung, "A Three-Dimensional Watermarking Algorithm Using the DCT Transform of Triangle Strips", IWDW 2003; LNCS 2939; pp.508-517; 2004; Springer-Verlag.
- [28] Kim, Min-Su; Valette S'ebastien; Jung Ho-Youl; Prost, R'emy, "Watermarking of 3D Irregular Meshes Based on Wavelet Multiresolution Analysis", IWDW 2005, LNCS 3710, pp. 313-324, 2005. Springer-Verlag.
- [29] Delp, Edward J., "An Introduction to Image and Video Watermarking", Purdue University, June 11, 1999
- [30] The VR 2.2 Software Developer's Kit, <http://www.cs.technion.ac.il/~cs234325>, July 1999
- [31] Virtue3D Optimizer Version 2.1, <http://www.virtue3d.com>.
- [32] ISO/IEC 14772-1 Virtual Reality Model Language (VRML), 180, 1997. (The Virtual Reality Modeling Language Specification, Version 2.0, ISO/IEC WD 14772, August 4, 1996, <http://www.graphcomp.com/info/specs/sgi/vrml/spec/>)