

Objects', IEEE Transactions on Visualization and Computer Graphics, Vol. 11, No.5, pp. 596-607, September/October (2005).

[28] Yu Zhi-qiang, Horace H.S. Ip, and L.F. Kwok, 'Robust watermarking of 3D polygonal models based on vertex scrambling', Proc. IEEE Computer Graphics International (CGI'03) Tokyo, Japan, IEEE Computer Society, July, 2003, pp.254-257.

[۲۹] رضا فرید، 'ارایه راهکاری جهت ارتقاء مقاومت در نهان نگاری مدل های سه بعدی'، کارشناسی ارشد، فنی و مهندسی، دانشگاه تربیت مدرس، ۱۳۸۵.
[۳۰] رضا فرید و نصرا... مقدم چرکری، 'روشی مقاوم در نهان نگاری مدل های سه بعدی مثلثی مبتنی بر میانه'، دوازدهمین کنفرانس بین المللی انجمن کامپیوتر ایران، دانشگاه شهید بهشتی، تهران، ایران، دانشگاه شهید بهشتی، ۱-۳ اسفند، ۱۳۸۵، pp.265-272.

رضا فرید با رتبه نخست در مقطع کارشناسی کامپیوتر، گرایش نرم افزار از دانشگاه شهید بهشتی تهران (در شهریور ۱۳۷۹) فارغ التحصیل شد و کارشناسی ارشد خود را در همان رشته و گرایش در دانشگاه تربیت مدرس (در دی ۱۳۸۵) به اتمام رساند. وی از مهر ۱۳۸۶، همکاری خود را با آزمایشگاه سیستم های خودکار هوشمند، دانشکده مهندسی، دانشگاه نیوساوت ولز (UNSW) استرالیا آغاز نموده و اکنون نیز به عنوان دانشجوی دکترا در همان دانشکده مشغول به تحصیل می باشد. زمینه های تحقیقاتی وی شامل بینایی ماشین، شناسایی اشیاء، مدل های سه بعدی، هوش مصنوعی، نهان نگاری اطلاعات، سیستم های پویا و بهینه سازی الگوریتم می باشد.



نصرااله مقدم کارشناسی خود را از دانشگاه شهید بهشتی (۱۳۶۴) و سپس کارشناسی ارشد (۱۳۷۱) و دکتری (۱۳۷۴) خود را از دانشگاه یاماناشی ژاپن در رشته مهندسی کامپیوتر اخذ نمود. او از سال ۱۳۷۵ به عنوان عضو هیئت علمی گروه کامپیوتر در دانشگاه تربیت مدرس به فعالیت پرداخت. عمده تحقیقات او در حوزه پردازش و بازیابی تصاویر، نهان نگاری اطلاعات در حوزه تصویر و ویدئو و مباحث یادگیری و بهینه سازی در شبکه های سنسوری است.



: چرخش، ۲: انتقال، ۳: تغییرمقیاس، ۴: تبدیل مشابهت، ۵: تبدیل خطی انتقال یافته
۶: دسته حمله برش و ۷: ساده سازی توری

سپاسگزاری

در اینجا لازم است از مرکز تحقیقات مخابرات ایران به جهت پشتیبانی مالی این پژوهش (به شماره شناسایی TMU85-10-76) تشکر گردد.

مراجع

- [15] A. Nikolaidis, S. Tsekeridou, Tefas A., and V. Solachidis, 'A survey on watermarking application scenarios and related attacks', IEEE Inter. Conf. on Image Processing (ICIP 2001), Thessaloniki, Greece, 7-10 October, 2001, pp.
- [16] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, 'Watermarking three-dimensional polygonal models', Proceedings of the fifth ACM international conference on Multimedia, Seattle, Washington, United States, ACM Press, Addison-Wesley Publishing, November, 1997, pp. 261-272.
- [17] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, 'Data embedding algorithms for geometrical and non-geometrical targets in three-dimensional polygonal models', Computer Communications (Elsevier), Vol. 21, No.15, pp. 1344-1354, (1998).
- [18] Ryutarou Ohbuchi, Akio Mukaiyama, and Shigeo Takahashi, 'A Frequency-Domain Approach to Watermarking 3D Shapes', Computer Graphics Forum, Vol. 21, No.3, pp. 373-382, (2002).
- [19] Ryutarou Ohbuchi, Akio Mukaiyama, and Shigeo Takahashi, 'Watermarking a 3D shape model defined as a point set', IEEE International Conference on Cyberworlds, IEEE press, Nov. 18-20, 2004, pp.
- [20] Ryutarou Ohbuchi, Shigeo Takahashi, Takahiko Miyazawa, and Akio Mukaiyama, 'Watermarking 3D Polygonal Meshes in the Mesh Spectral Domain', Graphics Interface, Ottawa, Canada, June, 2001, pp.
- [21] Emil Praun, Hugues Hoppe, and Adam Finkelstein, 'Robust Mesh Watermarking', Proceedings of the 26th annual conference on Computer graphics and interactive techniques, ACM Press/Addison-Wesley Publishing Co., 1999, pp. 49-56.
- [22] Vassilios Solachidis, and Ioannis Pitas, 'Watermarking digital 3D volumes in the Discrete Fourier Transform domain', IEEE International Conference on Multimedia & Expo (ICME 2005), Amsterdam, The Netherlands, July, 2005 pp.
- [23] The Virtual Reality Modeling Language (VRML) Specification, Version 2.0, ISO/IEC WD 14772, August 4, 1996, <http://www.graphcomp.com/info/specs/sgl/vrml/spec/>
- [24] S. Voloshynovskiy, Sh. Pereira, Th. Pun, Eggers J. J., K. Su, and Jonathan, 'Attacks on Digital Watermarks: Classification, Estimation-based Attacks, and Benchmarks', IEEE Comm. Magazine, August 2001 (2001).
- [25] Min Wu, and Bede Liu, 'Attacks and Countermeasures on Known Data Hiding Algorithms', Chapter 9: Multimedia Data Hiding, pp. 151-178, Springer, 2003.
- [26] Zhiqiang Yu, Horace H.S. Ip, and L.F. Kwok, 'A robust watermarking scheme for 3D triangular mesh models', Pattern Recognition (Pergamon), Vol. 36, No.11, pp. 2603-2614, (2003).
- [27] Stefanos Zafeiriou, Anastasios Tefas, and Ioannis Pitas, 'Blind Robust Watermarking Schemes for Copyright Protection of 3D Mesh
- [1] Edward Angel, 'Computer Graphics', Addison-Wesley, 1990.
- [2] Mohsen Ashourian, Reza Enteshari, and Jeonghee Jeon, 'Digital watermarking of three-dimensional polygonal models in the spherical coordinate system', Proc. IEEE Computer Graphics International (CGI'04), IEEE Computer Society, 2004, pp.590-593.
- [3] Oliver Benedens, 'Geometry-Based Watermarking of 3D Models', IEEE Computer Graphics and Applications, Vol. 19, No.1, pp. 46-55, January/February (1999).
- [4] Oliver Benedens, and Christoph Busch, 'Towards Blind Detection of Robust Watermarks in Polygonal Models', Computer Graphics Forum, Vol. 19, No.3, pp. 199-208, (2000).
- [5] F. Cayre, and B. Macq, 'Data hiding on 3-D triangle meshes', IEEE Transactions on Signal Processing, Vol. 51, No.4, pp. 939-949, April (2003).
- [6] Daniel Cotting, Tim Weyrich, Mark Pauly, and Markus Gross, 'Robust watermarking of point-sampled geometry', International Conference on Shape Modeling and Applications, Genova, Italy, IEEE Computer Society, June 7-9, 2004, pp.233-242.
- [7] Ingemar J. Cox, M. L. Miller, and J. A. Bloom, 'Digital Watermarking', Morgan Kaufman Publishers, 2002.
- [8] Thomas Harte, and Adrian G. Bors, 'Watermarking 3D models', Proc. IEEE International Conf. on Image Processing, Rochester, NY, USA, 3, Sep. 22-25, 2002, pp.661-664.
- [9] Jeonghee Jeon, Sang-Kwang Lee, and Yo-Sung Ho, 'A Three-Dimensional Watermarking Algorithm Using the DCT Transform of Triangle Strips', IWDW 2003, Springer-Verlag Berlin Heidelberg, 2004, pp.508-517.
- [10] JIN Jian-qiu, DAI Min-ya, BAO Hu-jun, and PENG Qun-sheng, 'Watermarking on 3D mesh based on spherical wavelet transform', Journal of Zhejiang University Science, Vol. 5, No.3, pp. 251-258, (2004).
- [11] A. Kalivas, A. Tefas, and I. Pitas, 'Watermarking of 3D models using principal component analysis', Proc. IEEE International Conf. Acoustics, Speech, and Signal Processing, 5, April, 2003, pp.676-679.
- [12] Min-Su Kim, Sébastien Valette, Ho-Youl Jung, and Rémy Prost, 'Watermarking of 3D Irregular Meshes Based on Wavelet Multiresolution Analysis', 4th International Workshop Digital Watermarking, LNCS 3710/2005, M. Barni et al. (Ed.), Siena, Italy, pp. 313-324, Springer Berlin / Heidelberg, 2005.
- [13] Suk-Hwan Lee, Tae-Su Kim, Seung-Jin Kim, Young Huh, Ki-Ryong Kwon, and Kuhn-Il Lee, '3D mesh watermarking using projection onto convex sets', Proc. International Conference on Imaging Science, Systems and Technology (CISST '04), Las Vegas, Nevada, USA, Vol. 3, CSREA Press, June 21-24, 2004, pp.1577-1580.
- [14] Li Li, David Zhangb, Zhigeng Pan, Jiaoying Shi, Kun Zhou, and Kai Ye, 'Watermarking 3D mesh by spherical parameterization', Computers & Graphics (Elsevier), Vol. 28, No.6, pp. 981-989, (2004).



حمله چرخش، انتقال، تغییرمقیاس یک‌نواخت، ترکیب سه حمله قبل یا تبدیل مشابهت، تبدیل خطی انتقال‌یافته، دسته حمله برش و ساده‌سازی توری مدنظر قرار گرفته است. در ستون ظرفیت، مشخص شده است که به ازای هر مثلث چند بابت قابلیت گنجاندن دارد و یا کلاً چند بیت در مدل‌ها گنجانده می‌شود. در ستون نهایی نیز نسبت شناسایی هر روش در صورت وجود بیان شده است. مواردی که در روش مربوطه اشاره نشده‌اند با علامت پرسش (?) مشخص شده‌اند.

انتخاب ترتیب اندیس رؤس به عنوان عامل مرتب‌سازی عناصر موجب شده است که روش در برابر حملاتی که ترتیب رؤس را تغییر می‌دهند، مقاومت کامل نداشته باشد و در برابر سایر حملات جز ساده‌سازی توری و دست‌کاری‌های اتصالات، مقاومت از خود نشان دهد. بهبود آرایه شده روی روش نیز در واقع نکته‌ای کلیدی است. اندیس رؤس در برابر بسیاری از حملات اثرپذیری ندارد و لذا کاندیدای مناسبی برای برخی ویژگی‌های محاسباتی می‌تواند باشد.

از جمله کارهای آتی می‌توان به بررسی آرایه راهکار مناسب جهت تعیین هوشمند مثلث‌ها با حفظ شفافیت مدل و بدون نیاز به نظارت کاربر اشاره نمود. همچنین با انتخاب خودکار بازه‌ای در انتخاب مثلث‌های مرتب شده بر حسب مساحت، می‌توان مقاومت روش نخست را بهبود داد. از آن‌جا که در هر دو روش، گنجاندن به صورت تکراری صورت می‌پذیرد، انتظار مقاومت در برابر حمله برش را می‌توان داشت که بررسی اثر این حمله و نحوه مواجهه با آن نیز می‌تواند به عنوان فعالیت بعدی مطرح باشد.

رشته نهان‌نگاری به منظور گنجاندن در بازه‌ای از مثلث‌های انتخابی گنجانده می‌شود. توزیع رشته نهان‌نگاری روی مجموعه انتخاب شده، شیوه‌ای است که بسیاری از روش‌ها از آن استفاده کرده‌اند. در این روش نیز، در هر

عنصر پایه روش، دو بیت گنجانده می‌شود. در واقع به کمک دوبیت از رشته نهان‌نگاری مشخص می‌شود کدام میانه مثلث و کدام مثلث ناشی از رسم آن میانه باید به مدل افزوده گردد. در بسیاری از روش‌ها، روش استخراج به نوعی معکوس روش گنجاندن بنا می‌شود. روش آرایه شده نیز دو جدول (۲) و (۳) را به منظور گنجاندن و استخراج مطرح کرده است.

حمله مشابهت و حمله تبدیل خطی انتقال‌یافته، دو مجموعه حمله بسیار محتمل هستند. روش اولیه، مبتنی بر میانه و مساحت مثلث‌ها، در برابر حمله نخست و روش بهبودیافته در این مقاله، مبتنی بر میانه و اندیس رؤس، در برابر هر دو حمله مقاوم است. روش بهبود یافته اگرچه در مرحله استخراج زمان بیشتری را می‌طلبد، با این وجود، مقاومت آن در برابر ترکیب حملات چرخش، تغییرمقیاس، انتقال و کشیدن، یا همان مجموعه حمله خطی انتقال‌یافته، مناسب است. از جمله مشخصه هر دو روش آن است که در مرحله استخراج به مدل اصلی نیازی ندارند. مطابق جدول ۵ مقایسه‌ای روش‌ها و حملات مورد پوشش مشخص است که روش در این خصوص بر کدام روش‌ها برتری دارد. ستون نوع به دو دسته کور و آگاه اشاره می‌کند. در ستون‌های مشخص شده با شماره ۱ الی ۷ به ترتیب مقاومت در برابر

جدول ۵. مقایسه روش پیشنهادی و چند روش تاکنون آرایه شده

ردیف	نام روش و مراجع	سال	نوع	حوزه	۱	۲	۳	۴	۵	۶	۷	ظرفیت	نسبت شناسایی
۱	TSQ [16]	۱۹۹۷	کور	فضایی	۱	۲	۳	۴	-	۶	-	۰/۱۸ هر مثلث	؟
۲	TVR [16]	۱۹۹۷	کور	فضایی	۱	۲	۳	۴	۵	-	-	۰/۲۰ هر مثلث	؟
۳	جابجایی نسبت به مرکزمدل [۲۶]	۲۰۰۳	آگاه	فضایی	۱	۲	-	-	-	۶	۷	۵۰ بیت	۰/۵ تا ۱
۴	تغییر فاصله نسبت به مرکز جسم [۲۸]	۲۰۰۳	آگاه	فضایی	۱	۲	۳	۴	-	۶	۷	۵۰ بیت	۰/۵ تا ۱
۵	پارامتری کردن کروی، موجک [۱۰]	۲۰۰۴	آگاه	فرکانس	-	-	-	-	-	-	۷	؟	۰/۸ تا ۰/۹
۶	POA [27]	۲۰۰۵	کور	فرکانس	۱	۲	۳	۴	-	-	-	؟	۰/۹
۷	روش پیشنهادی	۲۰۰۷	کور	فضایی	۱	۲	۳	۴	۵	۶	-	۷۰ بیت پیام، ۰/۲۵ به ازای هر مثلث	۱

دقت شناسایی را بدست آورد. در این دو رابطه، $d(\theta)$ بیانگر رشته استخراج شده، $w(\theta)$ رشته پیام اصلی گنجانده شده است. مقایسه نسبت شناسایی با یک حد آستانه مورد قبول می تواند در اثبات

$$e_w(\theta) = \begin{cases} 1 & \text{if } (w(\theta) \neq d(\theta)) \\ 0 & \text{otherwise} \end{cases} \quad \text{رابطه (۲)}$$

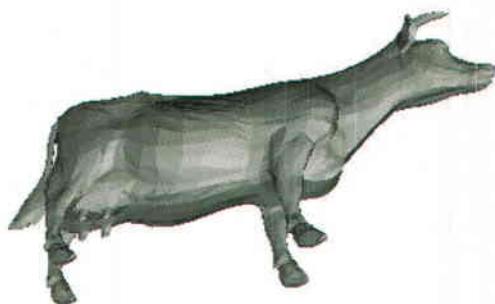
$$D_w = 1 - \frac{\text{card} \{e_w(\theta)\}}{\text{card} \{w(\theta)\}} \quad \text{رابطه (۳)}$$

مالکیت بکار برده شود [۲۷؛ ۱۱]

در تمام حملات، ۴۵ درجه حول بردار معین $(0/10, -0/6, -0/8)$ ، فاکتور تغییرمقیاس برای سه حمله اول برابر $0/5$ و مابقی برابر 2 ، دو زاویه کشیدن در روش دوم برای تمام حملات 75 و 60 درجه و برای انتقال در حمله های 1 و 4 بردار $T1=(0.03, -0.04, 0.08)$ ، برای حمله های شماره 2 و 5 بردار $T2=(3.0, -4.0, 2.6)$ و برای حمله های شماره 3 و 6 بردار $T3=(5.0, 2.0, -8.0)$ تعریف شده است.

۴-۱- ارزیابی روش

در پایان استخراج، باید شیوه ای برای تعیین میزان مقاومت روش و توانایی شناسایی آن ارائه داد. همانگونه که در رابطه های (۲) و (۳) آمده است، با مقایسه بیت به بیت پیام استخراج شده و پیام نهان نگاری شده، می توان



مدل دوم پس از حمله جدید



مدل نخست پس از حمله جدید

شکل ۱. دو مدل نهان نگاری شده پس از اعمال حمله

به ویژه روش های حوزه تبدیل را ندارد. انتخاب میانه از آن نظر اهمیت دارد که میانه به عنوان یک ویژگی مقاوم از یک مثلث است. انتخاب مثلث ها جهت گنجاندن یک رشته پیام، مبتنی بر مساحت آن ها و ضریبی انتخاب شده توسط کاربر فرض گردیده است تا تقسیم مثلث به دو مثلث منجر به تولید مثلث های بسیار کوچک نشود. چرا که در مدل هایی با چگالی بالاتر، و مثلث هایی با مساحت کمتر، تغییرات بیشتر محسوس خواهند بود. همان طور که مشاهده شد، اغلب روش ها در عنصرپایه گنجاندن خود نیز ترتیبی خاص را معرفی می کنند. در این روش نیز رسم میانه که پایه کار را تشکیل می دهد، ترتیب خاصی دارد. در روش اولیه، این ترتیب با بزرگی اضلاع مثلث مشخص می شود و به جهت عدم مقاومت آن در برابر حمله کشیدن، در روش بهبودیافته، این ترتیب بر اساس اندیس رئوس مقابل اضلاع پیشنهاد گردیده است.

برخی روش ها، علاوه بر رشته نهان نگاری، از رشته رمز نیز به منظور افزایش امنیت بهره می گیرند. در این روش به منظور ساده سازی پیاده سازی و با توجه به عدم نیاز روش به چنین امکانی، از رشته رمز استفاده ای نشده است.

جدول ۴: مقایسه نسبت شناسایی دو روش در شش حمله مختلف

فاکتور تغییر مقیاس	۰/۵	۰/۵	۰/۵	۰/۵	۲	۲
بردار انتقال	T1	T2	T3	T1	T2	T3
شماره حمله	۱	۲	۳	۴	۵	۶
مدل اول	روش ۱	۰/۹۷	۰/۹۷	۰/۹۶	۰/۹۷	۰/۹۷
اول	روش ۲	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰
مدل دوم	روش ۱	۰/۷۳	۰/۷۵	۰/۷۴	۰/۹۰	۰/۹۱
دوم	روش ۲	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰

نسبت های شناسایی در جدول ۴ با استفاده از روابط ۲ و ۳ بدست آمده اند.

۵- نتیجه گیری

در این نوشتار، دو روش جهت نهان نگاری مدل های سه بعدی مثلثی مبتنی بر افزودن مثلثی حاوی میانه مثلث ها ارائه شد. در مقایسه با روش های دیگر، ایده ای که در این مقاله معرفی شده است، پیچیدگی مفهومی برخی روش ها

۳-۱- روش بهبود یافته مبتنی بر میانه و اندیس رؤس

روش مبتنی بر میانه و مساحت دارای چالش‌هایی است که مهم‌ترین آن، خطای محاسبات ممیزشناور است. این خطا موجب تغییر ترتیب مساحت مثلث‌ها بر اساس حمله مورد استفاده می‌شود؛ به نحوی که ترتیب رشته استخراج شده بهم خورده، نسبت شناسایی کاهش می‌یابد. از سویی دیگر، همان‌طور که در فرمول (۱) [۱]، که کشیدن در راستای محور x را نشان می‌دهد، نشان داده شده است، طول اضلاع مثلث، و در واقع ترتیب گنجاندن درون هر مثلث، در برابر حمله کشیدن مقاوم نیست.

$$x' = x + y \cot \theta + z \cot \phi \quad (\text{رابطه ۱})$$

$$y' = y$$

$$z' = z$$

برای بهبود روش، توصیف سطوح در این مدل‌ها را مورد نظر قرار می‌دهیم. از آن جا که هر سطح با اندیس رؤس آن توصیف می‌شود، مرتب‌سازی نزولی این اندیس‌ها می‌تواند عاملی مناسب جهت جایگزینی عامل مساحت و طول اضلاع مثلث در روش شود [۲۹].

از این رو، مطابق روش قبل، در ابتدا مجموعه‌ای از مثلث‌ها انتخاب می‌شوند. این بار، با توجه به مقایسه ترتیب نزولی رؤس توصیف هر مثلث لیست مثلث‌های انتخابی، مرتب می‌شوند تا ترتیب گنجاندن در لیست مربوطه مشخص شود.

در گام بعد، در هر مثلث، فرض می‌شود راس A بزرگ‌ترین اندیس و راس C کوچک‌ترین اندیس را داشته باشد. بر همین اساس و مطابق جدول (۲) می‌توان گنجاندن را سامان‌دهی کرد. جدول (۳) نیز با همین شرایط می‌تواند به منظور استخراج نهان‌نگاری مدنظر قرار گیرد.

۴ - پیاده‌سازی و آزمون روش

در پیاده‌سازی روش، سه برنامه در محیط ویژوال ++C به منظور گنجاندن، حمله به مدل و استخراج پیاده‌سازی گردید. از میان مدل‌های سه بعدی، دو مدل Beethoven با تعداد ۲۵۲۱ راس و ۵۰۲۸ سطح (مثلث) و Cow با تعداد ۲۹۰۳ راس و ۵۸۰۴ مثلث مدنظر قرار گرفتند. گنجاندن در مدل نخست، ۴۹ بار تکرار و در مدل دوم، بیش از ۷۹ بار تکرار می‌شود.

دو مدل نهان‌نگاری شده، تحت حمله ترکیبی چرخش، تغییرمقیاس، انتقال و کشیدن، که تبدیل خطی انتقال یافته نیز نامیده می‌شود، قرار گرفت که حاصل در شکل (۱) آرایه شده است.

در مرحله استخراج نیز، دو مثلث که دو راس مشترک و یک راس غیرمشترک دارند، برای بررسی مرحله بعد انتخاب می‌شوند. نتیجه استخراج روی هر دو مدل، بازایی کامل تمامی تکرارهای پیام گنجانده شده و در نتیجه نسبت شناسایی یک بوده است. در جدول (۴)، نتایج دو روش اولیه و توسعه یافته برای دو مدل مقایسه شده است. برای روش اول، حمله ترکیبی چرخش، انتقال و تغییرمقیاس یک‌نواخت ارزیابی شده است و برای روش دوم، حمله کشیدن نیز به ترکیب حملات افزوده شده است. درجه چرخش

جدول ۲: 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	BCM_b	
شروع رشته	M_a	ABM_a	

در مرحله استخراج، دو مثلث که در دو راس مشترک باشند و مساحت یکی تقریباً دو برابر مساحت دیگری باشد، مورد بررسی قرار می‌گیرند تا مشخص شود که آیا راس غیرمشترک یکی می‌تواند میانه مثلث دیگری باشد یا خیر. در صورت مثبت بودن پاسخ، دو مثلث، به عنوان مثلث‌های واجد نهان‌نگاری شناسایی می‌شوند.

سپس، برای هر مثلث سه ناحیه در نظر گرفته می‌شود که ناحیه ۱ بیانگر کوچک‌ترین ضلع مثلث و ناحیه ۳ برابر بزرگ‌ترین ضلع مثلثی 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. پس از پایان کلیه بررسی‌ها، مثلث‌هایی که حاوی نهان‌نگاری تشخیص داده شده‌اند؛ بر اساس مساحت، مرتب می‌شوند تا مجموعه گدهای دوبیتی استخراج شده، رشته پیام نهان‌نگاری شده را به صورت تکرار شده آرایه دهند. هر تکرار با کد شروع از تکرار بعدی قابل تفکیک خواهد بود.

جدول ۳ نحوه استخراج کد ذخیره شده بر اساس میانه و مثلث را نشان می‌دهد. با مقایسه بیت به بیت پیام استخراج شده با پیام نهان‌نگاری شده، می‌توان مقدار دقت شناسایی را به دست آورد.

جدول ۳: نحوه استخراج پیام نهان‌نگاری 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

است که باید به مدل افزوده شود و در ستون شکل نیز شکل مثلثها برای فهم بهتر موضوع ارایه شده است.

جدول ۱: مروری مقایسه ای از تحقیقات مشابه

I: Informed, B: Blind, F.: Frequency, S.: Spatial

Type	Method	Ref. No.	Domain	Name of Attack																		
				Geometrical	rotation	translation	uniform scaling	similarity transform	lossy compression	affine transform	mesh smoothing	mesh simplification	polygon simplification alg.	randomization of vertex coordinations	Cropping	vertex reordering	connectivity reordering	remeshing	introduction of noise	additive random noise	random noise added to vertices	Insertion of other watermarks
B.	Wavelet Multiresolution Analysis	[12]	F.					✓	✓	✓							✓					
I.	Spectral Analysis	[6]	F.					✓		✓	✓	✓			✓			✓		✓		
B.	TSQ	[16]	S.		✓	✓	✓	✓									✓					
B.	TVR	[16]	S.							✓												
B.	TSPS	[16]	S.	✓													✓					
I.	Mesh Spectral	[20]	F.					✓			✓						✓				✓	
I.	Mesh Spectral- Extended	[18]	F.					✓			✓	✓					✓					
I.	Mesh Spectral	[18]	F.					✓									✓					
I.	NBE (Normal Bin Encoding)	[4]	S.										✓						✓	✓		
I.	Spread Spectrum	[21]	F.		✓	✓	✓	✓			✓	✓					✓	✓			✓	
I.	Spectral Analysis	[19]	F.					✓				✓					✓			✓		
I.	EGI	[3]	F.										✓	✓					✓			
B.	POA	[27]	F.					✓														
B.	SPOA (Sectional POA)	[27]	F.					✓				✓										
B.	Principal Component Analysis	[11]	F.	✓	✓	✓	✓															
I.	Spherical Fourier	[14]	F.		✓	✓	✓	✓			✓						✓	✓				
I.	perturbing the distance of vertices	[26]	S.									✓					✓				✓	
I.	Spherical Wavelet	[10]	F.									✓						✓				
I.	perturbing the distance of vertices	[28]	S.		✓	✓	✓	✓			✓	✓					✓	✓			✓	✓
B.	Discrete Fourier Transform magnitude	[22]	F.		✓	✓	✓	✓									✓				✓	
B.	extended TSPS	[5]	S.		✓	✓	✓	✓		✓												
B.	Projection On Convex Sets	[13]	F.							✓		✓					✓				✓	
I.	DCT	[9]	F.						✓	✓										✓		✓
B.	AIE (Affine Invariant Embedding)	[4]	S.							✓												
I.	Spherical coordinate	[2]	S.						✓	✓		✓								✓		

است. ضمن آنکه مقاومت روش‌ها در برابر برخی حملات در جدول نشان داده شده است.

۳- نهانگاری مبتنی بر میانه و مساحت

روش‌های گوناگونی برای نمایش مدل‌های سه‌بعدی ارائه شده است. از آن جمله می‌توان به تمرکز شیوه نمایش مدل بر روی فایل‌های زبان مدل-سازی واقعیت مجازی اشاره کرد [۲۳].

در این شیوه نمایش، مدل توسط مجموعه‌ای از نقاط و سطوح ناشی از اتصال این نقاط به یکدیگر توصیف می‌شود. یعنی برای توصیف مثلثی چون ABC باید 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 ساختاری تعریف شده است که هر نقطه توسط مجموعه مختصات سه‌مقداری (X_i, Y_i, Z_i) معرفی می‌شود. هر سطح (چندضلعی) نیز با دنباله‌ای از اندیس نقاط $(V_1, V_2, V_3, \dots)$ مشخص می‌شود که با اندیس ۱- پایان آن مشخص می‌گردد. در این روش، سطوح مثلثی در فرآیند گنجاندن، مدنظر قرار گرفته‌اند. در روش موجود در این مقاله، انتخاب مثلث‌ها بر اساس شرطی روی مساحت آنها صورت می‌گیرد. این شرط به کمک ضریبی قابل تغییر توسط کاربر، شکل می‌یابد. در مجموعه مثلث‌های انتخاب شده، ترتیب اجرای روش گنجاندن نیز مبتنی بر اندازه مساحت مثلث‌هاست [۲۹].

همچنین، در این روش به منظور اعمال نهان نگاری از ویژگی میانه استفاده شده است. ویژگی منحصر بفرد میانه به منظور بکارگیری در نهانگاری آن است که 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 این روش پیشنهادی این مقاله، اضلاع هر مثلث، بر اساس طول آن‌ها به صورت نزولی مرتب شده‌اند. در هر مثلث، یکی از سه میانه، بر اساس پیامی که قصد گنجاندن آن را داریم و متناظر با ترتیب مشخص شده اضلاع است، انتخاب می‌شود. به واسطه انتخاب هر میانه نیز دو مثلث جدید ایجاد می‌شود که یکی از این دو مثلث، بر اساس پیام مورد نظر و ترتیب بزرگی طول اضلاع، انتخاب شده و به مجموعه سطوح مدل افزوده می‌گردد.

پیام مربوط به نهان نگاری در روش پیشنهادی، یک کد دودویی هفتاد بیتی (یا ۱۰ کاراکتری) فرض شده است [۲]. پیام هفتاد بیتی مذکور، به‌عنوان نهان‌نگار، با به‌کارگیری ۳۶ مثلث برای یک‌بار در مدل قابل گنجاندن است. یک مثلث از این ۳۶ مثلث به منظور مشخص کردن شروع رشته و ۳۵ مثلث دیگر جهت گنجاندن ۷۰ بیت اطلاعات به‌کار گرفته می‌شود. واضح است با توجه به تعداد مثلث‌های لیست مرتب شده، گنجاندن به صورت تکرار شونده صورت گرفته است که این امر سبب افزایش مقاومت در مقابل حملات برش می‌شود.

جدول ۲ روش گنجاندن و جدول ۳ چگونگی استخراج پیام نهان‌نگاری شده را نشان می‌دهد. لازم به ذکر است در کلیه اشکال فرض شده است که طول اضلاع a، b و c که به ترتیب در برابر رئوس A، B و C قرار دارند، به صورت صعودی است.

در جدول (۲)، ستون کد، بیانگر دو بیت رشته نهان‌نگار است؛ ستون راس، بیانگر راسی است که به مدل افزوده می‌شود؛ ستون مثلث، بیانگر مثلثی

در مدل گنجانده می‌شود تا مقاومت در برابر حملات برش حاصل گردد. این روش از چند منظر قابل توجه است: تعریف عنصر پایه درشت‌دانه، به‌کارگیری ویژگی متمایزکننده مثلث‌ها، انتخاب ویژگی مقاوم در برابر حمله مشابهت، استفاده از عنصری به منظور شناسایی عنصر پایه گنجاندن، لزوم تصریح ترتیب عناصر گنجاندن، گنجاندن به کمک تغییر موقعیت رئوس مثلث، استفاده از تکرار به منظور مقاومت در برابر برش و استفاده از مدل‌های زبان مدل‌سازی واقعیت مجازی.

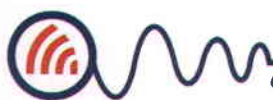
روش TVR [۱۶] نیز توری مثلثی به عنوان ورودی می‌پذیرد و در مرحله استخراج به مدل اولیه نیاز ندارد. عنصر پایه گنجاندن در این روش، نسبت حجم یک زوج چندوجهی است. چیدمان این روش توپولوژیکی و یک‌بعدی است. ویژگی مورد استفاده در روش هندسی است و نهان‌نگاری در حوزه فضایی صورت می‌گیرد. از آن‌جا که نسبت حجم دو چندوجهی در برابر تبدیل خطی انتقال‌یافته مقاوم است، این روش نیز، نخستین تلاش در خصوص مقاومت در برابر تبدیل خطی انتقال‌یافته تلقی می‌شود [۴]. استفاده از نسبت حجم دو چندوجهی برای مقاومت در برابر تبدیل خطی انتقال-یافته، استفاده از چیدمان توپولوژیکی و استفاده از گرانیگاه مثلث به منظور نقطه پایه ساخت احجام موارد قابل توجه در این روش هستند.

روش TSPS [۱۶] نیز مبتنی بر مدل توری بوده که عنصر پایه گنجاندن و دست‌کاری در این روش توپولوژیکی است. عنصر پایه گنجاندن، باریکه نواری از مثلث‌های همسایه است که هر کدام بیتی از اطلاعات را رمز می‌کنند. از موارد حایز اهمیت در این روش می‌توان به استفاده از باریکه مثلثی به عنوان عنصر پایه توپولوژیکی، لزوم تعریف ترتیب برای اضلاع مثلث و مقاومت چیدمان و عنصر پایه توپولوژیکی در برابر حملات هندسی اشاره کرد. در توسعه این روش [۵]، از نسبت دو بخش یک پاره‌خط به منظور افزایش مقاومت در برابر تبدیل خطی انتقال‌یافته استفاده شده و لزوم کنترل میزان تغییرات به منظور حفظ شفافیت مطرح شده است.

در روش POCS [۱۴] مرکز جرم جسم به مبدا مختصات انتقال داده می‌شود. رئوس مدل انتقال داده شده، به مختصات کروی تبدیل می‌شوند و تمام مولفه‌های آن به K زیربخش تقسیم می‌شوند؛ به نحوی که K تعداد بیت‌های نهان‌نگار است. استفاده از انتقال ویژگی خاصی از مدل مانند مرکز جرم به مختصاتی مشخص به منظور افزایش مقاومت، استفاده از مختصات کروی و شعاع آن و بخش‌بندی مقادیر مولفه مورد استفاده به منظور بخش بندی مدل مواردی هستند که در این روش، آموخته به نظر می‌آیند.

برخی روش‌ها به گنجاندن بر حسب مقادیر غیرهندسی مانند بافت توجه نشان داده‌اند [۱۷]. روشی دیگر به دست‌کاری فاصله گره‌ها تا مرکز مدل توجه داشته است [۲۶]. دسته‌ای از روش‌ها نیز بر حوزه تبدیل یا فرکانس متمرکز شده‌اند. توسعه تکنیک طیف گسترده [۲۱]، هیستوگرام جهت تولید شده بر اساس بردارهای نرمال [۳]، تجزیه‌های مختلف از مدل مانند، تجزیه eigenvalue [۶؛ ۱۸؛ ۱۹؛ ۲۰]، تجزیه مولفه پایه [۱۱] و تجزیه موجک [۱۲]، استفاده از پارامتری کردن کروی [۱۴] و ایده‌هایی مشابه در این دسته مطرح شده‌اند.

جدول ۱ مقایسه کلی از برخی از روش‌های مطرح در زمینه نهان‌نگاری مدل‌های سه‌بعدی را نشان می‌دهد. دسته‌بندی روش‌ها بر اساس حوزه در زمان نهان‌نگاری و نیاز و یا عدم نیاز به مدل در زمان استخراج صورت گرفته



نیاز به وجود رسانه فاقد نهان‌نگاری، دو دسته روش نهان‌نگاری آگاهانه و کور مطرح می‌باشد [۷].

از جمله مسایل مهم در نهان‌نگاری موضوع حملات است. در حالت کلی، هر پردازشی که منجر به خنثی کردن هدف نهان‌نگاری و نه لزوماً حذف آن شود، حمله نامیده می‌شود. حمله، که گاهی از آن به دست‌کاری و خراب‌کاری نیز یاد می‌شود، اصولاً کیفیت بصری رسانه را کاهش چشمگیری نمی‌دهد [۱۵؛ ۲۴؛ ۲۵]. حملات را می‌توان از منظرهای گوناگون مورد بررسی قرار داد. از منظر نوع حمله نیز حملات به دسته‌های مختلفی چون حملات هندسی و توپولوژیکی تقسیم می‌شوند. دسته نخست موجب تغییرات هندسی در مدل مانند موقعیت رئوس یک مدل می‌شوند. دسته دوم همسایگی سطوح و نحوه اتصال اجزای پایه مدل را دست‌کاری می‌نمایند [۲۹].

تمرکز این نوشتار بر رسانه‌ای از نوعی دیگر و در بُعدی جدید یعنی مدل‌های سه‌بعدی است. نخستین گام در خصوص نهان‌نگاری در مدل‌های سه‌بعدی به سال ۱۹۹۷ برمی‌گردد [۱۶]. در مدل‌های سه‌بعدی، مدل توسط نقاطی سه‌بعدی و مجموعه‌ای از سطوح توصیف می‌شوند. کاربردهایی از این مدل، در مواردی مانند هنر فیلم‌برداری و واقعیت مجازی است که محصول اولیه توسط فردی خلق و توسط افراد دیگری مورد استفاده قرار می‌گیرد [۸]. در یک دسته‌بندی کلی، گنجاندن در روش‌های نهان‌نگاری، در مدل‌های سه‌بعدی به دو شیوه صورت می‌پذیرد. در دسته اول روش‌ها، گنجاندن در دامنه فضایی سامان‌دهی می‌شود و مستقیماً اطلاعاتی مانند موقعیت رئوس مورد توجه می‌باشند [۶]. در مقابل در دسته دوم، دامنه تغییر شکل یافته برای گنجاندن اطلاعات مدنظر قرار گرفته می‌شود. به عنوان نمونه، در این دسته، از تکنیک‌هایی مانند طیف گسترده، تجزیه توری، دامنه موجک، تبدیل گسسته کسینوس [۹] و تبدیل فوری [۲۲] بهره گرفته شده است.

برای بیان مدل سه‌بعدی نیز روش‌های مختلفی می‌توان در پیش گرفت. مثلاً در یک مدل مثلث‌بندی‌شده، می‌توان یک ترتیب یک بعدی از مثلث‌ها بر اساس مساحت‌شان یا ترتیبی دوبعدی از اتصال مثلث‌ها به یکدیگر را به عنوان چیدمان انتخاب کرد. این بیان به دو شیوه کلی همسایگی و کمتی ظاهر می‌شود. شیوه نخست، غالباً در برابر تبدیلات هندسی مقاوم است. در شیوه دیگر، تفاوت مقادیری از مدل مانند مساحت مدنظر قرار می‌گیرد. یافتن جزء اولیه آغازین نیز نقطه حساسی در بیان چیدمان مدل است؛ چرا که باید در برابر دستکاری‌ها مقاوم باشد [۱۷].

به طور خلاصه می‌توان گفت مواردی مانند تعدد و تنوع حملات و مقاوم‌سازی روش در برابر حملات، آگاهانه و یا کور بودن روش، دشواری مقایسه روش‌های نهان‌نگاری در مدل‌های سه‌بعدی توری به دلایل فقدان شیوه نمایش استاندارد، مقاومت و پیچیدگی الگوریتم، به عنوان چالش‌ها در این حوزه مطرح می‌شوند [۱۸].

۲-۱- اهداف تحقیق

در این مقاله، بهبودی بر تحقیق قبلی مولف [۳۰] صورت گرفته است. تمرکز بر ارایه روشی مقاوم در نهان‌نگاری اطلاعات برای مدل‌های سه‌بعدی است. از میان شیوه‌های نمایش مدل سه‌بعدی، شیوه انتخابی ما مبتنی بر مدل توری است.

در تحقیق قبلی به این اصل تاکید داشتیم که ویژگی ای انتخابی در مدل سه بعدی به عنوان مقصد نهان نگاری باید چنان باشد که حداقل امکان در مقابل حملات مختلف، تغییرناپذیر باشد. به این منظور میانه مثلث به عنوان ویژگی مناسب مطرح شد. میانه از این نظر به عنوان ویژگی کارا در مدل های سه بعدی معرفی می شود که در برابر انتقال، چرخش، تغییر مقیاس و هر تغییری که نسبت بین دو ناحیه ناشی از رسم میانه را تغییر ندهد، معتبر خواهد بود. بر این اساس، در هر مثلث یکی از سه میانه بر اساس پیامی که قصد گنجاندن آن را داریم، انتخاب می شود. به واسطه انتخاب هر میانه نیز دو مثلث جدید ایجاد خواهد شد که یکی از این دو، بر اساس پیام مورد نظر، انتخاب شده و به مجموعه سطوح مدل افزوده میگردد. از جمله چالش های اساسی نهان نگاری مبتنی بر میانه می توان به ضعف روش در مقابل خطای محاسبات ممیزشناور اشاره نمود. این خطا موجب تغییر ترتیب مساحت مثلث ها بر اساس حمله مورد استفاده می شود؛ به نحوی که ترتیب رشته استخراج شده بهم خورده، نسبت شناسایی کاهش می یابد.

به این منظور در مقاله حاضر، روش بهبود یافته ای نسبت به روش اول که مبتنی بر میانه و ترتیب نزولی اندیس رئوس است، معرفی می گردد. از آنجا که هر سطح با اندیس رئوس آن توصیف می شود، مرتب سازی نزولی این اندیس ها می تواند عاملی مناسب جهت جایگزینی با عامل مساحت و طول اضلاع مثلث در روش شود. در آزمایشات صورت گرفته نشان خواهیم داد که مقاومت روش بهبود یافته در مقابل دسته دیگر از حملات، از آن جمله حملات خطی، به چه میزان قابل توجه ای بهبود خواهد یافت.

ادامه مقاله در قالب بخش های زیر سامان دهی شده است. در بخش ۲، کلیاتی از تحقیقات صورت گرفته ارایه شده است. همچنین به ارایه مقایسه ای مابین روش های موجود می پردازیم. تحلیلی بر روش ارایه شده در این مقاله، موضوع بخش ۳ است. در بخش ۴، به پیاده سازی و آزمون روش پیشنهادی پرداخته شده است. در بخش پایانی، جمع بندی کار و زمینه کارهای آتی مطرح شده است. همچنین به مقایسه روش بهبود یافته با روش های مشابه در دنیا پرداخته ایم.

۲- مروری بر تحقیقات صورت گرفته

در این بخش، برخی از روش های تاکنون ارایه شده که از نتایج برخی از آن ها در روش پیشنهادی نیز بهره گرفته شده است، بررسی می شوند. روش های نهان نگاری در مدل های سه بعدی چندضلعی نیز همانند روش های موجود در مدل های دوبعدی، در دو حوزه تصویر یا فضایی و حوزه تبدیل یا فرکانس صورت می گیرند. گنجاندن در حوزه فضایی مبتنی بر تغییرات موقعیت رئوس، دست کاری توپولوژی و نظایر آن است، در حالی که در حوزه تبدیل، مدل به فضای دیگری برده شده و سپس نهان نگاری در آن حوزه صورت می گیرد [۵؛ ۲۷].

روش TSQ [۱۶] از جمله روش های نهان نگاری در مدل های سه بعدی است. این روش مبتنی بر توری مثلثی بوده و در مرحله استخراج به مدل اولیه نیازمند نیست. ویژگی مورد استفاده در این روش هندسی بوده و نهان نگاری در حوزه فضایی صورت می گیرد. گنجاندن در این روش بر روی عنصر پایه درشت دانه ای MEP مشتمل بر چهار مثلث که در همسایگی هم قرار دارند صورت می گیرد. ضمن آن که نهان نگاری نیز به صورت تکرار شونده



نهان نگاری مبتنی بر میانه و اندیس رئوس در مدل های سه بعدی مثلثی

رضا فرید

نصرا... مقدم چرکری

آزمایشگاه پردازش موازی و تصویر

دانشگاه تربیت مدرس، دانشکده فنی و مهندسی،

بخش مهندسی برق

rezaf@modars.ac.ir

آزمایشگاه پردازش موازی و تصویر

دانشگاه تربیت مدرس، دانشکده فنی و مهندسی،

بخش مهندسی برق

charkari@modares.ac.ir

۱- مقدمه

با رشد و تسهیل توزیع داده‌های چندرسانه‌ای از طریق شبکه‌های کامپیوترهای و ارتباطات اینترنتی مساله حفاظت از حق‌نشر و مالکیت معنوی به عنوان یکی از چالش‌های جدی مطرح می‌باشد. در این رابطه از نهان‌نگاری به عنوان یکی از رویکردهای مهم نام برده می‌شود. در نهان‌نگاری، اطلاعات در نوع مشخصی از داده رقمی، عموماً به صورت نامحسوس در رسانه موردنظر گنجانده می‌شود تا در کاربردهای گوناگونی مانند حفاظت از حق‌نشر و اثبات مالکیت رسانه مورد نظر، انتقال پنهان اطلاعات، تصدیق هویت و پیگیری نسخه‌های غیرمجاز بتوان از آن بهره جست [۷]. رسانه‌های مختلفی در نهان‌نگاری می‌توانند مدنظر قرار گیرند. در این راستا، صوت به عنوان رسانه‌ای تک‌بعدی در طول زمان، تصویر به عنوان نگاشتی از فضای دوبعدی و تصاویر ویدیویی متحرک در نهان‌نگاری به صورت وسیعی مورد توجه بوده‌اند [۸].

دو مرحله اصلی در نهان‌نگاری، گنجاندن و استخراج اطلاعات است. با توجه به نوع کاربرد، تکنیک مورد استفاده در نهان‌نگاری باید در برابر دست‌کاری‌های سهوی و عمدی که می‌تواند موجب تخریب داده نهان‌شده گردد، مقاوم یا شکننده باشد. از سویی دیگر در مرحله استخراج، بر اساس نیاز یا عدم

چکیده - در این مقاله، روشی جهت نهان‌نگاری اطلاعات در مدل‌های سه‌بعدی مثلثی در حوزه تصویر ارایه می‌شود. در ابتدا روشی مبتنی بر مساحت مثلث‌ها و میانه معرفی می‌شود. این روش مبتنی بر افزودن مثلث‌هایی به مدل اصلی سه بعدی است. این افزایش با توجه به رشته پیام مورد نظر در گنجاندن صورت می‌گیرد. بدین منظور، مجموعه‌ای از مثلث‌های مدل بر اساس مساحت، انتخاب می‌شوند تا لیست مثلث‌های منتخب تشکیل گردد. این لیست بر اساس عاملی مقاوم در برابر برخی حملات مرتب می‌شوند. سپس یکی از سه میانه هر مثلث بر حسب رشته پیامی که هدف اصلی، گنجاندن آن در مدل است؛ در نظر گرفته شده و یکی از دو مثلث ناشی از رسم آن میانه، بر اساس عامل ترتیب‌دهی در مثلث، به مدل افزوده می‌گردد. انتخاب به گونه‌ای است که مقاومت در برابر دسته‌ای از حملات مهم حاصل شود. روش موجود در برابر مجموعه حمله‌های چرخش، تغییر مقیاس و انتقال، که به حمله مشابهت نیز موسوم است، مقاوم است. در ادامه، به منظور بهبود روش، مرتب‌سازی مثلث‌ها و ترتیب انتخاب میانه بر اساس اندیس رئوس بنا می‌شود تا مقاومت روش در برابر حملات تبدیل خطی انتقال یافته نیز حاصل گردد. آزمایش‌های صورت گرفته بر روی مدل VRML کارایی روش‌ها را در مقابل حملات فوق‌الذکر نشان می‌دهد.

کلید واژه- حمله تبدیل خطی انتقال یافته، مقاومت، زبان مدل‌سازی واقعیت مجازی، نهان‌نگاری مدل‌های سه‌بعدی.