روش بهبودیافته نهان‌نگاری در مدل‌های سه‌بعدی مثلثی مبتنی بر میانه و اندیس رئوس

رضا فرید، نصرا... مقدم چرکری

دانشگاه تربیت مدرس، دانشکده فنی و مهندسی، بخش مهندسی برق

E-mail: Reza_Farid@modares.ac.ir, Charkari@modares.ac.ir

چکیده - در این نوشتار، روشی بهبودیافته در خصوص نهان‌نگاری اطلاعات در مدل‌های سه‌بعدی مثلثی معرفی می‌گردد. برای این منظور، مثلث‌هایی به مدل اصلی افزوده می‌شود. این افزایش با توجه به رشته پیام گنجاندنی صورت می‌گیرد. بدین منظور، مجموعه‌ای از مثلث‌های مدل بر اساس عاملی مبتنی بر مساحت مثلث، 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. انتخاب‌ها به گونه‌ای صورت می‌گیرد که مقاومت در برابر برخی حملات حاصل شود. روش پیشنهادی قبلی در برابر مجموعه حمله‌های چرخش، تغییر مقیاس و انتقال، که به حمله مشابهت نیز موسوم است، مقاوم بود؛ اما مقاومت روش در برابر حمله تبدیل خطی انتقال-یافته، به دلیل لحاظ کردن مساحت در ترتیب عناصر گنجاندن، فراهم نبود. در این مقاله، مرتب‌سازی مثلث‌ها و ترتیب انتخاب میانه بر اساس اندیس رئوس بنا می‌شود تا مقاومت روش در برابر تبدیل خطی انتقال یافته نیز حاصل گردد.

کلید واژه- حمله تبدیل خطی انتقال‌یافته، حمله مقاومت، زبان مدل‌سازی واقعیت مجازی، عدم نیاز به مدل اصلی، نهان‌نگاری مدل‌های سه‌بعدی.

۱- مقدمه

تسهیل و تسریع توزیع داده‌های رقمی توسط کامپیوترهای شخصی و ارتباطات اینترنتی موجب رشدی چشم‌گیر در استفاده و توزیع داده‌های چندرسانه‌ای و پررنگ شدن مساله حفاظت از حق‌نشر شده‌است. در مواجهه با این مساله، دو روش رمزنگاری و نهان‌نگاری وارد شده‌اند. در نهان‌نگاری، اطلاعات در نوع مشخصی از داده رقمی، اصولاً به صورت *نامحسوس*، گنجانده می‌شود تا در کاربردهای گوناگونی مانند حفاظت از حق‌نشر و اثبات مالکیت رسانه مورد نظر، انتقال پنهان اطلاعات، تصدیق هویت، نظارت بر پخش، پیگیری نسخه‌های غیرمجاز و بانک‌های اطلاعاتی بتوان از آن بهره جست. نهان‌نگاری در دو مرحله اصلی *گنجاندن* و *استخراج* صورت می‌گیرد. بسته به کاربرد، 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. از سویی دیگر، نیاز یا عدم نیاز به وجود رسانه فاقد نهان‌نگاری در مرحله استخراج نهان‌نگاری، دو دسته روش نهان‌نگاری *آگاهانه* و *کور* را مطرح ساخته است [۳].

رسانه‌های مختلفی در نهان‌نگاری مدنظر قرار گرفته‌اند. صوت به‌عنوان رسانه‌ای تک‌بُعدی در طول زمان، تصویر به‌عنوان نگاشتی از فضای دوبعدی و تصاویر ویدیویی متحرک در نهان‌نگاری به‌صورت وسیعی مورد توجه بوده‌اند[۱۸].

در بسیاری از کاربردها، در مسیر یا مدت رسیدن رسانه به گیرنده، پردازش‌هایی سهوی یا عمدی بر رسانه اثر می‌گذارند. این اثر می‌تواند منجر به تاثیر در نهان‌نگاری گنجانده شده گردد. 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[۵، ۱۰ و۱۵]. در یک دسته-

بندی کلی، حمله‌ها را می‌توان به چهار گروه حمله حذفی و *دخل‌وتصرف*، *هندسی*، *پنهان‌نگاری* و *تفسیر و پروتکل* تقسیم کرد [۱۱].

در حالت عام، در سنجش روش‌ها نیاز است که انواع مختلفی از رسانه مدنظر قرار گیرند. مثلاً در خصوص رسانه تصویر، هر تصویر از منظر پردازش به دلیلی مانند بافت، یکدستی، حجم، ترکیب، وضعیت لبه‌ها، میزان محو بودن، میزان روشنایی و کنتراست قابل توجه است [۱۹]. لذا توجه به وجود نمونه مناسب آزمون نیز در نهان‌نگاری مطرح است.

به ازای حملاتی که علیه نهان‌نگاری مطرح شده‌اند، روش-های مختلف مقابله نیز مورد توجه قرار گرفته‌اند. نکته کلیدی در این خصوص، مصونیت کلیت رسانه در حملات است. این نکته، نهان‌نگاری مبتنی بر محتوای رسانه را به عنوان شیوه‌ای کارآمد در افزایش مقاومت نهان‌نگاری، منتج ساخته است. در این نوع نهان‌نگاری، تلاش روش بر یافتن نقاط مشخصه‌ای از رسانه که در برابر حملات گوناگون مقاوم هستند، متمرکز می‌شود تا گنجاندن اطلاعات در نقاط مشخصه مربوطه صورت پذیرد [۶، ۱۲و۲۵].

تمرکز این نوشتار بر رسانه‌ای از نوعی دیگر و در بُعدی جدید یعنی مدل‌های سه‌بعدی است. در مدل‌هاس سه‌بعدی، مدل توسط نقاطی سه‌بعدی و مجموعه‌ای از سطوح توصیف می‌شوند. کاربردهایی از 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 برداشته شده است. تمرکز تلاش‌های صورت گرفته تاکنون نیز، بر شناسایی مشخصات مقاومی از مدل شده است که در برابر حملات تغییر نکند یا با انجام برخی تبدیلات بتوان بعد از حمله، باز همان مشخصات را یافت. از این مشخصات به عنوان مقصد گنجاندن استفاده می‌شود. شناسایی مشخصات پایه نهان‌نگاری، در مرحله استخراج نیز اهمیت دارد[۱۳].

در روش‌های نهان‌نگاری، سه خصوصیت اهمیت دارد که مصالحه میان آن‌ها بر اساس کاربرد مشخص می‌شود. نامحسوس بودن (یا بسته به کاربرد آشکار بودن)، مقاومت و ظرفیت این سه خصوصیت هستند. حملاتی که روش در مقابل آن‌ها باید مقاوم باشد نیز به دسته‌های مختلفی قابل تقسیم هستند. حملات هندسی مانند تبدیلات چرخش، تغییرمقیاس، انتقال و *تبدیل خطی انتقال‌یافته*، حملات توپولوژیکی مانند ساده‌سازی چندضلعی‌ها و سایر حملات مانند تبدیل فُرمت داده و خطاهای نمایش اعداد ممیزشناور نمونه‌هایی از این دست هستند[۱].

در یک مدل، *اجزای هندسی اولیه* توصیف‌کننده مدل اهمیت خاصی دارند. نقاط، خطوط، چندضلعی‌ها، چندضلعی‌های متصل، چندوجهی‌ها و چندوجهی‌های متصل مثال‌هایی از این اجزاء محسوب می‌شوند.

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 *کمّی* 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 [۷].

هر یک از الگوریتم‌های مطرح شده، در برابر ترکیبی از حملات یا حمله خاصی با مشکل مواجه می‌شوند. در برخی نمی‌توان به سرعت وجود نهان‌نگاری را رد کرد و پرداخت هزینه استخراج برای این منظور، اجتناب‌ناپذیر است. برخی مدل‌های سه‌بعدی مانند کَد نیز، به دلیل تولید محصول از روی مدل، هیچ تحملی در برابر کوچک‌ترین تغییرات در مدل خود را ندارند [۲۰].

به طور خلاصه می‌توان گفت مواردی مانند تعدد و تنوع حملات و مقاوم‌سازی روش در برابر حملات، مطلع یا کور بودن روش، دشواری مقایسه روش‌های نهان‌نگاری در مدل-های سه‌بعدی *توری* به دلایل فقدان شیوه نمایش استاندارد، عدم وجود مجموعه داده سه‌بعدی استاندارد به منظور ارزیابی روش‌ها، فقدان ابزار سنجش موثر تخریب شکل؛ بهبود امنیت، قابلیت اطمینان، مقاومت و الگوریتم پیچیده‌تر برای گنجاندن در طرح روش‌ها، به عنوان برخی چالش‌ها، خودنمایی می‌کنند [۲۴].

در یک دسته‌بندی کلی، روش‌های نهان‌نگاری، گنجاندن خود را مدل‌های سه بعدی به دو شیوه صورت می‌دهند. برخی روش‌ها، گنجاندن را در دامنه *فضایی* سامان‌دهی می‌کنند و مستقیماً روی اطلاعاتی مانند موقعیت رئوس کار می‌کنند [۱۶]. در مقابل، روش‌هایی دامنه *تغییر شکل یافته* را برای گنجاندن اطلاعات مدنظر قرار داده‌اند. به عنوان نمونه، روش‌های دسته دوم از تکنیک‌های طیف گسترده، تجزیه مش تحلیل چندگانه، دامنه موجک، تبدیل به تصویر و استفاده از روش‌های نهان‌نگاری تصاویر[۲۲]، تبدیل گسسته کسینوس [۲۱]، تبدیل فوریه [۱۷] و تحلیل مولفه پایه‌ای [۸، ۱۴] بهره گرفته‌اند[۱].

در مقاله حاضر، بهبودی بر تحقیق قبلی مولف [۲] صورت گرفته است. در آن مقاله، ضمن انتخاب مدل توری مثلثی، به جهت کارآمد بودن آن [۹]، به عنوان نوع مدل، به برخی نتایج کلی اشاره شده که در ارایه روش‌ها می‌توانند مفید واقع شوند. اصولاً، برای مقاومت در برابر حمله‌ای خاص، باید ویژگی‌ای از مدل را مدنظر داشت که در برابر آن حمله پایدار باشد. مثلاً استفاده از نوع خاصی ترتیب برای مقابله با حمله درهم‌سازی ترتیب رئوس؛ گنجاندن تکراری پیام و هم‌چنین بخش‌بندی مدل به منظور مقاومت در برابر حمله برش[۱۶] و استفاده از تکرار هر بیت پیام به جهت مقاومت در برابر اعوجاج، مفید خواهد بود.

ضمناً اشاره کردیم، یک روش خوب نهان‌نگاری به این موارد پاسخ می‌دهد[۹]: (۱) گنجاندن 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 سامان‌دهی شده است. در بخش ۲، کلیاتی در خصوص روش پیشنهادی قبل مطرح می‌گردد. تحلیلی بر روش قبل و ارایه روش جدید، موضوع بخش ۳ است. در بخش ۴، به پیاده‌سازی و آزمون روش پیشنهادی پرداخته شده است و در بخش پایانی، جمع‌بندی کار و زمینه کارهای آتی مطرح شده است.

۲- خلاصه روش مبتنی بر میانه و مساحت

روش‌های نمایش گوناگونی برای مدل‌های سه بعدی ارایه شده است. در روش ارایه شده قبلی که آن‌را روش مبتنی بر میانه و مساحتِ می‌توان نامید، تمرکز شیوه نمایش مدل بر روی فایل‌های زبان مدل‌سازی واقعیت مجازی می‌باشد[۲۶]. 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 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 $(v_i,v_j,v_k,\ldots)$ مشخص می‌شود که با اندیس ۱- پایان آن مشخص می‌گردد. در این روش، سطوح مثلثی در فرآیند گنجاندن، مدنظر قرار گرفته‌اند.

در روش مذکور، انتخاب مثلث‌ها بر اساس شرطی روی مساحت مثلث‌ها 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 مساحت مثلث‌هاست.

در خصوص ویژگی‌ای در مدل که به‌عنوان مقصد نهان‌نگاری انتخاب شده است، باید گفت که ایده روش مذکور، معرفی میانه مثلث بوده 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 این روش، اضلاع 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 مشخص‌شده اضلاع، 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.

پیامی که در مدل گنجانده شده است، یک کد دودویی هفتاد بیتی (یا ۱۰ کاراکتری) فرض شده است [۲۳]. پیام هفتاد بیتی مذکور، به‌عنوان نهان‌نگاره، 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 تکرارشونده صورت گرفته است.

در این روش، گنجاندن و استخراج مطابق جدول (۱) و (۲) صورت می‌گیرد. 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.

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	BCM_b	
شروع رشته	M_a	ABM_a	

در جدول (۱)، 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 ارایه شده است.

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 مثلث باشد. این‌که 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 شده‌است (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 کُدهای دوبیتی استخراج شده، رشته پیام نهان‌نگاری شده را به صورت تکرار شده ارایه دهند. هر تکرار با "کد شروع" از تکرار بعدی قابل تفکیک خواهد بود.

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

با مقایسه بیت به بیت پیام استخراج شده و پیام نهان‌نگاری شده، می‌توان مقدار شناسایی ناصحیح را به‌دست آورد. در ادامه، نسبت شناسایی، که قدرت شناسایی روش را بیان می‌کند، محاسبه خواهد شد.

آزمون روش مبتنی بر میانه و مساحت نشان داده است که روش در مقابل حملات چرخش، انتقال، تغییرمقیاس و ترکیب این حملات، مقاوم است. نسبت شناسایی نیز برای دو مدل مطرح شده در روش مذکور، به ترتیب حدود ۰/۹ و ۰/۷ بدست آمد.

۳- روش بهبودیافته

روش مبتنی بر میانه و مساحت با چند مشکل مواجه شد. دلیل عمده آن، خطای محاسبات ممیزشناور است. این خطا موجب تغییر مساحت مثلث‌ها بر اساس حمله مورد استفاده می‌شود؛ به نحوی که ترتیب رشته استخراج شده بهم خورده، نسبت شناسایی کمتر از یک می‌گردد.

از سویی دیگر، همان‌طور که در فرمول (۱)[۴]، که کشیدن در راستای محور x را نشان می‌دهد، ارایه شده است، طول اضلاع مثلث در برابر حمله کشیدن مقاوم نیست. بدین صورت، محاسبات ممیزشناور، ترتیب گنجاندن در لیست

مثلث‌های انتخابی و حمله کشیدن، ترتیب گنجاندن درون هر مثلث را به چالش می‌کشند.

$$\begin{aligned} x' &= x + y\cot\theta + z\cot\phi \\ y' &= y \\ z' &= z \end{aligned} \qquad (۱)$$

برای بهبود این موضوع، به سراغ توصیف سطوح در این مدل‌ها رفتیم. از آن‌جا که هر سطح با اندیس رئوس آن توصیف می‌شود، مرتب‌سازی نزولی این اندیس‌ها می‌تواند عاملی مناسب جهت جایگزینی عامل مساحت و طول اضلاع مثلث در روش شود.

از این رو، مطابق روش قبل، مجموعه‌ای از مثلث‌ها انتخاب می‌شوند. این بار، با توجه به مقایسه ترتیب نزولی رئوس 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 (۱) می‌توان گنجاندن را سامان‌دهی کرد. جدول (۲) نیز با همین شرایط می‌تواند به منظور استخراج نهان‌نگاری مدنظر قرار گیرد.

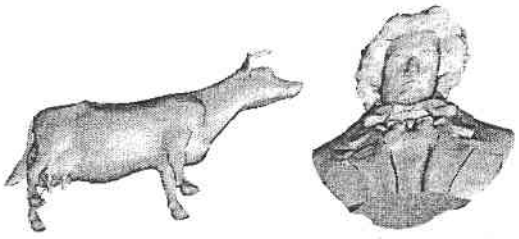
۴- پیاده‌سازی و آزمون روش

در پیاده‌سازی روش، سه برنامه در محیط ویژوال سی++ ۶,۰ به منظور گنجاندن، حمله و استخراج پیاده‌سازی گردید. دو مدل Beethoven و Cow که در روش قبلی نیز مدنظر قرار گرفته بودند، در این روش نیز استفاده شدند. گنجاندن در مدل نخست، بیش از 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 انتقال‌یافته نیز نامیده می‌شود، قرار گرفت که حاصل در شکل (۱) ارایه شده است.

در مرحله استخراج نیز، دو مثلث که دو راس مشترک و یک راس غیرمشترک دارند، به بررسی مرحله بعد می‌روند و لذا استخراج نسبت به روش قبل کمی بیشتر طول می‌کشد.

نتیجه استخراج روی هر دو مدل، بازیابی کامل تمامی تکرارهای پیام گنجانده شده و در نتیجه نسبت شناسایی یک بوده است. در جدول (۳)، نتایج دو روش برای دو مدل مقایسه شده است. برای روش اول، حمله ترکیبی چرخش، انتقال و تغییرمقیاس یک‌نواخت ارزیابی شده است و برای روش دوم به ترکیب حملات، کشیدن نیز افزوده شده است. درجه چرخش در تمام حملات، ۴۵ درجه حول بردار معین (۰/۰، ۰/۶، ۰/۸-)، فاکتور تغییرمقیاس برای سه حمله اول برابر ۰/۵ و مابقی برابر ۲، دو زاویه کشیدن برای تمام حملات ۷۵ و ۶۰ درجه و برای انتقال در حمله‌های ۱و۴، بردار T_1=(0.03,-0.04,0.08)، برای حمله‌های ۲و۵، بردار T_2=(3.0,-4.0,2.6) و برای حمله‌های ۳و۶، بردار T_3=(5.0,2.0,-8.0) مدنظر بوده است.



شکل ۱. دو مدل نهان‌نگاری شده پس از حمله

جدول (۳)، مقایسه نسبت شناسایی دو روش در شش حمله

	مقیاس	۰/۵	۰/۵	۰/۵	۲	۲	۲
	انتقال	T_1	T_2	T_3	T_1	T_2	T_3
	حمله	۱	۲	۳	۴	۵	۶
مدل ۱	روش۱	۰/۹۷	۰/۹۷	۰/۹۶	۰/۹۷	۰/۹۷	۰/۹۷
	روش۲	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰
مدل ۲	روش۱	۰/۷۳	۰/۷۵	۰/۷۴	۰/۹۰	۰/۹۱	۰/۷۹
	روش۲	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰	۱/۰

۵- نتیجه‌گیری

در این مقاله، ایده نهان‌نگاری مبتنی بر افزودن مثلثی حاوی میانه مثلث دیگر بهبود داده شد. بهبود صورت گرفته روی عامل ترتیب‌دهی مثلث‌ها در لیست مثلث‌های منتخب جهت گنجاندن که مبتنی بر مساحت بود و عامل ترتیب‌دهی درون هر مثلث که مبتنی بر طول اضلاع بود، ارایه شد. عامل مرتب‌سازی پیشنهادی، اندیس رئوس مثلث موجود در

بخش توصیف مثلث است. این عامل از حملات ترکیبی چرخش، تغییرمقیاس، انتقال و کشیدن تاثیر نمی‌پذیرد. از این‌رو، نسبت شناسایی "۱" در مرحله استخراج نهان‌نگاری بدست آمد.

درهم‌سازی مختصات رئوس را می‌توان چالشی در خصوص این روش دانست. در برابر برش نیز، مقاومت روش جای بررسی و آزمون دارد. مقاومت در برابر اعوجاج نیز با تغییر برخی شرایط ممکن خواهد بود.

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

[۱] فرید، رضا، **ارایه راهکاری جهت ارتقاء مقاومت در نهان‌نگاری مدل‌های سه‌بعدی**، پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس، تهران، دی ۸۵

[۲] فرید، رضا، مقدم، نصرا... **روشی مقاوم در نهان‌نگاری مدل‌های سه‌بعدی مثلثی مبتنی بر میانه**، دوازدهمین کنفرانس بین‌المللی انجمن کامپیوتر ایران، اسفند ۸۵

[3] Cox, Ingemar J., Miller, M. L., Bloow, J. A., *"Digital Watermarking"*, Morgan Kaufman Publishers, 2002.

[4] Angel, Edward, *"Computer Graphics"*, Addison-Wesley, 1990.

[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 Communications,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 Inter. Conf. on Image Processing (ICIP 2001), Thessaloniki, Greece, 7-10 October 2001.

[11] Meerwald, Peter, Pereira, Shelby, *"Attacks, applications and evaluation of known watermarking algorithms with Checkmark"*, SPIE Symposium, Electronic Imaging, Conf. on Security and Watermarking of Multimedia Contents IV Proceedings of SPIE, Vol. 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 Pub., Reading, WA, Nov. 1997, pp.261–272.

[14] Kalivas, A.,Tefas. A. ,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, Apr. 2003. (In ICME, 2003.)

[15] 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, (Attacks and Countermeasures), 2001.

[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] Petitcolas , Fabien A. P., Anderson, Ross J., *"Evaluation of copyright marking systems"*, Proceedings of IEEE Multimedia Systems'99, vol. 1, pp. 574-579.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] Ohbuchi, R., Mukaiyama, A., Takahashi, Sh.,*"A Frequency-Domain Approach to Watermarking 3D Shapes"*, Proc. EUROGRAPHICS 2002, (also as Computer Graphics Forum 21(3), pp. 373-382, 2002.

[25] 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, 2004, Springer.

[26] ISO/IEC 14772-1 Virtual Reality Model Language (VRML), 180, 1997. (The VRML Specification, Version 2.0, ISO/IEC WD 14772, August 4, 1996, http://www.graphcomp.com/info/specs/sgi/vrml/spec/)