ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

روش جدیدی به جهت درهم‌سازی تصاویر دیجیتال

علیرضا شاه‌حسینی، سید علی‌اصغر بهشتی شیرازی

دانشگاه علم و صنعت ایران- گروه مخابرات امن
ashahhoseini@ee.iust.ac.ir
abeheshti@iust.ac.ir

چکیده

درهم‌سازی تصاویر دیجیتال، به معنای تولید رشته‌بیتهایی وابسته به محتوا از روی تصاویر دیجیتال می‌باشد. در حالت کلی با مقایسه رشته‌های‌درهم تولیدی از روی دو تصویر می‌توان از یکسان بودن یا تفاوت ماهوی آن دو تصویر اطمینان حاصل نمود. این توابع، یکی از اصلی‌ترین ابزارهای احراز اصالت و اطمینان از دست‌نخوردگی تصاویر دیجیتال می‌باشند. درهم‌ساز تصویری پیشنهادی در این مقاله، درهم‌سازی مبتنی بر استخراج نقاط‌ویژگی تصویر و توصیف این نقاط‌ویژگی می‌باشد. در اینجا از DoG به جهت استخراج نقاط ویژگی تصویر و از یک روش توصیف مبتنی بر هیستوگرام مقادیر گرادیان روشنایی تصویر، به جهت توصیف نقاط ویژگی استفاده شده است. بررسیهای انجام شده، گویای آن است که قابلیت تفکیک تصاویر مشابه و متفاوت در رشته‌درهم‌های ۱۶۰۰ بیتی تولیدی در این مقاله، بسیار بهتر از الگوریتمهای دیگر می‌باشد. از ویژگیهای جالب الگوریتم پیشنهادی می‌توان به مقاومت بسیار خوب در برابر چرخش با زوایای مختلف تصویر و طول ثابت رشته‌درهم تولیدی اشاره نمود.

واژه‌های کلیدی

درهم‌ساز تصویری، احراز اصالت تصویر، استخراج ویژگی محلی، توصیف ویژگی، نهان‌نگاری

۱- مقدمه

در رمزنگاری بحثی تحت عنوان توابع درهم ساز وجود دارد که از آن به جهت اطمینان از صحت و دست‌نخوردگی اطلاعات و احراز اصالت اطلاعات استفاده می‌شود. این توابع بصورت یکطرفه‌ای از یک قطعه طولانی از متن اصلی، یک رشته بیتی کوتاه و معولا با طول ثابت استخراج می‌نمایند که خلاصه پیام[1] نامیده می‌شود. اگر پیام ورودی را با P و خلاصه پیام استخراج شده را با MD(P) نشان دهیم، یکطرفه بودن بودن تابع درهم ساز بدین معناست که با داشتن P به راحتی می‌توان MD(P) را محاسبه نمود اما محاسبه P با داشتن MD(P) یا بدست آوردن P' به نحوی که MD(P') = MD(P) عملا غیرممکن می‌باشد . دیگر خاصیت کلیدی این توابع، حساسیت بالای آنها به پیام می‌باشد . بدین معنا که تغییر حتی یک بیت از پیام ورودی، خروجی تابع درهم‌ساز را دچار تغییرات غیر قابل تخمین نموده و خروجی کاملا متفاوتی ایجاد می‌نماید. MD5 و SHA-1 مشهورترین این الگوریتم‌ها می‌باشند [۲] . تولید چکیده یا درهم سازی تصاویر دیجیتال ، به طرح بحث فوق برای تصویر دیجیتال می‌پردازد و امکان احراز اصالت تصویر[2] و اطمینان از دست نخوردگی و تمامیت[3] تصویر را فراهم می‌آورد. این توابع، کاربردهای متفاوت و متعددی دارند و از آنها می‌توان در طراحی الگوریتمهای واترمارکینگ اثبات‌کننده مالکیت تصاویر دیجیتال [۳-۷]، طراحی الگوریتمهای واترمارکینگ اثبات کننده اصالت تصاویر [۸-۹]، تولید کلید مبتنی بر محتوا در الگوریتم‌های نهان‌نگاری ویدئو [۱۰-۱۱] و... استفاده نمود . تنها تفاوت موجود بین این توابع و توابع درهم‌ساز مطروحه در رمزنگاری اینست که در اینجا تابع درهم ساز صرفا برای دو تصویر واقعا متفاوت، خروجی متفاوتی تولید می‌نماید و برای دو تصویر مشابه از لحاظ بیننده ، خروجی یکسانی تولید می‌گردد.

[1] Message Digest

[2] Content Authentication
[3] Integrity

به عبارت دیگر، اجرای الگوریتم درهم‌سازی بر روی تصویر اصلی و نسخ تغییر یافته آن بر اثر حملات عمدی و غیرعمدی پردازشی مانند اضافه‌کردن نویز ، هموارکردن[1] ، فیلترکردن و ... و حملات هندسی مانند برش ، چرخش و ... باید به خروجی یکسانی منجر می‌گردد . از آنجا که این توابع ، در حقیقت مشخصات ضروری تصویر را ذخیره می‌نمایند و به تغییرات قابل ادراک تصویر حساس می‌باشند، از آنها تعبیر به توابع درهم‌ساز تشخیصی[2] ، امضای دیجیتال تصویر[3] و image fingerprint نیز می‌شود.

تاکنون، الگوریتمهای درهم‌ساز تصویری بسیار متنوعی ارائه شده است. در [۱۲-۱۳] مرور جامعی بر این الگوریتمها انجام شده است. در این مقاله، بر دسته خاصی از این الگوریتمها، یعنی الگوریتمهای درهم‌سازی مبتنی بر استخراج ویژگی محلی، تمرکز شده است. تولید رشته‌درهم در الگوریتمهای درهم‌سازی مبتنی بر استخراج ویژگی، با استفاده از ویژگی‌های محلی استخراج‌شده از تصویر می‌باشد. مراد از یک ویژگی محلی، نقطه یا ناحیه‌ای از تصویر می‌باشد که متمایز از نقاط و نواحی موجود در همسایگی‌اش است. به عبارت کلی‌تر، الگوی[4] مستخرج از تصویر در آن نقطه یا ناحیه، متمایز از نقاط یا نواحی موجود در همسایگی‌اش می‌باشد. در آن نقطه یا ناحیه، شاهد تغییری بارز در یک یا چند خصیصه بصری تصویر (مانند شدت روشنایی، رنگ و بافت) می‌باشیم.

الگوریتمهای Dittman [۱۴]، Monga [۱۵]، Bhattecharjee [۱۶] و Lu [۱۷] ، اهم الگوریتمهای مبتنی بر استخراج نقطه‌ویژگی می‌باشند که تاکنون پیشنهاد شده است. تقریبا همه این الگوریتمها، الگوریتمهایی با مقاومت بسیار کم و شکنندگی بسیار بالا می‌باشند و رشته‌درهم‌هایی با طول غیرثابت تولید می‌نمایند. در این میان، تنها الگوریتم Lu می‌باشد که مقاومت بهتری دارد. به همین دلیل، الگوریتم پیشنهادی را با این الگوریتم مقایسه نموده‌ایم.

در ادامه، ابتدائا بحث مختصری در باب الزامات یک تابع درهم‌ساز تصویری انجام شده است و سپس به تبیین الگوریتم پیشنهادی و بررسی مشخصات آن پرداخته شده است.

۲- الزامات یک تابع درهم‌ساز تصویری

بنا به تعریف، یک درهم‌ساز تصویری، تابعی است که $I \in F$ (که در آن، F مجموعه تمام تصاویر طبیعی دارای ابعاد محدود می‌باشد) و کلید اختیاری k را به عنوان ورودی پذیرفته و رشته باینری hash=H(I,k) را در خروجی خود تولید می‌نماید.

در حالت کلی، دو رشته درهم را یکسان گویند هرگاه فاصله همینگ نرمالیزه آنها (تعداد بیتهای متفاوت دو رشته‌بیت بخش بر میانگین طول آنها) کوچکتر از حد آستانه α باشد و آنها را متفاوت گویند هرگاه این مقدار بزرگتر از حدآستانه β باشد. اگر I_{ident}، تصویری مشابه تصویر I و I_{diff}، تصویری متفاوت از تصویر I باشد و $0<\theta_1,\theta_2<1$ دو پارامتر دلخواه باشند و فاصله همینگ نرمالیزه دو رشته بیت h_1 و h_1 را با $D_H(h_1,h_2)$ نشان دهیم، مشخصات لازم برای یک تابع درهم ساز تصویری ایده‌آل به قرار زیر خواهد بود:

۱ . مقاومت[5] : به معنای تولید رشته‌های درهم یکسان بازای تصاویر مشابه می‌باشد. به عبارت فنی‌تر، در یک درهم‌ساز ایده‌آل داریم:

(۱)

$$P\{\ D_H[H(I,k),H(I_{Ident},k)]<\alpha\ \}\geq 1-\theta_1$$

یک درهم‌ساز ایده‌آل باید در برابر تمام حملاتی که ماهیت تصویر را تغییر نمی‌دهد مقاوم بوده و رشته‌درهم یکسانی را تولید نماید.

۲ . شکنندگی[6] : به معنای تولید رشته خروجی کاملا متفاوت بازای تصاویر غیرمشابه می‌باشد. به عبارت دیگر، در یک درهم‌ساز ایده‌آل داریم:

$$P\{\ D_H[H(I,k),H(I_{diff},k)]>\beta\ \}\geq 1-\theta_2 \qquad (۲)$$

یک درهم‌ساز ایده‌آل باید بتواند بین تصاویر مختلف (فرضا یک تصویر و نسخ تحریف‌شده آن) تمایز قایل شود.

۳ . امن‌بودن[7] : امنیت یک الگوریتم درهم‌سازی به معنای یکطرفه‌بودن[8] و مقاومت در برابر تصادم[9] آن الگوریتم می‌باشد. یکطرفه بودن یک درهم‌ساز تصویری بدین معناست که نمی‌توان از روی رشته‌درهم موجود، تصویری با رشته‌درهم یکسان تولید نمود. مقاومت در برابر تصادم یک درهم‌ساز نیز بدین معناست که با اطلاع از یک تصویر و رشته درهم معادل آن، نمی‌توان تصویری با رشته درهم یکسان تولید نمود. بعضا از این خاصیت تعبیر به تصادفی‌بودن یا غیرقابل تخمین بودن[10] رشته درهم‌ساز شده است[۱۲] و عنوان شده است که یک تابع‌درهم‌ساز تصویری ایده‌آل ، تابعی است که رابطه :

$$P\{\ H(I,k)=v\ \}\approx\frac{1}{2^q}\quad \forall v\in\{0,1\}^q \qquad (۳)$$

[1] Smoothing
[2] Perceptual Hash
[3] Image Signature
[4] Pattern

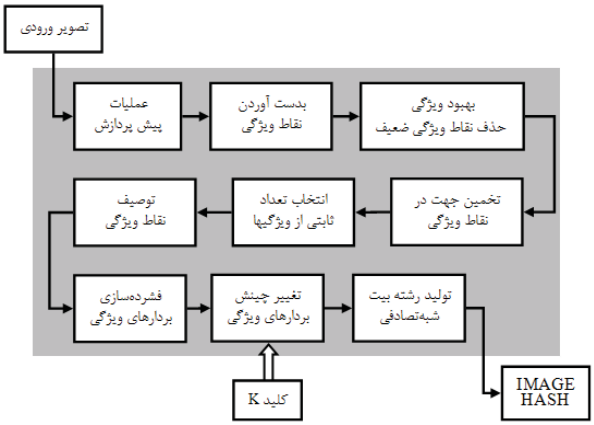
[5] Robustness
[6] Fragility
[7] Security
[8] One way Property
[9] Collision Resistance
[10] Unpredictability

در مورد آن صادق می‌باشد. اگرچه برخی مبتنی بر کلید بودن را یک شرط الزامی برای امنیت الگوریتم دانسته‌اند [۱۳]، اما الگوریتمهای درهم‌سازی غیرمبتنی بر کلیدی نیز موجود می‌باشد.

اینکه آیا امکان طراحی تابع درهم ساز تشخیصی براورده کننده سه شرط فوق وجود دارد یا نه (در یک زمان معقول) یک مسأله حل نشده است [۱۵] و هیچ کس در باب آن ادعا نکرده است وتاکنون هیچ سیستمی که سه شرط فوق را بازای θ_1, θ_2 و q مشخص و دلخواه براورده کند، ارائه نشده است. نکته مهم دیگر اینست که سه شرط فوق دارای همپوشانی و تداخل معانی می‌باشند و الگوریتم‌های درهم‌سازی باید موازنه‌ای بین این شروط برقرار نمایند.

۳- الگوریتم پیشنهادی

ساختار کلی الگوریتم درهم‌سازی پیشنهادی، در شکل ۱ نشان داده شده است. این ساختار، ساختاری متشکل از نه تابع پیش‌پردازش، استخراج نقاط ویژگی، بهبود ویژگی و حذف نقاط ویژگی ضعیف، تخمین جهت در نقاط ویژگی، انتخاب تعداد ثابتی از نقاط‌ویژگی، توصیف نقاط‌ویژگی، فشرده‌سازی بردارهای ویژگی، مبتنی بر کلید کردن چینش بردارهای ویژگی و تولید رشته‌بیت تصادفی می‌باشد و رشته درهمی با طول ثابت ۱۶۰۰ بیت تولید می‌نماید. ذیلا به تبیین این توابع پرداخته شده است.



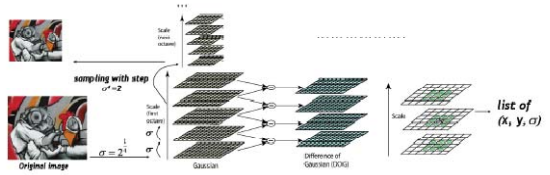
شکل ۱: ساختار کلی الگوریتم پیشنهادی

الف) عملیات پیش‌پردازش

در این مرحله یک سری عملیات پیش‌پردازش انجام می‌شود که درکل، تاثیر بسیار مثبتی بر عملکرد هر الگوریتم درهم‌سازی دارد [۱۵و۱۷]. تبدیل تصویر ورودی، به تصویری با ابعاد 256×256، تبدیل تصویر رنگی ورودی به تصویری با سطوح خاکستری، اصلاح هیستوگرام و استفاده از روشهای کاهش نویز از جمله این عملیات می‌باشد.

ب) استخراج نقطه ویژگی

استخراج نقطه‌ویژگی، یکی از مطرح‌ترین بحثهای عرصه پردازش تصویر، در طی ۵۰ سال گذشته و یکی از مهمترین اجزای ساختار پیشنهاد شده در این مقاله می‌باشد. بخش عمده‌ای از عملکرد این ساختار، مرهون استفاده از یک تابع استخراج نقطه‌ویژگی مناسب می‌باشد. شمایی کلی از تابع استخراج نقطه ویژگی استفاده شده در این مقاله، در شکل ۲ نشان داده شده است. از این الگوریتم، در [۲۰] و [۲۱] به جهت تشخیص‌شیء و تطبیق‌تصاویر استفاده شده است.



شکل ۲: شمایی از چگونگی استخراج نقطه‌ویژگی در الگوریتم پیشنهادی [۲۱]

گام اول در استخراج نقاط ویژگی، محاسبه نمایش مکان‌مقیاس تصویر می‌باشد. برای محاسبه هر سطح از نمایش مکان‌مقیاس در اینجا، از امتزاج تصویر اصلی با یک هسته گاوسی متقارن استفاده شده است. سطح اول یا سطح پایینی این نمایش، نتیجه امتزاج تصویر اصلی با یک هسته گاوسی با واریانس σ_0^2 می‌باشد. هر سطح بعدی نمایش نیز از امتزاج سطح قبلی نمایش با یک هسته گاوسی با واریانس s^2 بدست آمده است. به بیانی دیگر می‌توان گفت که سطح n ام در نمایش مکان مقیاس یک تصویر، نتیجه امتزاج تصویر اصلی با یک هسته گاوسی با انحراف استاندارد $\sigma_n = \sigma_0 s^n$ می‌باشد.

به جهت کاهش بار محاسباتی تولید نمایش مکان‌مقیاس، معمولا به موازات افزایش ضریب مقیاس در نمایش مکان-مقیاس، نرخ نمونه‌برداری کاهش داده می‌شود. از چنین نمایش مکان‌مقیاسی اغلب تحت عنوان هرم مکان‌مقیاس نام برده می‌شود در حالت کلی، کاهش نرخ نمونه‌برداری باید بگونه‌ای باشد که منجر به aliasing نگردد. برای این منظور بعد از هر Octave (دو برابر شدن ضریب مقیاس) از تصویر اصلی، نرخ نمونه‌برداری، 1/2 شده است و در فاصله هر Octave، نرخ نمونه‌برداری بلاتغییر مانده است. در ادامه، همانطور که در شکل ۲ نیز نشان داده شده است، با محاسبه تفاضل هر سطح از نمایش با سطح قبلی آن، نمایش مکان‌مقیاس با هسته DoG تصویر، تولید می‌شود و نقاط اکسترمم این نمایش مکان‌مقیاس، به عنوان نقطه‌ویژگی معرفی می‌شود. مراد از یک نقطه‌ویژگی در اینجا، نقطه‌ای است که قدرمطلق مقدار آن، بزرگتر از قدرمطلق مقدار۲۶ نقطه موجود در همسایگی آن نقطه در هرم DoG تصویر می‌باشد.

ج) حذف نقاط ویژگی ضعیف

نقاط ویژگی قرار گرفته برلبه‌های تصویر، نقاط ویژگی بسیار ناپایداری بوده و به مقادیر بسیار کوچک نویز به شدت حساس باشد [۲۰]. برای حل مشکل و بهبود نتایج، نیازمند یک مرحله فیلترکردن اضافی می‌باشیم تا نقاط قرار گرفته بر لبه‌های تصویر (که شائبه ناپایدار بودن آنها وجود دارد) را حذف نماییم. مشخصه بارز این نقاط این است که در آنها صرفا در یک جهت شاهد تغییر می‌باشیم. در این نقاط ، مقدار انحنا[1] در جهت لبه، مقداری بزرگ و مقدار انحنا در جهت عمود بر آن، مقداری کوچک می‌باشد. این دو مقدار انحنا را می‌توان از روی ماتریس Hessian محاسبه شده در مختصات و مقیاس نقطه‌ویژگی که فرمی بصورت:

$$H=\sigma^2\begin{bmatrix} L_{xx}(x,y,\sigma) & L_{xy}(x,y,\sigma) \\ L_{xy}(x,y,\sigma) & L_{yy}(x,y,\sigma)\end{bmatrix} \qquad (٤)$$

دارد، محاسبه نمود. مقادیر ویژه این ماتریس، مقدار انحنا در جهت و عمود بر جهت لبه در مختصات مورد بحث می‌باشد[۱۸]. ما در اینجا نیازی به محاسبه مقادیر ویژه نداریم. صرفا باید نسبت مقادیر ویژه را مورد بررسی قرار دهیم. با استفاده از جبرخطی ثابت می‌شود که:

$$\begin{aligned} Trace(H) &= L_{xx}+L_{yy}=\alpha+\beta \\ Det(H) &= L_{xx}L_{yy}-(L_{xy})^2=\alpha\beta \end{aligned} \qquad (٥)$$

α در این رابطه، مبین مقدار ویژه بزرگتر ماتریس H و β مبین مقدار ویژه کوچکتر آن می‌باشد. با تعریف $r=\alpha/\beta$ ، خواهیم داشت:

$$\frac{Trace(H)^2}{Det(H)}=\frac{(\alpha+\beta)^2}{\alpha\beta}=\frac{(r+1)^2}{r} \qquad (٦)$$

در صورتی که مقادیر ویژه ماتریس H یکسان باشند، این نسبت، حداقل مقدار خود را دارا می‌باشد و با افزایش r ، مقدار آن افزایش می‌یابد. حداکثر r مجاز منظور شده در اینجا برابر ۱۰ می‌باشد و نقاط ویژگی با r بزرگتر از ۱۰، به عنوان نقاط ویژگی قرار گرفته بر روی لبه منظور شده و حذف شده‌اند.

د) تخمین جهت در نقطه‌ویژگی

در این مرحله اجرایی از الگوریتم، به هر نقطه‌ویژگی یک مولفه θ (مبین جهت در نقطه‌ویژگی) نسبت داده می‌شود. برای محاسبه θ در یک نقطه ویژگی، ابتدا سطح L(x,y) از نمایش مکان‌مقیاس تصویر که ضریب مقیاس آن به مولفه مقیاس آن نقطه‌ویژگی نزدیکتر می‌باشد، انتخاب می‌شود. این کار باعث می‌شود که محاسبات در یک فضای ناوردا در برابر تغییر مقیاس صورت گیرد. اندازه $m(x,y)$ و جهت $\theta(x,y)$ گرادیان تصویر در هر پیکسل از تصویر L(x,y) را می‌توان با استفاده از روابط:

$$\begin{aligned} m(x,y) &= [(L(x+1,y)-L(x-1,y))^2+ \\ &\quad (L(x,y+1)-L(x,y-1))^2]^{0.5} \\ \theta(x,y) &= \tan^{-1}\left(\frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)}\right) \end{aligned} \qquad (٧)$$

محاسبه نمود. در اینجا برای بدست آوردن جهت در هر نقطه-ویژگی، از هیستوگرام مقادیر $\theta(x,y)$ واقع در دایره‌ای به شعاع $1.5s$ (s، مقیاس اشکارسازی نقطه‌ویژگی) به مرکز آن نقطه‌ویژگی استفاده شده است. هیستوگرام مورد استفاده در اینجا، دارای۳۶ ناحیه می‌باشد. در حالتی‌که بازای یک (x,y) واقع در همسایگی یک نقطه ویژگی، $\theta(x,y)$ مقداری بین $10\times(n-1)$ و $10\times n$ درجه داشته باشد، ناحیه nام هیستوگرام وزن‌دهی شده است. مقدار این وزن‌دهی، متناسب با حاصلضرب $m(x,y)$ و پنجره گاوسی دایروی به مرکز نقطه‌ویژگی و انحراف استاندارد برابر با $1.5s$ می‌باشد. زاویه متناظر با ناحیه‌ای از هیستوگرام که بیشترین مقدار را دارد، به عنوان تخمینی از جهت اصلی تصویر در نقطه‌ویژگی، منظور شده است. تخمین جهت در نقاط ویژگی، چهارمین گام اجرایی الگوریتم پیشنهادی می‌باشد. از این پارامتر، در ارائه توصیف ناوردا نسبت به چرخش از نقطه‌ویژگی استفاده شده است.

ه) انتخاب تعداد ثابتی از ویژگیها

تا این مرحله از الگوریتم، تعداد متغیری ویژگی انتخاب شده است و به هر یک زوج مرتبی به فرم (x,y,s,θ) تخصیص داده شده است. در این مرحله، از میان تعداد غیرثابت ویژگی تولیدشده، ۵۰ ویژگی که اساسی‌تر می‌باشند و مقیاس آشکارسازی آنها بزرگتر می‌باشد، انتخاب شده است. بررسیهای انجام شده [۱] گویای آن است که انتخاب تعداد کمتر نقطه-ویژگی، منجر به کاهش شکنندگی الگوریتم و انتخاب تعداد بیشتر نقطه‌ویژگی، منجر به کاهش مقاومت الگوریتم می‌گردد.

و) توصیف نقاط ویژگی

توصیف نقاط ویژگی ، دیگر کار انجام شده در الگوریتم پیشنهادی می‌باشد. در اینجا هر نقطه ویژگی استخراج شده، با توجه به مختصات اطرافش توصیف می‌شود. در روش توصیف ویژگی استفاده شده در طرح پیشنهادی، هر نقطه ویژگی با یک بردار ۱۲۸تایی توصیف می‌شود. در بررسی صورت گرفته در [۱۹] نشان داده شده است که این روش توصیف نقطه‌ویژگی که برای اولین بار در [۲۰] مورد استفاده قرار گرفته، یکی از

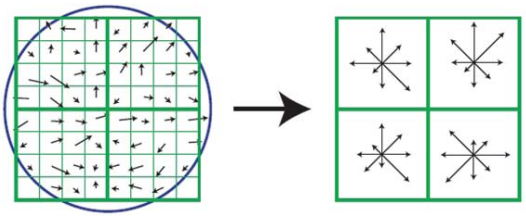
[1] Curvature

بهترین روشهای توصیف نقطه‌ویژگی قابل استفاده در تطبیق-تصاویر[1] می‌باشد.

در اینجا ابتدا بازای هر نقطه‌ویژگی، سطح L(x,y) از نمایش مکان‌مقیاس تصویر که ضریب مقیاس آن به مولفه مقیاس آن نقطه‌ویژگی (s) نزدیکتر می‌باشد، انتخاب شده است و سپس تصاویر $m(x,y)$ و $\theta(x,y)$ متناظر با تصویر L(x,y)، با استفاده از رابطه ۷ محاسبه شده و تصویر $m(x,y)$، با استفاده از یک پنجره گاوسی دایروی به مرکز نقطه‌ویژگی و انحراف استاندارد برابر با $r/2$ ، پنجره شده است و تصویر $n(x,y)$، تولید شده است.

توصیف نقطه‌ویژگی ارائه شده در اینجا، توصیفی ناوردا نسبت به چرخش می‌باشد. در اینجا از دستگاه مختصاتی به مرکزیت نقطه‌ویژگی استفاده شده است. محور xهای این دستگاه مختصات، محور با زاویه θ از افق و محور yهای این دستگاه مختصات، محور با زاویه $\theta+90$ از افق می‌باشد. هر یک از نقاط ویژگی، با استفاده از مقادیر اندازه‌گرادیان پنجره‌شده n(x,y) و زاویه گرادیان $\theta(x,y)$ در $r\times r$ نقطه با فاصله یکنواخت موجود در ناحیه مربعی $\{(x',y')|\ -r<x'<r\ ,\ -r<y'<r\}$ از دستگاه مختصات متناظر با آن نقاط‌ویژگی، توصیف شده است. بنابراین، تا این مرحله توانسته‌ایم هر نقطه‌ویژگی را با یک ماتریس $r\times r$ حاوی مولفه‌های مختلط، توصیف نماییم. این امر در شکل ۳-الف نشان داده شده است.همانطور که مشاهده می‌شود، در این شکل، r برابر ۸ می‌باشد و از ۶۴ بردار دو بعدی برای توصیف نقطه‌ویژگی، استفاده شده است. دایره نشان داده شده در این شکل، نمادی از پنجره گاوسی استفاده شده می‌باشد.

در ادامه، ماتریس $r\times r$ حاصله به بلوکهای ناهمپوشان 4×4 تقسیم شده و هیستوگرام هر بلوک محاسبه می‌شود. خطوط پررنگ در شکل ۳-الف نشان‌دهنده مرز بلوکهای 4×4 می-باشد. شکل ۳- ب نشان‌دهنده نحوه محاسبه هیستوگرام در هر بلوک می‌باشد. هیستوگرام محاسبه شده در اینجا، متشکل از ۸ ناحیه می‌باشد. درصورتی که زاویه مولفه سطر i ام و ستون j ام بلوک



(ب) (الف)

شکل ۳: شمایی از عملکرد الگوریتم توصیف ویژگی

$(\angle a_{ij})$، مقداری بین $45\times(n-1)$ و $45\times n$ درجه داشته باشد، ناحیه n ام هیستوگرام (که در هیستوگرام‌های شکل ۳- ب با برداری با زاویه $45\times n$ از افق نشان داده شده است) وزن‌دهی می‌شود. مقدار این وزن‌دهی، متناسب با $|a_{ij}|$ (اندازه مولفه سطر i ام و ستون j ام بلوک) می‌باشد. بنابراین در حالت کلی، هر مولفه بلوک، موجب وزن‌دهی تنها یکی از نواحی هیستوگرام متناظر با آن بلوک می‌گردد. با توجه به اینکه در اینجا هر بلوک 4×4، با یک بردار به طول ۸ توصیف شده است، هر نقطه ویژگی، توصیفی بطول $8\times(r/4)\times(r/4)$ خواهد داشت. با توجه به انتخاب r=16 در پیاده‌سازی انجام شده، طول بردار توصیف‌کننده هر نقطه‌ویژگی برابر ۱۲۸ می‌باشد.

ز) فشرده‌سازی بردارهای ویژگی

تا این مرحله، هر نقطه ویژگی با یک بردار بطول ۱۲۸ توصیف شده است. در این مرحله سعی شده است تا به نوعی طول این بردار کاهش یابد. در این مرحله، از تبدیل DWT که یکی از متداولترین روشهای کاهش طول بردار ویژگی می‌باشد، استفاده شده است. در اینجا با دوبار اعمال تبدیل موجک و درنظرگرفتن مولفه‌های تقریب، بردارهای ۱۲۸ مولفه‌ای توصیف‌کننده، به بردارهایی بطول ۳۲ تبدیل شده است. بررسیهای [۱] گویای مناسب بودن این درجه از فشرده‌سازی می‌باشد.

ح) چینش مبتنی بر کلید

این مرحله، اختیاری بوده و Hash تصویری را به یک MAC تصویری تبدیل می‌نماید. در مقالات، تاکید زیادی بر مبتنی بر کلید بودن پروسه درهم‌سازی وجود دارد. در اینجا با استفاده از یک کلید تصادفی، چینش عناصر بردارهای ویژگی بدست آمده را تغییر می‌دهیم. این کار سبب پیچیده‌تر شدن و مبتنی بر کلیدشدن ارتباط بین خروجی و ورودی تابع درهم‌ساز می‌گردد.

ط) فاز نهایی

در این مرحله، مولفه‌های هر یک از بردارهای توصیف کننده ویژگی بدست آمده تا این مرحله، با مقدار میانه‌اش مقایسه می‌شود و در صورتی که مقدار یک مولفه بردار بزرگتر از مقدار میانه‌بردار باشد، آن مولفه با ۱ و در صورتی که مقدار مولفه کوچکتر از مقدار میانه بردار باشد، آن مولفه با صفر جایگزین می‌شود. به عبارت دیگر، هر یک از بردارهای ۳۲ مولفه‌ای موجود، به یک رشته ۳۲ بیتی تصادفی تبدیل می‌شود. در اینجا ما ۵۰ رشته ۳۲بیتی داریم که هریک از آنها حاوی تعداد برابری صفر و یک می‌باشد و توصیفی از یک نقطه‌ویژگی ارائه می‌دهد. رشته‌درهم ۱۶۰۰ بیتی نهایی، از چینش کنارهم این ۵۰ رشته ۳۲بیتی بدست می‌آید.

[1] Image Matching

۴- ارزیابی الگوریتم پیشنهادی

در این بخش از گزارش، به بررسی عملکرد الگوریتم پیشنهادی پرداخته شده است. تمام بررسیهای این فصل، بر روی پنجاه تصویر طبیعی موجود در پایگاه داده USC-SIPI [۲۲] انجام شده است و از نرم‌افزار Matlab برای پیاده‌سازی الگوریتمها، مقایسه نتایج و رسم نمودارها استفاده شده است. در این قسمت از مقاله، عملکرد الگوریتم پیشنهادی، با عملکرد دو الگوریتم Mihcak [۲۳] و Lu [۱۷] مقایسه شده است. نتایج گزارش شده توسط مولفین، گویای آن است که در بین الگوریتمهای مبتنی بر استخراج نقطه‌ویژگی موجود، تنها الگوریتم Lu از مقاومت قابل قبولی برخوردار می‌باشد. الگوریتم Mihcak نیز یکی از معروف‌ترین و مقاوم‌ترین الگوریتمهای غیرمبتنی بر استخراج نقطه‌ویژگی موجود می‌باشد. دلیل مقایسه الگوریتم پیشنهادی با این دو الگوریتم، همین می‌باشد.

در حالت کلی، فاصله همینگ نرمالیزه بین رشته‌های درهم تولید شده توسط یک الگوریتم درهم‌سازی، متداولترین معیار براورد عملکرد آن الگوریتم درهم‌سازی می‌باشد. بنا به تعریف، فاصله همینگ نرمالیزه بین دو رشته بیت، تعداد بیتهای متفاوت آن دو رشته‌بیت بخش بر میانگین طول آنها می‌باشد. این معیار را نمی‌توان مستقیما در مورد الگوریتمهای مبتنی بر استخراج نقطه‌ویژگی بکار برد. علت این است که رشته درهم تولیدی در الگوریتمهای مبتنی بر استخراج نقطه‌ویژگی، رشته-درهم تولیدی، یکتا نمی‌باشد. در این الگوریتمها، ابتدا تعدادی نقطه‌ویژگی استخراج می‌شود و سپس هر نقطه‌ویژگی با یک رشته‌بیت با طول مشخص (فرضا ۶۴ بیت در الگوریتم Lu)، توصیف می‌شود. رشته‌درهم نهایی در این الگوریتمها، از کنارهم قرار دادن این رشته‌بیتهای توصیف‌کننده نقاط ویژگی، تولید می‌شود. برای مقایسه دو رشته‌درهم در اینجا، ابتدا باید رشته بیتهای توصیف‌کننده معادل، تعیین شود. دو رشته‌بیت توصیف-کننده معادل، دو رشته‌بیت توصیف‌کننده‌ای می‌باشند که فاصله همینگ نرمالیزه بین آنها، کوچکتر از حد آستانه ۰.۱۵و کوچکتر از فاصله همینگ نرمالیزه بین آن رشته‌بیت و دیگر رشته‌بیتهای توصیف کننده مستخرج از رشته‌درهم دوم می‌باشد. در ادامه، چینش یکسانی را در در مورد رشته‌بیتهای توصیف‌کننده در دو رشته درهم، اعمال می‌نماییم بگونه‌ای که رشته‌بیتهای توصیف‌کننده معادل در دو رشته‌درهم ، موقعیت یکسانی داشته باشند. فاصله همینگ نرمالیزه بین رشته‌های درهم تولید شده توسط یک الگوریتم درهم‌سازی مبتنی بر استخراج نقطه‌ویژگی، فاصله همینگ نرمالیزه بین این دو رشته-درهم می‌باشد.

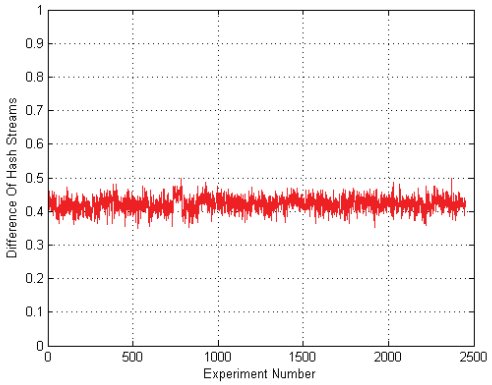
مطلوب ما این است که فاصله همینگ نرمالیزه بین رشته‌های درهم مستخرج از دو تصویر متفاوت نیز مقداری نزدیک ۰.۵ داشته باشد. نزدیک ۰.۵ بودن این مقدار را می‌توان به منزله تصادفی بودن خروجی درهم‌ساز نیز تفسیر نمود. با مشاهده شکل ۴، می‌توان به عملکرد مطلوب‌تر الگوریتم پیشنهادی در تشخیص تصاویر متفاوت، پی برد. این شکل، از مقایسه ۲۴۵۰ زوج تصویر متفاوت تولید شده است. همانطورکه مشاهده می‌شود، الگوریتم پیشنهادی دارای عملکرد مطلوبی می‌باشد.

از طرف دیگر، مبتنی بر کلید کردن فرایند تولید رشته‌درهم، منجر به پیچیده‌تر شدن رابطه بین رشته‌درهم و تصویر، افزایش میزان "غیرقابل تخمین بودن" رشته‌درهم و نتیجتا افزایش امنیت الگوریتم می‌گردد.

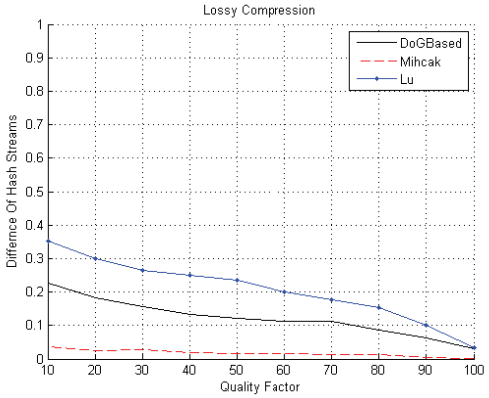
شکلهای ۷،۶،۵ و ۸ به ترتیب نشان‌دهنده مقاومت الگوریتم پیشنهادی، دربرابر حملات فشرده‌سازی باتلف، نویز، فیلتر میانه و چرخش می‌باشند. محور عمودی در این شکلها، فاصله همینگ نرمالیزه بین تصویر اصلی و تصویر تغییریافته بر اثر حمله را نشان می‌دهد. همانطور که مشاهده می‌شود، مقاومت الگوریتم پیشنهادی، در همه موارد مطلوب‌تر از مقاومت الگوریتم Lu می‌باشد. این در حالی است مقاومت الگوریتم پیشنهادی در برابر حملات پردازشی مانند اضافه‌کردن نویز، فشرده‌سازی باتلف و فیلتر کردن، کمتر از مقاومت الگوریتم Mihcak می‌باشد. با این وجود، شکل ۸ نشان می‌دهد که مقاومت الگوریتم پیشنهادی در برابر حملاتی مانند چرخش، بسیار بیشتر از مقاومت الگوریتم Mihcak می‌باشد.

مسأله احراز اصالت تصویر را می‌توان یک مسأله آزمون فرضیه دو فرضی دانست و قابلیت یک الگوریتم درهم‌سازی در تمیزدادن تصاویر مشابه و متفاوت را می‌توان متناظر با قابلیت آن الگوریتم در طبقه‌بندی مناسب تصویر دریافتی دانست. نمودار ROC ، نموداری است که با نشان‌دادن رابطه بین احتمال تشخیص صحیح شباهت دو تصویر (P_D) و احتمال عدم تشخیص تفاوت دو تصویر (P_F) ، مقایسه عملکرد الگوریتمهای درهم‌سازی را به بهترین وجه، ممکن می‌سازد [۱۵]. در شکل ۹ ، نمودار ROC الگوریتم پیشنهادی، با نمودار ROC الگوریتمهای Lu و Mihcak مقایسه شده است. برای رسم این نمودار، از ۲۴۵۰ مقایسه بین رشته‌درهم‌های حاصله از تصاویر متفاوت و ۱۸۴۰۰ مقایسه بین رشته‌درهم‌های حاصله از تصاویر مشابه استفاده شده است. از این شکل مشاهده می‌شود که الگوریتم پیشنهادی، بهترین عملکرد را در تفکیک تصاویر مشابه و متفاوت، از خود نشان می‌دهد. در جدول ۱، مقایسه‌ای کیفی بین این الگوریتم و دیگر الگوریتمهای نامبرده شده در این مقاله انجام شده است. این جدول بر اساس بررسیهای انجام شده در این بخش ، نتایج گزارش شده توسط نویسندگان مقالات و دیگر نویسندگان و شبیه‌سازیهای مجدد انجام شده، تنظیم شده است. این جدول، گویای موفقیت الگوریتم

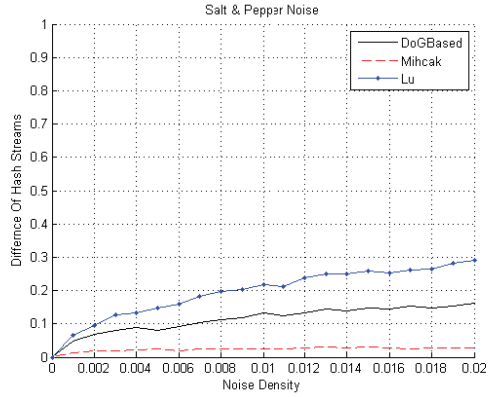
پیشنهادی، در تولید یک رشته‌درهم مبتنی بر استخراج نقطـه-ویژگی مقاوم، امن ، شکننده و با طول ثابت می‌باشد.



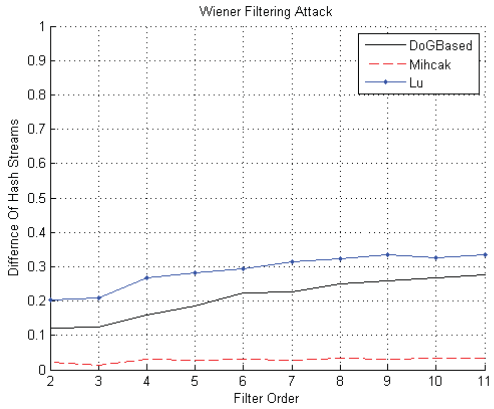
شکل۴: فاصله همینگ بین رشته درهم‌های مستخرج از تصاویر متفاوت



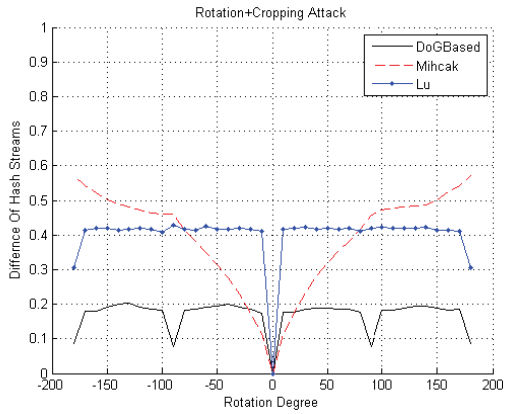
شکل۵: مقاومت الگوریتم در برابر فشرده‌سازی باتلف با کیفیتهای مختلف



شکل۶: مقاومت الگوریتم در برابر نویز فلفل نمکی با واریانسهای مختلف



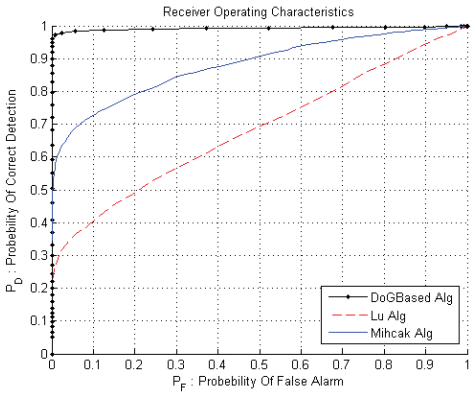
شکل۷: مقاومت الگوریتم در برابر فیلتر میانه از درجه‌های مختف



شکل۸: مقاومت الگوریتم در برابر چرخش با زوایای مختلف

جدول ۱: مقایسه کیفی الگوریتمهای پیشنهادی و دیگر الگوریتمهای درهم سازی موجود

	مقاومت	شکنندگی	امنیت	طول رشته درهم
الگوریتم Mihcak	متوسط	متوسط	متوسط	۱۰۲۴ بیت
الگوریتم Dittman	ضعیف	خوب	خوب	متغیر
الگوریتم Bhattacharjee	ضعیف	خوب	متوسط	متغیر
الگوریتم Mouga	متوسط	خوب	متوسط	متغیر
الگوریتم Lu	متوسط	متوسط	خوب	متغیر
الگوریتم مبتنی بر DOG پیشنهادی	خوب	خوب	خوب	۱۶۰۰بیت



شکل۹: مقایسه نمودار ROC الگوریتمهای درهم‌سازی مختلف

۵- نتیجه‌گیری

در این مقاله، یک الگوریتم درهم‌سازی مبتنی بر استخراج نقطه-ویژگی جدید پیشنهاد داده شد و نشان داده شد که این الگوریتم، از مقاومت، شکنندگی و امنیت مناسبتری در مقایسه با الگوریتمهای مبتنی بر استخراج نقطه‌ویژگی موجود و بسیاری از الگوریتمهای غیرمبتنی بر استخراج نقطه‌ویژگی موجود، برخوردار می‌باشد (جدول۱). مقاومت بسیار مناسب در برابر چرخش با زوایای مختلف تصویر (حداکثر تغییر برابر با ۰.۲)، طول ثابت ۱۶۰۰ بیتی رشته‌درهم و تصادفی بودن آن را می‌توان از ویژگیهای بارز الگوریتم پیشنهادی دانست.

مراجع

[۱] علیرضا شاه‌حسینی "طراحی و پیاده‌سازی یک درهم‌ساز مقاوم و امن تصاویر دیجیتال" پایان‌نامه کارشناسی ارشد دانشگاه علم و صنعت ایران ۱۳۸۸.

[2] " Cryptography : Theory & Practice " 3e , By : D.Stinson , Chapman & hall , 2006.

[3] H.Sencar , N.Memon , " Combatting ambiguty attacks via selective detection of embedded watermarks " , IEEE Trans. On Information Forensics & Security , Vol.2 , No.4 , DEC 2007 .

[4] H.Sencar , N.Memon , " Watermarking & ownership problem : a revisit " , DRM 05 , Nov 2005.

[5] C.Lu , S.Sun , P.Chang , " Robust hash-based image watermarking with resistance to geometric distortions and watermark-estimation attacks " SPIE-IS&T Electronic Imaging Vol.5681 , 2005 .

[6] C.Lu , C.Yu , " On the security of mesh-basedmedia hash-dependent watermarking against protocol attacks " , IEEE Conf , 2005 .

[7] C.Lu , S.Sun , C.Hsu , P.Chang , " Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection " , IEEE Trans . on Multimedia , Vol.8 , No 4 , Aug 2006 .

[8] J. Cannons and P. Moulin, “Design and statistical analysis of a hash aided image watermarking system,” IEEE Trans. Image Process., vol.13, no. 10, pp. 1393–1408, Oct. 2004.

[9] L. Xie and G. R. Arce, " A class of authentication digital watermarks for secure multimedia communication " , IEEE Trans. on Image Processing, vol. 10, pp. 1754-1764, Nov. 2001.

[10] B.Coskum , B.Sankur , N.Memon , " Spatio-Temporal transform based video hashing " , IEEE Trans. On Multimedia , Vol. 8 , No. 6 , DEC 2006.

[11] C.Roover , C.Vleechouwer , F.Lefebvre , B.Macq " Robust video hashing based on radial projections of key frames " , IEEE Trans. on Signal Processing , Vol.53 , No.10 ,Oct 2005.

[12] S.Wang , X.Zhang , "Recent developments of perceptual image hashing" ,Journal Of Shanghai University, 2007.

[13] S.Han , C.H.Chu , S.Yang , 'Content-Based Image Authentication: Current Status, Issues, and challenges",IEEE International Conference Of Semantic Computing, 2007.

[14] J.Dittman, A. Steinmetz, and R. Steinmetz, “Content based digital signature for motion picture authentication and content-fragile watermarking”, Proc. IEEE Int. Conf. Multimedia Computing and Systems, pp. 209–213,1999.

[15] V.Monga , B.Evans , " Perceptual image hashing via feature points : Performance Evaluation and Tradeoffs " , IEEE Trans . on Image Processing , Vol 15, No.11 , Nov 2006 .

[16] S.Bhatacherjee , M.Kutter, “ Compression tolerant image authentication ” , presented at the IEEE Conf. Image Processing, 1998.

[17] C.-S. Lu, C.-Y. Hsu , " Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication",Journal Of Multimedia Systems ,2005.

[18] C. Harris and M. Stephens, “A combined corner and edge detector,” in Alvey Vision Conference, pp. 147–151, 1988.

[19] K. Mikolajczyk and C. Schmid, “A performance evaluation of local descriptors,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 10, pp. 1615–1630, 2005.

[20] D. G. Lowe. Object recognition from local scale-invariant features. In Proceedings of the 7th International Conference on Computer Vision, Kerkyra, Greece, 1999.

[21] D. Lowe, “Distinctive image features from scale-invariant keypoints,” International Journal of Computer Vision, vol. 2, no. 60, pp. 91–110, 2004.

[22] "USC-SIPI database" , http://sipi.usc.edu/database/, 2004.

[23] K. Mihcak and R. Venkatesan, " New iterative geometric techniques for robust image Hashing " , Proc. ACM Workshop on Security and Privacy in Digital Rights Manage-ment, pp. 13-21, Nov. 2001.