نشریه علمی‌ترویجی محاسبات نرم

سال هفتم/ شمارهٔ اول/ بهار و تابستان ۱۳۹۷/ صفحهٔ ۶۲ـ۷۹

دریافت مقاله: ۱۳۹۷/۰۴/۳۱

پذیرش مقاله: ۱۳۹۸/۱۲/۱۹

ارزیابی کارایی تشخیص جعل کپی‌ـ انتقال تصاویر مبتنی بر بلاک‌بندی

فرزانه هویدا[۱*]، اسدالله شاه‌بهرامی[۲]

[۱] دانشجوی کارشناسی ارشد، گروه کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد لاهیجان، لاهیجان، ایران

hoveyda.f@gmail.com

[۲] دانشیار، گروه کامپیوتر، دانشکده فنی و مهندسی، دانشگاه گیلان، رشت، ایران

shahbahrami@guilan.ac.ir

چکیده: جعل کپی‌ـ انتقال، نوع خاصی از تحریف است که در آن بخش یا بخش‌هایی از یک تصویر، در قسمت‌های دیگری از همان تصویر کپی می‌شوند. این نوع دستکاری به‌منظور پنهان کردن بخش خاصی از تصویر و یا تکثیر یک یا چند شیء در همان تصویر انجام می‌گیرد. روش‌های متعددی برای تشخیص جعل کپی‌ـ انتقال ارائه شده است که شامل دو روش مبتنی بر بلوک[۱] و مبتنی بر نقاط کلیدی[۲] است. در این مقاله، یک روش تشخیص جعل کپی‌ـ انتقال بر اساس ویژگی‌های ترکیبی ارائه می‌شود. از ترکیب توصیفگرهای SIFT[۳]، KAZE، HOG[۴] و Zernike در جهت آشکارسازی جعل‌های کپی‌ـ انتقال استفاده می‌شود. نتایج پیاده‌سازی ترکیب توصیفگرها روی تصاویر جعل‌شده، نشان داد که این نوع ترکیب باعث افزایش دقت تشخیص نسبت به استفادهٔ تک‌تک و دوبه‌دوی توصیفگرها می‌گردد؛ اما این کارایی و دقت بالا با هزینهٔ زیاد محاسبات به دست می‌آید. لذا برای کاهش حجم محاسبات از الگوریتم ژنتیک[۵] در جهت بهینه‌سازی توصیفگرها و از الگوریتم تحلیل مؤلفهٔ اصلی برای کاهش ابعاد ویژگی‌ها استفاده شد. نتایج نشان داد که توصیفگر HOG با دقت ۹۳/۵۹ نسبت به دیگر توصیفگرها عملکرد بهتری برای تشخیص نقاط جعل دارد. ترکیب چهار توصیفگر موجب می‌شود تا عملکرد سیستم به میزان حدود ۳درصد نسبت به HOG بهبود یافته و به دقت ۹۶/۲۹ برسد. الگوریتم ژنتیک با انتخاب بهترین ویژگی‌ها به درصد تشخیص ۹۶/۹۴ رسید. با استفاده از تحلیل مؤلفهٔ اصلی، ابعاد ویژگی‌ها به ۳۵ بُعد کاهش داده شد که درصد تشخیص ۹۴/۶۳ به دست آمد.

واژه‌های کلیدی: کپی‌ـ انتقال، بلوک‌بندی، ارزیابی، جعل، ترکیب توصیفگرها.

1. Block-based
2. Key point-based
3. Scale Invariant Features Transform (SIFT)
4. Histogram of oriented Gradients (HOG)
5. Genetics Algorithm (GA)

۱. مقدمه

تصاویر یکی از واسطه‌های ارتباطات هستند. در دنیای امروز تصاویر دیجیتالی جزء داده‌های اصلی مورد استفاده قرار می‌گیرند؛ زیرا با توسعه و گسترش انواع دستگاه‌های دیجیتالی مانند دوربین‌ها و موبایل‌ها در هر لحظه و مکان می‌توان تصاویر مختلف را ضبط و اخذ کرد. از طرف دیگر امروزه با انواع نرم‌افزارهای مختلفی از قبیل Photoshop, Paint Touch Retouch, Superimpose, Photoblend و... می‌توان تصاویر را به‌راحتی دستکاری کرد. تصاویر دیجیتالی در بخش‌های زیادی استفاده می‌شوند؛ مانند مسائل نظامی، پزشکی، عکاسی و... . اگر تصویری که منبع یک سند است دستکاری شود، در بسیاری از کاربردها قابل استفاده نخواهد بود. بنابراین، سؤالی که مطرح می‌شود، این است که چگونه ما تصاویر دستکاری‌شده و پردازش‌شده را از تصاویر اصلی تشخیص دهیم [۱].

تصاویر اصلی به کمک روش‌های مختلفی مانند کپی‌ـ انتقال، روتوش کردن و پیوند تصاویر جعل می‌شوند. در کپی‌ـ انتقال، قسمتی از یک تصویر در بخش‌های دیگر از همان تصویر انتقال داده می‌شود. روتوش کردن، اصلاح یا حذف جزئیات ناخواسته در تصویر است. پیوند تصاویر نیز شامل ادغام دو یا چند تصویر و تغییر تصویر اصلی برای تولید تصویر جعلی است [۱ و ۲]. با توجه به اینکه کارهایی مختلفی برای تشخیص جعل کپی‌ـ انتقال صورت گرفته، دقت تشخیص این روش‌ها پایین است. لذا ارائه و شناسایی الگوریتم‌های که توانایی بیشتری در تشخیص جعل‌های صورت‌گرفته داشته باشد، از چالش‌های پیش روست [۲].

هدف اصلی این مقاله، ارائهٔ روشی برای بالا بردن دقت تشخیص سیستم‌های جعل کپی‌ـ انتقال است، در این راستا از ترکیب توصیفگرهای عمومی مانند SIFT و توصیفگرهای محلی مانند KAZE و توصیفگرهای HOG و Zernike استفاده شده است [۲].

نتایج پیاده‌سازی با توجه به آزمایش‌های مختلف و بررسی چهار توصیفگر SIFT، KAZE، HOG و Zernike نشان داد که توصیفگر HOG نسبت به دیگر روش‌ها عملکرد بهتری از خود ارائه می‌دهد و دارای دقت بیشتری است. سپس ترکیب ویژگی‌های HOG+Zernike، SIFT+KAZE، SIFT+KAZE+HOG مورد محاسبه قرار گرفت. نتایج پیاده‌سازی نشان داد که تلفیق ویژگی‌های چهار توصیفگر دارای دقت بیشتری است. در ادامه، از الگوریتم ژنتیک برای انتخاب بهترین ویژگی و از تحلیل مؤلفهٔ اصلی برای کاهش ابعاد تصویر استفاده شده است.

این پژوهش به‌صورت زیر سازمان‌دهی شده است. در بخش دوم، دربارهٔ برخی از پیشینه‌های تحقیق بحث می‌شود. در بخش سوم به ترکیب روش‌ها و در بخش چهارم، به پیاده‌سازی و ارزیابی پرداخته شده است. در بخش پنجم آزمایش‌های پژوهش انجام شده و نتیجهٔ حاصل از آن در بخش ششم مطرح گردیده است.

۲. طلاعات اولیه و پیشینهٔ تحقیق

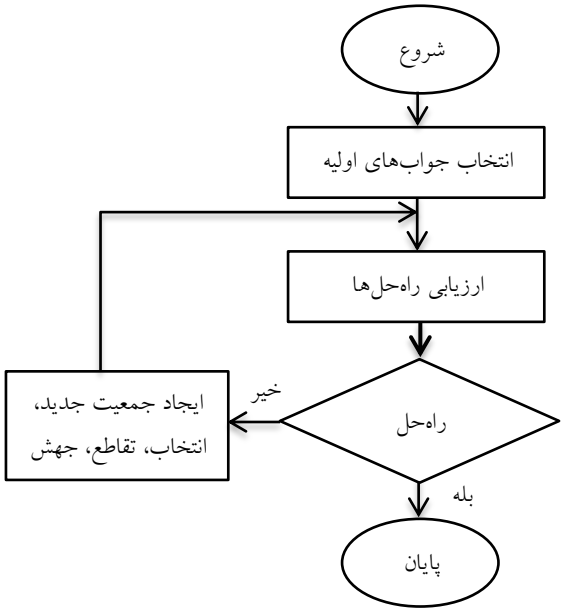
در این بخش، مفاهیم اولیهٔ تعدادی از روش‌های تشخیص جعل کپی‌ـ انتقال تعریف می‌شود و سپس به کارهای انجام‌شده در این زمینه پرداخته خواهد شد.

۲ـ۱. الگوریتم ژنتیک

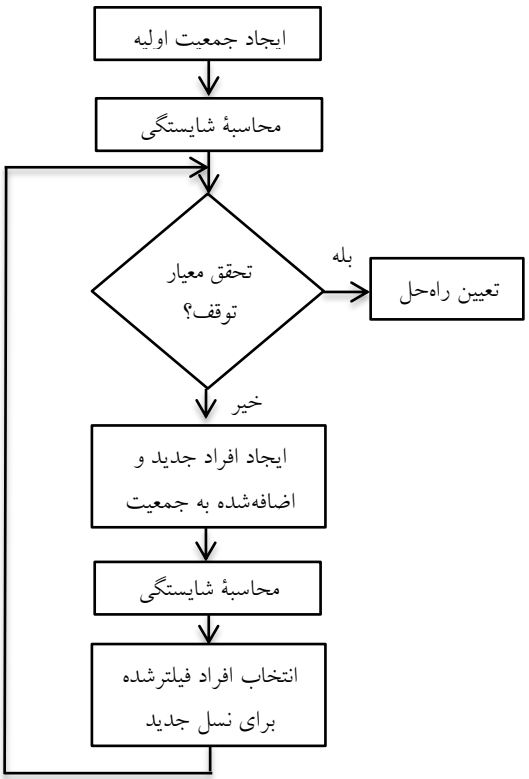
الگوریتم ژنتیک یک الگوریتم بهینه‌سازی است. ایدهٔ اصلی الگوریتم ژنتیک این است که ابتدا با جمعیت اولیه‌ای که به‌صورت دلخواه انتخاب شده است، شروع می‌شود. سپس، عملکرد نسبی آن‌ها ارزیابی می‌گردد. بر اساس این عملکرد، یک جمعیت جدید با استفاده از پتانسیل راه‌حل‌ها از عامل‌های تکاملی ساده ایجاد می‌شود. این روند تا رسیدن به یک راه‌حل رضایت‌بخش نیز تکرار می‌شود. روند کلی این الگوریتم در شکل (۱) نشان داده شده است.

پیاده‌سازی و اجرای الگوریتم‌های ژنتیکی، تفاوت‌های چشمگیری از لحاظ ساخت جمعیت جدید دارند. برخی از پیاده‌سازی‌ها با اعمال عملگرهای ژنتیکی، یک جمعیت جداگانه از افراد جدید را در هر نسل به وجود می‌آورند. پیاده‌سازی‌های دیگر، جمعیت فعلی را با اضافه کردن افراد جدید، گسترش داده و سپس با حذف نامناسب‌ترین افراد، جمعیت جدید را به وجود می‌آورند (شکل ۲). همچنین الگوریتم‌های ژنتیکی وجود دارند که اصلاً از تولید نسل استفاده نمی‌کنند. در عوض، دارای جابه‌جایی پیوسته‌اند. بر

طبق روش ایجاد یک جمعیت جدید، GA از سایر عملگرها، به‌خصوص عملگر انتخاب استفاده کرده و همچنین موقعیت محاسبهٔ برازش هر فرد را نیز مدنظر قرار می‌دهد [۳ و ۴].



شکل (۱): روال کلی الگوریتم ژنتیک [۳]



شکل (۲): توصیف یک الگوریتم ژنتیک با تعمیم جمعیت فعلی [۳]

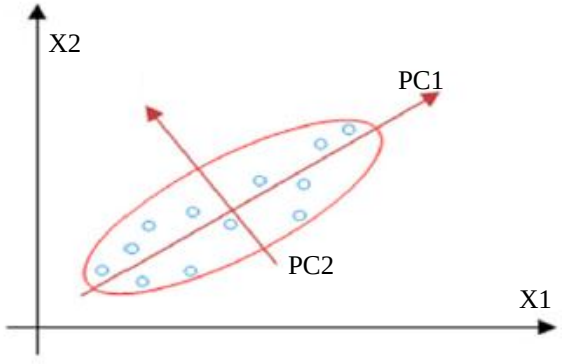
۲ـ۲. تحلیل مؤلفه‌های اصلی

از عوامل مهم در دقت و کارایی طبقه‌بندی‌کننده‌ها، کاهش ابعاد فضای ویژگی است. کاهش هزینهٔ محاسباتی و دقت طبقه‌بندی، دو دلیل عمدهٔ کاهش بُعد فضای ویژگی است. یکی از روش‌های معمول کاهش بعد فضای داده‌ها و استخراج ویژگی، روش تحلیل مؤلفه‌های اصلی (PCA) است. این روش به دنبال یک بازنمایی از داده‌ها برحسب کوچک‌ترین متوسط مربعات خطا بین داده‌های بازنمایی‌شده و اصلی است. لذا تحلیل مؤلفه‌های اصلی کاری به استخراج ویژگی‌های بهینه به‌منظور طبقه‌بندی ندارد؛ به عبارتی، این روش به‌منظور استخراج ویژگی و کاهش بعد، تنها به داده‌های ورودی توجه می‌کند و کلاس داده‌ها را در نظر نمی‌گیرد. تحلیل مؤلفهٔ اصلی یک روش ساده برای کاهش ابعاد است. به‌طور کلی، کاربرد عمدهٔ روش تحلیل اجزای اساسی عبارت است از کاهش تعداد متغیرها و یافتن ساختار ارتباطی بین متغیرها که در حقیقت همان دسته‌بندی متغیرهاست. شکل (۳) نمودار پراکنش نقاطی را روی دو محور مختصات X1 و X2 نشان می‌دهد [۵]. برای تعیین جهت عمومی نقاط، یک بیضی رسم می‌شود تا همبستگی بین متغیرها مشخص شود. برخی از نقاط خارج از بیضی و البته تجمع تعداد زیادی از آن‌ها روی قطر اصلی بیضی مشاهده می‌شود. جهت اصلی پراکنش نقاط نه در امتداد X1 و نه در امتداد X2 است بلکه بین آن‌ها و بیشتر در امتداد قطر اصلی بیضی می‌باشد. این محور PC1 نامیده می‌شود که اولین جزء اصلی تغییرپذیری X1 و X2 است. دومین جزء (PC2) در امتداد قطر فرعی بیضی است که دقیقاً بر PC1 عمود بوده و باقی تغییرات در X1 و X2 را شرح می‌دهد PC1 و PC2 دو محور جدید برای شرح X1 و X2 می‌باشند [۵ و ۶].

۲ـ۳. گرادیان هیستوگرام جهت‌دار

گرادیان هیستوگرام جهت‌دار (HOG) یک توصیفگر ویژگی است که برای تشخیص نقاط متحرک در پردازش تصویر و بینایی ماشین استفاده می‌شود. این توصیفگر، توزیع گرادیان‌های محلی یا جهت‌های لبه است که می‌توانند به‌خوبی

تصویر را توصیف کنند. این ویژگی، جهت گرادیان تصویر را در همسایگی محلی نشان می‌دهد. فاصلهٔ بین ۰ تا ۱۸۰ درجه یا ۰ تا ۳۶۰ درجه به n قسمت مساوی تقسیم می‌شود. n تعداد جهت‌های گرادیان است. با حرکت فیلترهای گوسی [۱, ۰, -۱] یا ترانهاده آن بر تصویر مانند مشتق‌گیری جهت‌دار گرادیان تصویر محاسبه شده و تحت زوایای ۲۰ درجه، ۲۰ درجه مشتق گیری انجام می‌شود. سپس لبه‌های جهت دار به دست می‌آیند [۷].



شکل (۳): انتقال داده‌ها به مؤلفهٔ اساسی [۵]

۲ـ۴. توصیفگر SIFT

الگوریتم SIFT یک الگوریتم توصیف‌کنندهٔ ویژگی است. هرگاه تصویری به این الگوریتم داده می‌شود، این الگوریتم نقاط کلیدی تصویر را استخراج می‌کند. در مرحلهٔ بعد برای هرکدام از نقاط کلیدی استخراج‌شده، یک شناسنامه ساخته می‌شود. الگوریتم SIFT استخراج ویژگی محلی انجام می‌دهد و جزئیات تصویرها را بررسی می‌کند. چالشی که وجود دارد این است که این الگوریتم‌ها باید در برابر چرخش، نور، نویز، تغییرات روشنایی و مقیاس مقاوم باشند؛ اما SIFT نسبت به تغییرات روشنایی به‌صورت جزئی مقاوم است [۸].

۲ـ۵. توصیفگر KAZE

کلمهٔ KAZE یک کلمهٔ ژاپنی به معنی باد است. در طبیعت باد به‌عنوان جریان هوا در مقیاس بزرگ تعریف شده است؛ به‌طور معمول این جریان به‌وسیلهٔ فرایندهای غیرخطی اداره می‌شود. این الگوریتم به‌وسیلهٔ Perona پیشنهاد شده است؛ که برخلاف الگوریتم SIFT ویژگی‌های عمومی تصویر را استخراج می‌کند. تصویری که به‌عنوان ورودی به این الگوریتم داده می‌شود با استفاده از انتگرال تصویر و فرمول‌های KAZE طبق روابط (۱) و (۲) بهبود داده می‌شود [۹].

$$g_1=\exp\left(-\frac{|\nabla L_\sigma|^2}{k^2}\right) \quad , \quad g_2=\frac{1}{1+\frac{|\nabla L_\sigma|^2}{k^2}} \qquad (۱)$$

$$g_3=\begin{cases} 1 & , \quad |\nabla L_\sigma|^2=0 \\ 1-\exp\left(-\frac{3.315}{(|\nabla L_\sigma|/k)^8}\right) & , |\nabla L_\sigma|^2>0 \end{cases} \qquad (۲)$$

g_1 : حاشیه‌های با کنتراست بالا، ∇L_σ :گرادیان تصویر است.
k: فاکتور کنتراست که سطح انتشار را کنترل می‌کند.
g_2 : مناطق گسترده تصویر را در مناطق کوچک‌تر افزایش می‌دهد.
g_3 : مناطق مات‌شدهٔ تصویر است.

۲ـ۶. گشتاور Zernike

یک روش تشخیص جعل کپی‌ـ انتقال استفاده از گشتاور Zernike است، که مکان نواحی تکراری را مشخص می‌کند. گشتاور Zernike مجموعه‌ای از چندجمله‌ای‌های مختلط را ارائه می‌کند که مجموعهٔ متعامد کاملی داخل دایرهٔ واحد تشکیل می‌دهند؛ دایرهٔ واحد همان مجموعه $x^2+y^2=1$ است. ساختار این چندجمله‌ای‌ها به‌صورت رابطهٔ (۳) است.

$$V_{nm}(x,y)=V_{nm}(\rho,\theta)=R_{nm}(\rho)\exp(jm\theta) \qquad (۳)$$

n: صفر یا عدد صحیح مثبت؛ m: عدد صحیح مثبت یا منفی با این شرط $n\geq|m|$, $n-|m|$؛ ρ: طول بردار مبدأ تا نقطه (x,y)، θ: زاویهٔ بین بردار و محور x در جهت پادساعت‌گرد، $R_{nm}(\rho)$: یا همان چندجمله‌ای‌های شعاعی نیز این‌گونه تعریف می‌شود:

(۴)

$$R_{nm}(\rho)=\sum_{x=0}^{n-|m|/2}(-1)^x.\frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!}\rho^{n-2x}$$

که برای این چندجمله‌ای‌ها می‌توان نوشت:

$$R_{n-m}(\rho)=R_{nm}(\rho) \qquad (۵)$$

$$\iint_{x^2+y^2\le 1}[V_{nm}(x,y)*V_{\rho g}(x,y)dxdy=\frac{\pi}{n+1}\delta_{n\rho}\delta_{mg}$$
$$\rho_{ab}=\begin{cases}1 & a=b\\ 0\end{cases} \qquad (۶)$$

ممـان Zernike نگاشـت توابـع تصـویر بـر روی ایـن چندجمله‌ای‌هاست. گشتاور Zernike از مرتبه n بـا تکـرار m برای تصویر پیوسته تابع f(x,y) که قسمت بیرونی دایرهٔ واحـد را محو می‌کند، به‌صورت زیر است:

$$A_{nm}=\frac{n+1}{\pi}\iint_{x^2+y^2\le 1}f(x,y)V_{nm^*}(\rho,\theta)dxdy \qquad (۷)$$

برای تصویر دیجیتالی، انتگـرال‌هـا توسـط مجمـوع بـرای به‌دست‌آوردن معادلهٔ زیر جایگزین می‌شوند:

$$A_{nm}=\frac{n+1}{\pi}\sum_x\sum_y f(x,y)V_{nm^*}(\rho,\theta) \qquad x^2+y^2\le 1 \qquad (۸)$$

در محاسبهٔ Zernike مرکـز تصـویر در مرکـز دایـره قـرار می‌گیرد و بقیهٔ تصـویر بـه داخـل دایـره نگاشـت مـی‌شـود و آن‌هایی که بیرون دایره می‌افتد، در محاسـبه وارد نمـی‌شـوند. همچنین توجه شود که $A_{nm^*}=A_{n-m}$ است.

محققان گشتاور Zernike را به‌عنوان روشی برای استخراج مشخصه‌ها از زیربلـوک‌هـای همپوشـانی در تصـویر پیشـنهاد دادند. این بردارهای مشخصه بر اسـاس حـروف الفبـا مرتـب می‌شوند و شباهت‌های بـین دو بلـوک مجـاور بـا اسـتفاده از فاصلهٔ اقلیدسی و یک آستانه برای پیدا کردن نشانه‌ای از جعل کپی‌ـ انتقال محاسبه می‌شود، صحت و کامـل بـودن و مقیـاس F1 روی نواحی مشکوک اعمال می‌شود تا جعل کپی‌ـ انتقال را تأیید کند [۱۰ـ۱۲].

۲ـ۷. پیشینهٔ تحقیق

روش‌های زیادی برای تشخیص جعل‌های کپی‌ـ انتقال وجود دارد ولی مسئلهٔ بسیار مهم این اسـت کـه آیـا ایـن روش‌هـا در برابـر عملیات‌هایی مثل چرخش، تغییر جهت، نویز و... مقاوم هستند یـا خیر؟ در سال‌های اخیر، روش‌های متعددی برای تشخیص جعـل کپی‌ـ انتقال ارائه شده است، بسیاری از آن‌ها را مـی‌تـوان بـه‌طـور سنتی به دو روش مبتنی بر بلوک و روش مبتنی بـر نقـاط کلیـدی طبقه‌بندی کرد [۱۳]. در روش‌هـای مبتنـی بـر بلـوک تصـویر بـه بلوک‌هایی تقسیم می‌شود و ویژگی‌ها از این بلـوک‌هـا اسـتخراج مـی‌گـردد ولـی روش‌هـای مبتنـی بـر نقـاط کلیـدی سـعی در به‌دست‌آوردن نقاط حساس و مهم در تصویر دارند.

در [۲] برای نشان دادن بلوک‌های تصـویر از ضـرایب تبـدیل کسینوسی گسسته[1] استفاده شده اسـت. سـپس یـک روش بهبـود یافته بر اساس DCT برای تشخیص جعـل کپـی‌ـ انتقـال پیشـنهاد شده است. با توجه به الگوبرداری ارائـه‌شـده، اگرچـه روش‌هـای مبتنی بر بلوک می‌تواند جعل کپی‌ـ انتقال را در بسـیاری از مـوارد مانند اضافه کردن نویز و فشـرده‌سـازی JPEG[2] تشـخیص دهـد، وقتی تصاویر به اندازهٔ بزرگ تغییر می‌یابند با خطا مواجه می‌شوند [۱۴]. در [۱۵] با آنالیز اجزای مؤلفهٔ اصلی در بلوک‌هـای تصـاویر، ابعاد تصاویر کاهش پیدا کرد. هفـت ویژگـی بـر مبنـای میـانگین شدت پیکسل در هر کانال RGB و برخی از اطلاعـات جهـت‌دار هر بلوک استخراج شد [۱۶]. در [۱۳] ۲۴ نقطهٔ محوشده محاسـبه شـد و یـک بخـش از ویژگـی‌هـای هـر بلـوک را تولیـد کـرد. پژوهشگران در [۱۶] تبدیل موجک گسسته و تحلیل اجزای اصلی را برای استخراج ویژگی ترکیب کرده‌اند. آن‌ها ابتدا تبدیل موجک گسسته را روی تصویر اعمال کرده، سپس ابعـاد هـر بلـوک را بـا تحلیل اجزای اصلی کاهش داده‌اند.

علاوه بر این تقریبـاً تمـام ایـن روش‌هـا در تعـداد زیـادی از بلوک‌ها و بردارهای ویژگی استخراج‌شده از آن‌ها تـوده‌ای هسـتند که منجر به پیچیدگی محاسباتی بالا مـی‌شـوند. در [۱۳] از تبـدیل فوریه ملین[3] برای به دست آوردن ویژگی‌های بلوک اسـتفاده شـد. در [۱۴] پیشنهاد شد که تصویر به چهار زیرشـاخه[4] بـا اسـتفاده از تبدیل موجک دیجیتال[5] تجزیه شود و سپس مقدار انحصـاری[6] در این بلوک‌ها اعمال می‌گردد. ضریب همبسـتگی فوریـه بـه‌عنـوان اندازه‌گیری شباهت بین بلوک در شکل ورودی قطبی[7] بـه دسـت آورده شد. سپس آن‌ها زمانی که مقدار آن کمتر از یک حد آسـتانه اسـت بلـوک را حـذف مـی‌کننـد [۲]. در [۱۳] ویژگـی‌هـایی از بلوک‌های دایره‌ای با استفاده از چرخش یکنواخت ثابت الگوهـای

1. Discrete Cosine Transform (DCT)
2. Joint Photographic Experts Group (JPEG)
3. Fourier-Mellin Transform (FMT)
4. Sub-band
5. Discrete Wavelet Transform (DWT)
6. Singular Value Decomposition (SVD)
7. Log-polar

دودویی محلی[1] را استخراج کردند. همچنین تغییرات‌هارمونیک قطبی[2] به تصویب رسانده شد که محتویات بلوک‌های دایره‌ای را توصیف می‌کند. در [۱۰] گشتاور Zernike[3] به‌عنوان ویژگی بلوک برای تشخیص مناطق تکراری مورد استفاده قرار داده شد. الگوریتم Patch Match و اصلاح آن برای مقابله با عملیات چرخش مورد بررسی قرار گرفت [۱۷]. با توجه به معیارهای پیشنهادشده در [۲] اگر چه روش‌های مبتنی بر بلوک می‌توانند جعل کپی‌ـ انتقال را در اکثر موارد مانند فشرده‌سازی JPEG آشکار کنند، هنگامی که در مناطق تکرار به‌اندازهٔ بزرگ تغییر اندازه و چرخش پیدا می‌کنند از بین می‌روند. علاوه بر این، تقریباً تمام این روش‌ها در تعداد زیادی از بلوک‌ها و بردارهای ویژگی استخراج‌شده از بلوک‌ها توده‌ای هستند که منجر به پیچیدگی محاسباتی بالا می‌شوند. به‌عنوان جایگزینی برای روش‌های مبتنی بر بلوک، روش تشخیص جعل کپی‌ـ انتقال مبتنی بر نقاط کلیدی پیشنهاد شده است. در این روش برخلاف روش مبتنی بر بلوک، ویژگی‌های خوب تصویر، شناسایی و انتخاب شدند.

در مقایسه با روش مبتنی بر بلوک، روش های مبتنی بر نقاط کلیدی در برابر تحولات هندسی از جمله تغییر اندازه در مقیاس بزرگ قوی‌ترند. علاوه بر این، هزینهٔ محاسبات به‌دست‌آمده پایین‌تر است؛ چون تعداد نقاط به‌طور چشمگیری کمتر است. با این حال، در چنین روشی با اینکه ممکن است نقاط کلیدی به‌اندازهٔ کافی برای تجزیه و تحلیل وجود داشته باشد، مشکلاتی در محل بخش همگن به وجود خواهد آمد. روش‌های متعددی برای تبدیل ویژگی‌های مقیاس‌پذیر به تصاویر میزبان برای استخراج نقاط ویژگی استفاده شده است. برای مثال از الگوریتم SIFT برای تشخیص جعل استفاده می‌شود که در برابر مقیاس‌پذیری و تبدیلات چرخش مقاوم است و دقت به‌دست‌آمده برابر ۹۲/۵٪ است [۱۸]. در [۲] ویژگی‌های SIFT برای تعیین منطقهٔ کپی‌شده از طریق استفاده از نقشه‌های همبستگی انتخاب شدند. الگوریتم SIFT به تبدیلات هندسی حساس نیست و عملکرد ضعیفی برای تشخیص جعل‌های نواحی کوچک دارد و نواحی جعل‌شده مکان‌یابی نمی‌شوند و دقت به‌دست‌آمده برابر ۹۰٪ است [۱۹]. در [۱۰] پژوهشگران از الگوریتم SIFT برای شناسایی نقاط جعل استفاده کردند که این روش به تبدیلات و اعوجاج روشنایی بدلیل استفاده از SIFT حساس نیست. دقت به‌دست‌آمده برابر ۷۳/۳۶٪ است. در [۲۰] از الگوریتم SIFT برای استخراج مشخصه‌ها و از تکنیک تطبیق برای تطبیق مشخصه و از الگوریتم خوشه‌بندی نیز برای تشخیص و مکان‌یابی نواحی جعل شده استفاده شده است. سپس یک روش مبتنی بر خوشه‌بندی نقطه‌های همگرا پیشنهاد شد. [۲] بعدها روش خود را با معرفی یک فاز جدید خوشه‌بندی قوی بر اساس الگوریتم Toldoو Fusiello بهبود بخشید. در [۱۰ و ۲۱] ممان‌های Zernike از بلوک‌ها به‌عنوان ویژگی استخراج گردید. ممان‌های Zernike به‌دلیل جبری بودن در برابر چرخش مقاوم هستند و به همین دلیل برای موقعیت‌هایی که علاوه بر انتقال، چرخش نیز انجام شده باشد، مناسب‌اند. در [۱۶] نیز این ممان به‌عنوان ویژگی از هر بلوک استخراج شد. در [۲۲] یک روش تشخیص جعل کپی‌ـ انتقال پیشنهاد شد که در آن نقطه SURF استخراج شده و با الگوریتم درختی k-d همخوانی دارد. برای روش‌های تشخیص جعل کپی‌ـ انتقال از نقاط گوشهٔ هریس و بخش آمار در تصاویر دیجیتال استفاده شد. روش‌های متعددی برای تبدیل ویژگی‌های مقیاس‌پذیر به تصاویر میزبان برای استخراج نقاط ویژگی استفاده می‌شود. برای مثال، ویژگی‌های SIFT برای تعیین منطقهٔ کپی‌شده از طریق استفاده از نقشه های همبستگی انتخاب شدند. استخراج ویژگی در بیشتر روش‌های مبتنی بر نقاط کلیدی بر مبنای الگوریتم SIFT انجام می‌شود. روش تشخیص مبتنی بر نقاط کلیدی، به‌دلیل نداشتن نقاط همسان کافی ممکن است رد شود، یک روش تشخیص جعل کپی‌ـ انتقال بر اساس ویژگی‌های ترکیبی پیشنهاد شده است. یک تشخیص‌دهندهٔ نقطه‌ای KAZE در ترکیب با SIFT برای استخراج نقاط ویژگی بیشتر به کار رفته است. ایدهٔ اصلی این روش تشخیص جعل کپی‌ـ انتقال مبتنی بر بلوک است که به تقسیم

1. Local binary pattern (LBP)
2. Polar Harmonic
3. Zernike moment

تصویر ورودی با بلوک‌های همپوشان ثابت پرداخته و پس از آن جفت بلوک‌های مشابه را پیدا می‌کند. با استفاده از ترکیب دو ویژگی SIFT و KAZE ویژگی‌های نقاط بیشتری استخراج کردند. نتایج تجربی نشان می‌دهد که روش ارائه‌شده دقیقاً می‌تواند حتی پس از تحریف مانند چرخش، مقیاس‌پذیری، فشرده‌سازی JPEG و اضافه کردن نویز، مناطق تکراری را تشخیص دهد [۲].

در [۲۳] روش مبتنی بر بلوک و مبتنی بر نقاط کلیدی با یکدیگر ادغام شده است. ابتدا تصویر اصلی به بلوک تقسیم شده و نقاط کلیدی از هر بلوک تصویر استخراج می‌شوند. تعداد نقاط کلیدی مشابه مشخص‌شده از یک جفت بلوک، از یک آستانه از پیش تعیین‌شده فراتر رفته و سپس آن جفت بلوک از هم جدا می‌شوند. بلوک‌های همسان به‌عنوان منطقه جعل در نظر گرفته می‌شوند و خروجی پس از عملیات مورفولوژی نمایش داده می‌شود. در [۲۴] یک روش شناسایی جعل کپی‌ـ انتقال مبتنی بر KAZE و SURF ارائه شده است. ویژگی‌های KAZE و SURF دارای مزایای استخراج سریع و ویژگی استحکام‌اند که در این روش مورد استفاده قرار گرفته و برای پیدا کردن بخش‌های جعل‌شده در تصویر استفاده شده‌اند. در [۲۵] ویژگی‌های SIFT، SURF و HOG و ویژگی‌های ترکیبی (SURF+HOG یا SIFT+HOG) برای تشخیص جعل کپی‌ـ انتقال مقایسه شد و نتیجه نشان داد که SIFT بهترین نتیجه را در تشخیص دقت می‌دهد. پس از بررسی ویژگی‌های ترکیبی (SURF+HOG یا SIFT+HOG) نتیجهٔ بهتری برای تشخیص جعل در مقایسه با وقتی که ویژگی‌های SIFT،SURF یا HOG تنها استفاده می‌شوند به دست آمد.

نتیجه این پژوهش نشان داد که طرح پیشنهادی می‌تواند مناطق جعلی را در تصاویر مختل‌شده، حتی در شرایطی که منطقهٔ آسیب دیده یا تصویر مخدوش می‌شود، تشخیص دهد. در زمینهٔ تشخیص جعل کپی‌ـ انتقال کارهای زیادی انجام گرفته که برخی از آن‌ها در جدول (۱) نیز نشان داده شده است.

جدول (۱): روش‌های مکان‌یابی و تشخیص جعل کپی‌ـ انتقال

ردیف	منابع	روش‌شناسی و دادگان	محدودیت‌ها	کارایی
۱	[۲]	از الگوریتم SIFT و الگوریتم KAZE برای استخراج مشخصه استفاده شد. دادگان: ۴۸ تصویر پایه و ۴۸ تصویر جعل‌شده	دقت تشخیص الگوریتم SIFT، ۸۳/۲۶٪ و دقت تشخیص الگوریتم KAZE، ۸۳/۴۵٪ برآورد شد.	هر دو الگوریتم به‌تنهایی کل ویژگی‌های یک تصویر را بیرون نمی‌کشند. بنابراین با ترکیب SIFT+KAZE درصد تشخیص ۹۲٪/۲۷ به دست آمد.
۲	[۸]	از الگوریتم SIFT برای تشخیص جعل استفاده می‌شود. دادگان: MICC-F2000-MICC-F220	به تبدیلات هندسی حساس نیست. دقت: ۹۰٪	عملکرد ضعیفی برای تشخیص جعل‌های نواحی کوچک دارد و نواحی جعل‌شده مکان‌یابی نمی‌شوند.
۳	[۲۵]	ویژگی‌های ترکیبی (SURF+HOG یا SIFT+HOG) برای تشخیص جعل کپی‌ـ انتقال مقایسه شد.	نتیجه نشان داد که SIFT بهترین نتیجه را در دقت می‌دهد. دقت: ۹۸/۲۰٪	اما با ترکیب SIFT+HOG، دقت تشخیص بیشتری به دست آمد. دقت: ۹۸/۲۱٪
۴	[۲۶]	مشخصه‌های زرنیک و معیارهای کیفیت تصویر از تصویر ورودی استخراج شدند. از شبکهٔ عصبی مصنوعی برای دسته‌بندی استفاده شده است. دادگان: DVMM	پیچیدگی زمانی بالاست.	دقت: ۶۳۹/۹٪
۵	[۲۷]	از الگوریتم SIFT برای شناسایی جعل استفاده می‌شود. دادگان: توسط خود محققان ساخته شده است.	به تبدیلات و اعوجاج روشنایی به‌دلیل استفاده از SIFT حساس نیست. دقت: ۷۳/۳۶٪	برای شناسایی نواحی تکثیرشده عملکرد ضعیفی دارد.

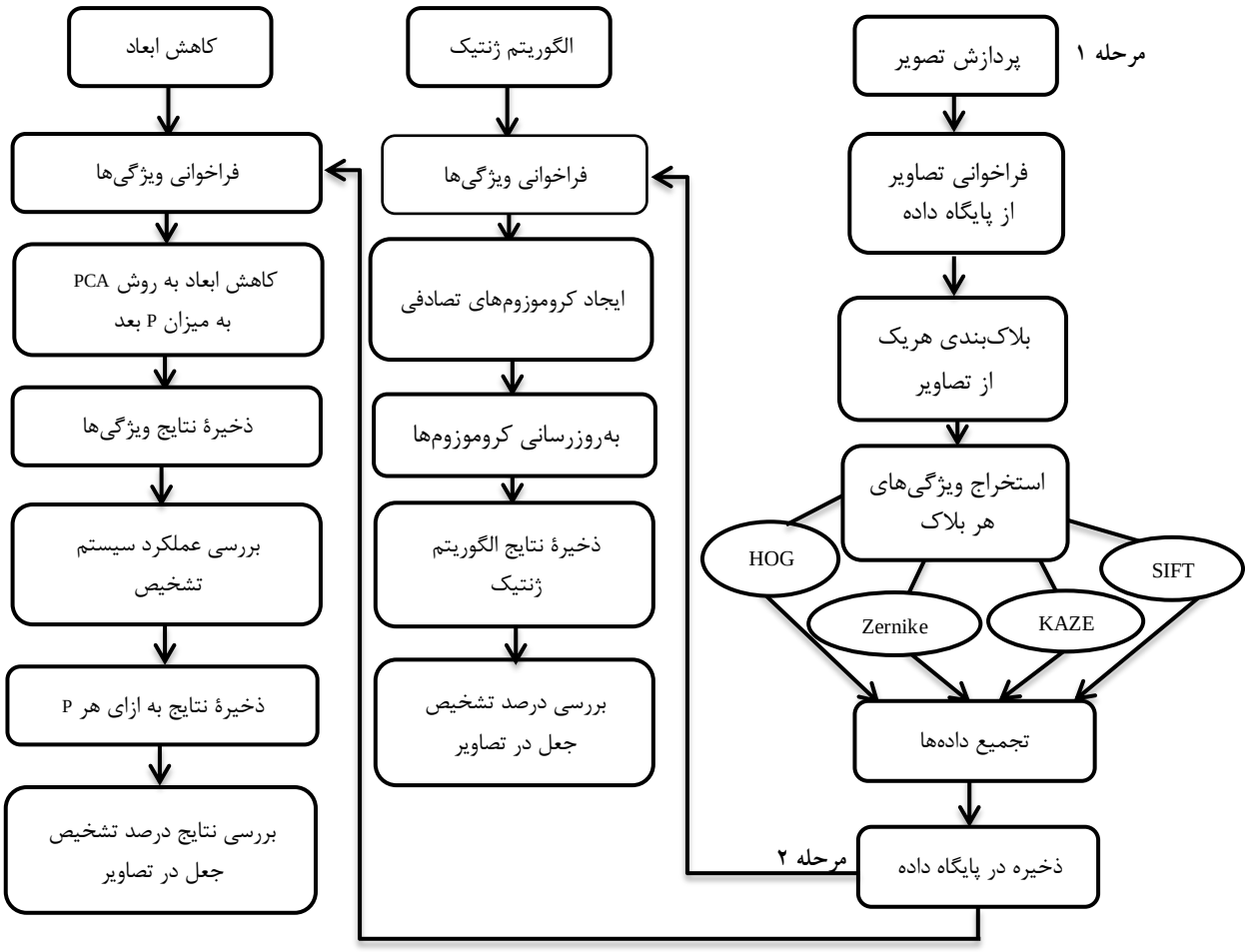
ردیف	منابع	روش‌شناسی و دادگان	محدودیت‌ها	کارایی
۶	[۲۸]	از الگوریتم SIFT برای استخراج مشخصه‌ها استفاده می‌شود و از تکنیک تطبیق برای تطبیق مشخصه استفاده می‌شود و از الگوریتم خوشه‌بندی برای تشخیص و مکان‌یابی نواحی جعل شده استفاده می‌شود. دادگان: F2000- MICC-F600 & MICC	روش خوشه‌بندی در برابر تبدیلات هندسی و جعل کپی_ انتقال مقاوم است و نواحی جعل‌شده را مکان‌یابی می‌کند. دقت: ٪۹۲	نواحی جعل‌شده مکان‌یابی نمی‌شوند.
۷	[۲۹]	الگوریتم SIFT برای تشخیص جعل استفاده می‌شود. دادگان: UCID	دقت: ٪۹۲/۵	در برابر مقیاس‌پذیری و تبدیلات چرخش مقاوم نیست.
۸	[۳۰]	از الگوریتم بهبودیافته بلوک برای تشخیص جعل استفاده می‌شود. دادگان: ۲۰۰ تصویر	این شیوه در برابر فشرده‌سازی JPEG و تاری گاوسی مقاوم است و همچنین در مکان‌یابی شکل و سایز جعل تصویر مؤثر است. دقت: ٪۷۳	در برابر تبدیلات هندسی مقاوم نیست.
۹	[۳۱]	تصویر ورودی به فضای رنگ YCBCR تبدیل می‌شود و توصیفگر WLD با چند درجه تفکیک برای استخراج مشخصه اعمال می‌شود. از SVM برای دسته بندی استفاده می‌شود. دادگان: TIDE V1.0-CASIA	دقت: ٪۹۳/۳۳	نواحی جعل‌شده مکان‌یابی نمی‌شوند.
۱۰	[۳۲]	تصویر ورودی به فضای رنگ YCBCR تبدیل می‌شود و مشخصه‌های محلی و عمومی از کانال‌های رنگ‌تابی و روشنایی با استفاده از گشتاور زرنیک استخراج می‌شوند. ماتریس هش از مشخصه‌های استخراج‌شده محلی و عمومی تشکیل می‌شود. مقدار هش تصویر تست شده و مقدار هش تصویر صحیح مقایسه می‌شود تا جعل را تشخیص دهد. دادگان: ۱۰۰۰تصویر واقعی و ۱۰۰۰تصویر جعل‌شده	در برابر فشرده‌سازی JPEG و چرخش با زاویه کم و مقیاس‌پذیری کم مقاوم است.	در برابر تبدیلات هندسی مثل چرخش و مقیاس‌پذیری مقاوم نیست.
۱۱	[۳۳]	مشخصه‌ها با استفاده از تبدیل فوریه هر بلوک از تصویر استخراج می‌شوند جعل توسط اعمال الگوریتم تطبیق بلوک مبتنی بر آستانه تشخیص داده می‌شود.	در برابر فشرده‌سازی JPEG و تار ی حساس نیست و اندازهٔ بردارهای مشخصه خیلی کوچک است. دقت: ٪۸۶/۵۷	به تبدیلات هندسی حساس است در برابر چرخش با زاویه کلی و مقیاس‌پذیری مقاوم نیست.
۱۲	[۳۴]	یک مدل بازگشت خودکار با استفاده از فیلتر میانگین از تصویر ورودی طراحی می‌شود که بعد عامل‌های آن برای دسته‌بندی در SVM قرار می‌گیرند. دادگان: ۶۶۹۰ تصویر واقعی و جعلی	دقت: ٪۹۸	فرایند انتخاب مشخصهٔ دستی انجام می‌شود.
۱۳	[۳۵]	از تبدیل موجک برای استخراج ویژگی‌های با اندازهٔ ۴۵۰ استفاده می‌شود که نمایانگر تکه‌های ycrb در داخل تصویر است. سپس از یک شبکهٔ عصبی برای طبقه‌بندی تکه‌های جعلی استفاده می‌شود.	این ایده با از بین بردن ویژگی‌های روشنایی بیان شده است.	دقت تشخیص: ٪۹۷/۱۱

۳. روش پیشنهادی

در روش پیشنهادی در این پژوهش، تصویر به بلوک‌هایی تقسیم می‌شود، هرکدام از این بلوک‌ها اطلاعات قسمتی از تصویر را در اختیار دارد و باید ویژگی‌های کلی آن استخراج شود. توصیفگرهای SIFT، KAZE، HOG و Zernike از هر بلوک استخراج می‌شود. هر توصیفگر روابط خاص خود را دارد و نوع خاصی از تصویر را توصیف می‌کند. HOG تصویر را بر اساس گرادیان، SIFT و KAZE بر اساس مشتق‌های محلی و زرنیک به‌صورت دایره‌وار توصیف می‌کند. ترکیب بردارهای این توصیفگرها سبب افزایش عملکرد سیستم تشخیص جعل می‌شود؛ اما همهٔ ویژگی‌های استخراج‌شده در سیستم تشخیص جعل مشارکت نمی‌کنند و ترکیب بردارهای توصیفگرها موجب افزایش حجم محاسبات می‌شود، لذا به‌منظور کاهش حجم محاسبات می‌توان از الگوریتم‌های انتخاب ویژگی مانند الگوریتم ژنتیک، به انتخاب ابعاد مناسب بردارهای ویژگی استخراج‌شده از توصیفگرها پرداخت. از سوی دیگر، حجم اشغال‌شده نیز یکی از چالش‌های این‌گونه سیستم‌هاست. بنابراین در این پژوهش از الگوریتم‌های کاهش ابعاد برای حل این چالش استفاده شده است. همان طور که ذکر شد، از الگوریتم ژنتیک پس از انتخاب ویژگی استفاده خواهد شد. این الگوریتم با ایجاد جمعیت اولیهٔ تصادفی در پی ایجاد جواب‌های تصادفی برای مسئله انتخاب ویژگی است. این جمعیت از کروموزوم‌ها تشکیل شده است. تعداد این کروموزوم‌ها در این پژوهش برای هر نسل ۱۰۰ عدد در نظر گرفته شد. هر کروموزوم از ژن‌هایی تشکیل می‌شود، هر ژن از کروموزوم‌ها در الگوریتم ژنتیک یک ویژگی است. این ژن‌ها احتمال انتخاب ویژگی نظیر خود در جدول ویژگی‌ها را نشان می‌دهد. یک حد آستانه برای این احتمالات تعیین شده است که برابر عدد ۰/۵ می‌باشد. هرکدام از ژن‌ها که احتمال انتخابشان بیشتر از حد آستانه باشد انتخاب می‌شود. پس از انتخاب ویژگی‌ها، مرحلهٔ بررسی تصاویر آغاز می‌شود. در این مرحله با توجه به ویژگی‌های انتخاب‌شده بلوک‌ها مقایسات رخ می‌دهد. پس از بررسی کل بلوک‌ها و تشخیص نقاط جعل، به بررسی عملکرد کلی سیستم پرداخته می‌شود. در این مقاله به دنبال کاهش میزان حجم محاسبات و خطای تشخیص هستیم. هرچه تعداد ویژگی‌ها کاهش یابد، میزان حجم فضای اشغالی و میزان محاسبات کاهش می‌یابد. از طرفی کاهش خطای تشخیص نقاط جعل را نیز می بایست در نظر گرفت. بنابراین مجموع دو پارامتر نسبت ویژگی‌ها و خطای تشخیص به‌عنوان تابع هدف تعیین می‌شود. پس از بررسی نهایی، کروموزوم‌های هر نسل بر اساس میزان تابع هدف مرتب می‌شوند. بنابراین آن دسته از جواب‌هایی که مناسب‌ترند در بالای نسل قرار می‌گیرند. برای ایجاد نسل جدید می‌بایست از کروموزوم‌های با جواب مناسب استفاده کرد. در نتیجه در این پژوهش ۴۰درصد جمعیت نسل گذشته به نسل جدید منتقل می‌شوند. دیگر کروموزوم‌ها نیز از طریق عملگرهای ادغام تک‌نقطه‌ای (۲۰درصد نسل جدید)، ادغام دونقطه‌ای (۲۰درصد نسل جدید) و جهش (۲۰درصد نسل جدید) به‌روز شده و به نسل جدید اضافه می‌شوند. این الگوریتم در طی ۱۰۰ بار تکرار صورت پذیرفته و در پایان آن بهترین کروموزوم انتخاب می‌شود. از طرفی می‌توان با ترکیب ویژگی‌ها، ابعاد را کاهش داد. در نتیجه به‌جای استفاده از الگوریتم ژنتیک، از الگوریتم تحلیل مؤلفهٔ اصلی استفاده می‌شود. در این بخش، هیچ ویژگی حذف نخواهد شد بلکه ابعاد آن بایکدیگر ترکیب می‌شود. در این بخش، هدف آن است که همهٔ ویژگی‌ها حضور داشته باشند و با کاهش ابعاد آن حجم اشغال‌شده کاهش یابد. بنابراین این پژوهش، به سه بخش تقسیم می‌شود: بخش اول پردازش تصاویر و استخراج ویژگی‌ها برای تشخیص جعل در تصاویر است. بخش دوم، انتخاب ویژگی‌ها توسط الگوریتم ژنتیک و بخش سوم به کاهش ابعاد داده با استفاده از تحلیل مؤلفهٔ اصلی اختصاص می‌یابد. همان طور که در شکل (۴) مشاهده می‌گردد، در ابتدا تصاویر از پایگاه داده فراخوانی می‌گردد. این تصاویر در محیط شبیه‌سازی متلب به ماتریس‌هایی تبدیل می‌شود. به‌ازای هرکدام از تصاویر پایگاه داده، چهار ویژگی مطرح‌شده استخراج می‌شود. این ویژگی‌ها در نهایت در پایگاه داده ذخیره می‌گردد تا در مراحل بعدی

پژوهش بتوان از آن استفاده کرد. در مرحلهٔ (۲)، ویژگی‌های تصاویر که از مرحلهٔ قبل استخراج شده و در پایگاه داده ذخیره شده‌اند فراخوانی می‌شود. الگوریتم ژنتیک در ابتدای اجرای خود یک جمعیت با کروموزوم‌های تصادفی ایجاد می‌کند، سپس در طی یک روند اجرایی این نسل‌ها به‌روز شده و کرومزوم‌ها به جواب بهینه همگرا می‌شوند. در نتیجه در پایان اجرای این الگوریتم ویژگی‌هایی که سبب کاهش حجم محاسبات و کاهش خطا می‌گردد انتخاب می‌شود. عملگرهای انتخاب‌شده در این پژوهش برای به‌روزرسانی کروموزوم‌ها عملگرهای ادغام تک‌نقطه‌ای و دونقطه‌ای و عملگر جهش انتخاب شده است.

در مرحلهٔ (۳)، روند اجرای کاهش ابعاد با استفاده از الگوریتم تحلیل مؤلفهٔ اصلی نشان داده شده است. همانند استفاده از الگوریتم ژنتیک، ویژگی‌های استخراج‌شده تصاویر از پایگاه داده فراخوانی می‌شوند. تعداد ابعاد کاهش(P) مشخص شده و ابعاد ویژگی‌ها ترکیب شده و کاهش می‌یابد. در نتیجه در پایان این بخش با کاهش ابعاد ویژگی‌ها به بررسی میزان تشخیص نقاط جعل در تصاویر پرداخته شده است. برای بررسی عملکرد، پس از بررسی نقاط تصویر توسط الگوریتم‌های مطرح‌شده، نتایج آن با نتایج ارائه‌شده در پایگاه داده مقایسه می‌شود.



شکل (۴): اعمال الگوریتم‌های ژنتیک و تحلیل مؤلفهٔ اصلی برای بهینه‌سازی و کاهش ابعاد به‌طور موازی

۴. پیاده‌سازی و ارزیابی

در این قسمت نتایج حاصل از پیاده‌سازی روش پیشنهادی روی تصاویر پایگاه داده مقاله [۱۳] که در سایت http://www5.cs.fau.de/research/data// است، ارائه می‌شود.

۴ـ۱. محیط پیاده‌سازی

شبیه‌سازی انجام‌شده در این بخش در تمامی کدها در نرم‌افزار مهندسی متلب نوشته و اجرا شده است. نتایج هر بخش از خروجی توابع استخراج و مورد بررسی قرار گرفته است. مراحل سه بخش استخراج ویژگی، الگوریتم ژنتیک و تحلیل مؤلفهٔ اصلی در این بخش توضیح و نتایج آن نشان داده شده است. این شبیه‌سازی در یک سیستم با مشخصات Intel(R) Core(TM) i7-4702MQ، 2.20GHz و میزان 16 RAM گیگابایتی و ویندوز ۸ اجرا گرفته شده است.

۴ـ۲. داده‌های استفاده‌شده و معیار ارزیابی

مجموعه داده‌های استفاده‌شده شامل ۹۶ تصویر است؛ که ۴۸ تصویر مکان جعل را اعلام کرده و ۴۸ تصویر پایه و تصاویر تغییریافتهٔ آن مانند چرخش، تغییر اندازه، فشرده‌سازی JPEG به همراه نویز است. اندازهٔ متوسط تصاویر این پایگاه داده حدود ۲۳۰۰×۲۳۰۰ پیکسل و حجم دستکاری‌شده در حدود ۱۰٪ از هر تصویر است. نمونه‌ای از تصاویر در شکل (۵) ارائه شده است.

شکل (۵): دو نمونه از تصاویر دستکاری‌شده در پایگاه داده [۱۳]

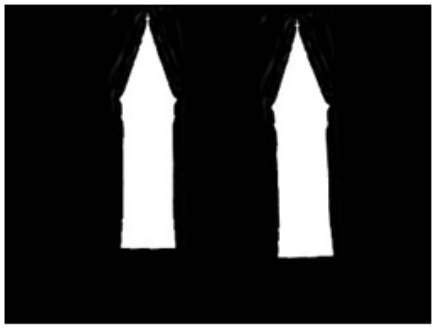
۴ـ۳. استخراج ویژگی‌های تصاویر

همان طور که بیان شد، چهار ویژگی SIFT، KAZE، Zernikeو HOG از هر بلوک تصویر استخراج می‌شود. در ابتدا تصاویر از پایگاه داده فراخوانی می‌گردد. در این بخش دو تصویر در پایگاه داده موجود است: یک تصویر اصلی و یک تصویر جعل شده که در شکل (۶) نشان داده شده است.

(الف) (ب)

شکل (۶): نمونه تصویر پایگاه داده (الف) اصلی، (ب) جعل‌شده (بخشی از بنای تصویر جعل و در سمت دیگر اضافه شده است)

برای مقایسهٔ نتایج محاسبه‌شده با تصاویر اصلی، پایگاه داده مکان جعل‌شده را نیز مانند شکل (۷) در اختیار پژوهشگران قرار می‌دهد. همان طور که مشاهده می‌شود، در این تصویر مکان جعل‌شده در شکل (۶ ب) مشاهده می‌شود.

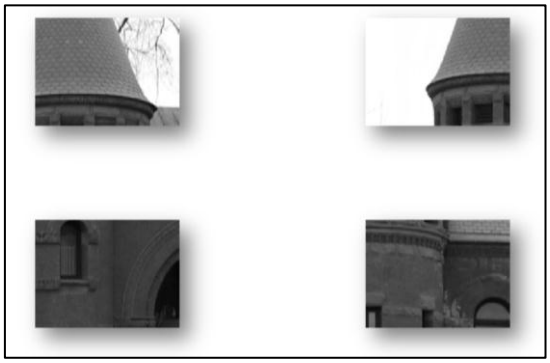


شکل (۷): مکان جعل‌شده در تصویر نمونه شکل (۶ ب)

در شکل (۸) نیز نمونه‌هایی از تصاویر مشخص‌شده از نقاط جعل نشان داده شده است؛ نقاط سفید به مفهوم نقاط سفید به مفهوم نقاط جعل‌شده و نقاط مشکی بدون تغییر است. بنابراین برای محاسبهٔ عملکرد ایدهٔ پژوهش، نتایج یافت‌شده به این شکل و به‌صورت نسبت محاسبه شده است. هرچه تعداد نقاط یافت‌شده توسط پژوهش به این تصویر شبیه‌تر باشد، عملکرد بهتری نسبت به دیگر الگوریتم‌ها دارد. در بخش بعدی، هرکدام از تصاویر پس از فراخوانی به بلوک‌هایی تقسیم شده است. این بلوک‌ها به‌اندازهٔ ۰/۱ از تصویر انتخاب شده است. اندازهٔ تصویر شکل (۷)، ۹۸۰ پیکسل در ۱۳۰۶ پیکسل است؛ بنابراین اندازهٔ بلوک‌ها نیز به میزان ۹۸ پیکسل در ۱۳۰ پیکسل جداسازی شده؛ همچنین نمونه‌هایی از این بلوک‌ها در شکل (۹) نشان داده است. سپس یکی از نمونه‌های شکل (۹) انتخاب شده و ویژگی آن در جدول (۲) ارائه شده است.

(ب) (الف)

شکل (۸): نمونه ماسک‌های تشخیص مکان‌های جعل در تصاویر (در تصاویر الف، بخشی از تصویر کپی و در همان تصویر اضافه شده است. در تصاویر ب، نواحی جعل‌شده با نقاط سفید مشخص شده است) [۱۳]



شکل (۹): نمونه‌هایی از بلوک‌های جداشده از تصویر شکل (۶) (ب)

در بخش بعدی پژوهش، یکی از نمونه‌های شکل (۹) انتخاب و ویژگی آن در جدول (۲) ارائه شد. در این جدول، پس از استخراج هر بلوک ویژگی‌های آن استخراج شده است. توسط این روش و رسم دایره‌هایی روی تصویر می‌توان جهت و تمرکز نقاط را روی تصویر مورد مقایسه قرار داد. در این پژوهش، ۱۱ دایرهٔ هم‌مرکز روی تصویر رسم شده است و تعداد نقاط مهم در هر دایره شمارش می‌گردد. در این حالت، می‌توان تمرکز نقاط را در دوایر مورد بررسی و مقایسه قرار داد.

جدول (۲): ویژگی‌های استخراج از یک بلوک نمونه شکل (۶) (ب)

Sift	KAZE	HoG	Zernik
۲۴۰۴/۰۰	۱۸۸/۰۰	۴۹۸۸/۰۰	۸۳۹/۴۰
۱۱۸۱/۰۰	۱۸۸/۰۰	۲۵۲۶/۰۰	۰/۵۰
۶۸۵/۰۰	۱۸۸/۰۰	۱۳۳۸/۰۰	۰۱/۴۱
۳۹۹/۰۰	۱۸۸/۰۰	۳۹۵/۰۰	۰/۰۹
۱۹۷/۰۰	۱۸۸/۰۰	۱۳۱۷/۰۰	۱/۳۴
۵۶/۰۰	۱۸۸/۰۰	۳۵۳/۰۰	۰/۸۸
۱۴/۰۰	۱۸۸/۰۰	۵۶/۰۰	۲/۱۸
۴۲/۰۰	۱۸۸/۰۰	۱/۰۰	۱/۰۰
۳۹/۰۰	۱۸۸/۰۰	۴/۰۰	۱/۱۱
۱۸۸/۰۰	۱۶۸۹۹/۰۰	۰/۰۰	۱/۴۶

در صورت مقایسهٔ دو بلوک می‌توان به‌صورت شکل‌های ۱۰، ۱۱، ۱۲ و ۱۳ عمل کرد. در این شکل‌ها مقایسهٔ هرکدام از ویژگی‌ها با فاصلهٔ اقلیدسی به دست آمده و میزان فاصلهٔ دو بلوک محاسبه شده است. بخش‌هایی از بلوک‌ها که بر هم منطبق شده، نشانهٔ نقاط جعل در تصویر است.

۴ـ۴. پیاده‌سازی الگوریتم ژنتیک و انتخاب ویژگی‌های مؤثر

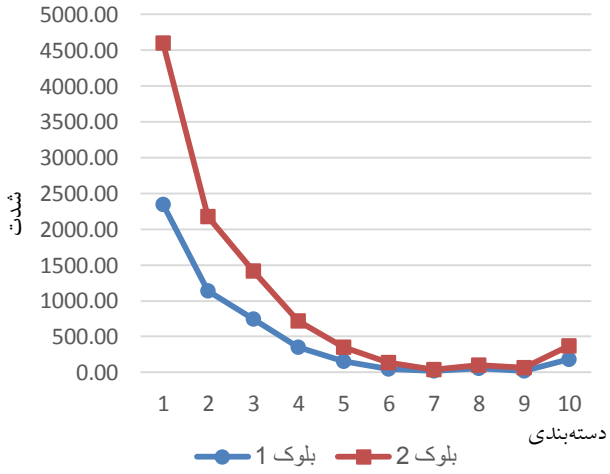
برای بهبود سیستم و افزایش دقت و سرعت از الگوریتم ژنتیک استفاده می‌شود. در الگوریتم ژنتیک ۵۰ کروموزوم در نظر گرفته شده و هر کروموزوم به‌صورت رابطهٔ (۹) تعریف می‌شود. این الگوریتم با ۱۰۰ بار تکرار داده‌های مناسب را برای تشخیص جنسیت از میان داده‌های ترکیبی انتخاب کرده و از این طریق، حجم داده‌ها کاهش می‌یابد.

رابطهٔ (۹): تابع هزینه= میانگین درصد خطای تشخیص×۰/۵ + تعداد ویژگی انتخاب شده×۰/۵

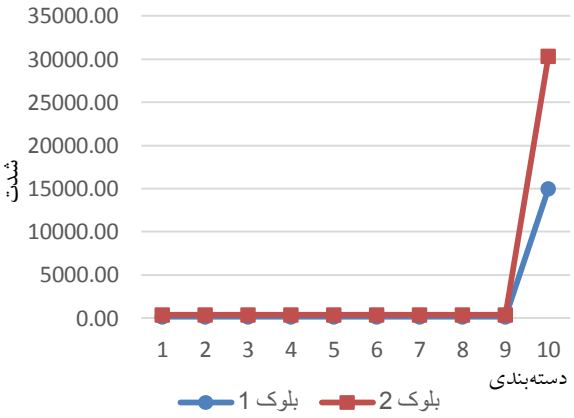
شایان ذکر است هر کروموزوم یک راه‌حل کاهش بعد در این پژوهش است؛ هریک از اعضای این کروموزوم یک عدد بین صفر تا یک در نظر گرفته می‌شود. این اعداد احتمال حضور این کروموزوم را مشخص می‌کنند. اعداد بیشتر از ۰/۵ به‌عنوان حضور آن و عدد زیر ۰/۵ به‌عنوان عدم حضور تعیین شده است. ژن انتخاب ویژگی نیز به‌صورت رابطهٔ (۱۰) نیز به دست می‌آید.

رابطهٔ (۱۰): ژن انتخاب ویژگی

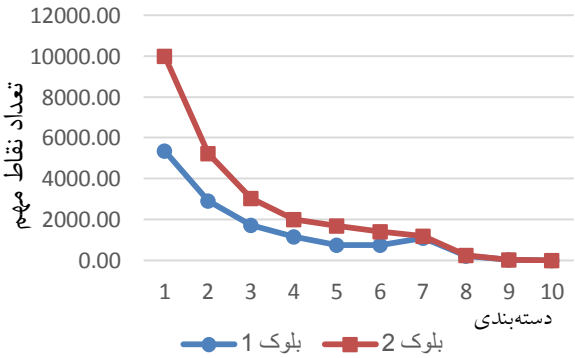
$$Gen=[a1\ a2\ a3\ \dots\dots\dots\ a40]$$



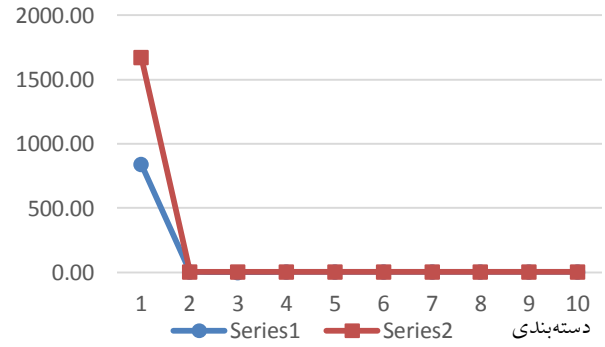
شکل (۱۰): مقایسهٔ بردارهای Sift دو بلوک از یک تصویر



شکل (۱۱): مقایسهٔ بردارهای KAZE دو بلوک از یک تصویر



شکل (۱۲): مقایسهٔ بردارهای HoG دو بلوک از یک تصویر



شکل (۱۳): مقایسهٔ بردارهای Zernike دو بلوک از یک تصویر

در جدول (۳) نمونه‌ای از بردار انتخاب ویژگی نشان داده شده است. در این جدول، شمارهٔ ویژگی‌ها و ارزشی که الگوریتم ژنتیک به آن داده ارائه شده است.

در جدول (۴) بر اساس جدول (۳)، حضور و عدم حضور ویژگی‌ها مشخص می‌شود. ویژگی‌هایی که ارزش آن‌ها بیشتر از عدد ۰/۵ باشد مورد قبول است؛ در غیر این صورت در ادامه از آن ویژگی‌ها استفاده نمی‌شود.

جدول (۳): نمونهٔ ارزش ژن انتخاب ویژگی

ویژگی	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
ارزش	۰/۲۳	۰/۵۸	۰/۳۴	۰/۶۷	۰/۶۰	۰/۲۰	۰/۱۸	۰/۳۶	۰/۵۳	۰/۵۵
ویژگی	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
ارزش	۰/۲۸	۰/۳۴	۰/۹۰	۰/۶۲	۰/۲۸	۰/۷۲	۰/۱۹	۰/۰۸	۰/۱۷	۰/۴۱
ویژگی	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10
ارزش	۰/۳۵	۰/۲۴	۰/۲۶	۰/۶۴	۰/۵۶	۰/۰۹	۰/۶۷	۰/۸۹	۰/۷۱	۰/۴۳
ویژگی	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8	Z9	Z10
ارزش	۰/۶۷	۰/۴۴	۰/۲۹	۰/۷۱	۰/۷۵	۰/۵۴	۰/۱۹	۰/۴۶	۰/۲۶	۰/۲۸

جدول (۴): ویژگی‌های انتخاب‌شده بر اساس کروموزوم جدول (۳)

نوع ویژگی	Zernike	HOG	KAZE	SIFT
انتخاب‌شده	۱-۴-۵-۶	۴-۵-۷-۸-۹	۳-۴-۶	۲-۴-۵-۹-۱۰

هزینهٔ محاسبه‌شده برای این کروموزوم به میزان ۰/۲۶۹۸ درصد است. نمونهٔ کروموزوم دیگر که در این نسل ایجاد شده، به‌صورت جدول (۵) است.

در مرحلهٔ بعد، ویژگی‌ها با استفاده از عملگرهای ادغام تک‌نقطه‌ای و دونقطه‌ای و همچنین جهش کروموزوم‌ها به‌روز می‌شوند؛ که در جدول (۶) نتیجهٔ به‌روزرسانی کروموزوم‌ها نشان داده شده است.

جدول (۵): ویژگی‌های انتخاب‌شده توسط کروموزوم‌های نمونه

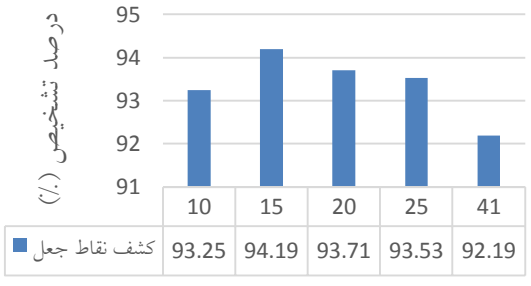
شمارهٔ کروموزوم	Zernike	HOG	KAZE	SIFT	ارزش
۱	۱-۴-۵-۶	۴-۵-۷-۸-۹	۳-۴-۶	۲-۴-۵-۹-۱۰	۰/۲۶۹۸
۲	۲-۳-۸-۹	۵-۷-۸	۶-۸-۱۰	۳-۴-۸	۰/۲۴۳۰
۳	۱-۷-۱۰	۵-۹	۴	۵-۶-۷-۹	۰/۲۷۴۹
۴	۳-۴	۲-۸-۱۰	۳-۷-۸	۵-۹	۰/۲۶۵۹

جدول (۶): به‌روزرسانی کروموزوم‌های جدول (۵)

شماره کروموزوم	توضیحات	Zernike	HOG	KAZE	SIFT	ارزش
۱	ادغام تک‌نقطه‌ای	۱-۴-۵-۶	۴-۵-۷-۸-۹	۳-۴-۸-۱۰	۳-۴-۸	۰/۲۰۶۸
۲	ادغام تک‌نقطه‌ای	۲-۳-۸-۹	۵-۷-۸	۶	۲-۴-۵-۹-۱۰	۰/۱۸۹۲
۳	ادغام دونقطه‌ای	۱-۷-۱۰	۵-۸-۱۰	۳-۷-۸	۵-۶-۷-۹	۰/۳۲۵۷
۴	ادغام دونقطه‌ای	۳-۴	۲-۹	۴	۵-۹	۰/۲۶۷۱
۵	جهش	۱-۶	۴-۵-۹	۳-۵-۸	۲-۴-۶-۹-۱۰	۰/۲۰۶۷

۴ـ۵. پیاده‌سازی الگوریتم تحلیل مؤلفهٔ اصلی و کاهش ابعاد ویژگی‌ها

در این بخش، پس از اعمال الگوریتم تحلیل مؤلفهٔ اصلی به بررسی عملکرد سیستم پرداخته، میزان کاهش ابعاد به‌صورت شکل (۱۴) در نظر گرفته شده و همچنین میزان کشف نقاط جعل نیز بررسی شده است.



شکل (۱۴): بررسی درصد تشخیص میزان کشف جعل به‌ازای کاهش ابعاد مختلف

همان طور که در شکل (۱۴) مشاهده می‌شود، با تغییر ابعاد ویژگی‌های استخراج‌شده، میزان درصد تشخیص نیز تغییر می‌کند. نتایج پژوهش نشان داد که با کاهش ابعاد به میزان ۱۵ بعد، می‌توان درصد تشخیص را به میزان ۹۴/۱۹درصد بهبود داد. که این میزان نسبت به زمانی که از تمامی ابعاد ویژگی‌ها استفاده می‌شود، درصد تشخیص را به میزان حدود ۲درصد بهینه می‌کند.

۵. نتایج پژوهش

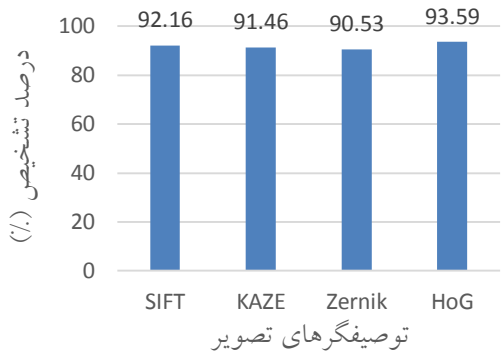
برای ارزیابی سیستم، آزمایشاتی با درنظر گرفتن انتخاب داده‌های مناسب و کاهش ابعاد داده‌ها به‌صورت جداگانه و ترکیبی طراحی شده و میزان تأثیر آن‌ها بر تشخیص نقاط جعل مورد بررسی قرار گرفته است. جدول(۷) عناوین آزمایشات را نشان می‌دهد.

جدول (۷): عناوین آزمایش‌ها

ردیف	عنوان آزمایش
۱	بررسی میزان تشخیص جعل توسط هریک از توصیفگرها به‌صورت جداگانه
۲	بررسی میزان تشخیص جعل به‌وسیلهٔ ترکیب توصیفگرهای SIFT، KAZE، Zernike و HOG
۳	بررسی عملکرد الگوریتم ژنتیک بر انتخاب ویژگی‌های مناسب با استفاده از توصیفگرهای SIFT، KAZEج، Zernike و HOG
۴	بررسی عملکرد روش تحلیل مؤلفهٔ اصلی بر کاهش ابعاد داده‌های استخراج‌شده از توصیفگرهای SIFT، KAZE، Zernike و HOG

همان طور که در جدول (۷) مشاهده می‌شود، در این پژوهش چهار آزمایش در نظر گرفته شده است. در آزمایش اول به دنبال یافتن میزان ارزش هریک از توصیفگرها برای کشف نقاط جعل در تصاویر پایگاه داده هستیم. در این آزمایش هریک از توصیفگرها جداگانه بررسی شده‌اند. در آزمایش دوم، سه نوع ترکیب از ویژگی‌ها بررسی می‌شوند. در این مرحله، هیچ‌یک از ابعاد این ویژگی‌ها حذف نشدند. در این بخش نیز تأثیر استفاده از چند توصیفگر به‌طور هم‌زمان بررسی شده است. در آزمایش سوم، با استفاده از الگوریتم ژنتیک ابعادی از این ویژگی‌ها انتخاب شده است. در واقع تنها با این ابعاد به مقایسهٔ بلوک‌ها پرداخته می‌شود تا به هدف این بخش که کاهش ابعاد ویژگی‌ها و کاهش میزان خطای تشخیص است برسیم. در مرحله چهارم، با استفاده از تحلیل مؤلفهٔ اصلی به دنبال کاهش ابعاد نیز هستیم. در نتیجه با کاهش ابعاد، میزان تشخیص مکان‌های جعل تصاویر بررسی می‌شود.

پایگاه داده مقایسه‌شده و میزان تشابه مکان‌های تشخیص داده‌شده محاسبه می‌شود. هریک از توصیفگرها ویژگی‌های منحصربه‌فردی از بلوک‌ها را استخراج کرده‌اند که می‌توان آن‌ها را مورد مقایسه قرار داد.



شکل (۱۵): مقایسهٔ درصد تشخیص هریک از توصیفگرها

همان طور که در شکل (۱۵) مشاهده می‌شود، دو توصیفگر HOG و SIFT از دیگر توصیفگرها درصد تشخیص بهتری دارد. توصیفگر HOG نسبت به توصیفگر SIFT به میزان ۲درصد و نسبت به توصیفگر Zernike به میزان ۴درصد تشخیص بهتری در نقاط جعل‌شده دارد.

۵ـ۱. بررسی میزان تشخیص جعل توسط هریک از توصیفگرها

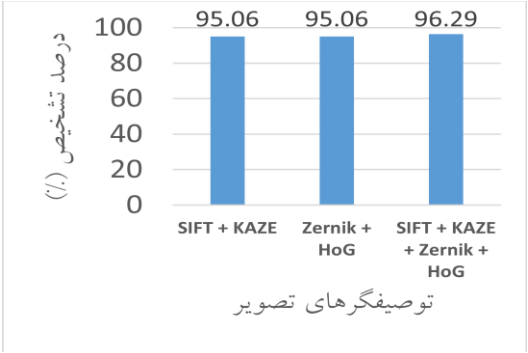
در این بخش از آزمایش، هریک از توصیفگرها برای تشخیص نقاط جعل به‌صورت جداگانه روی تصاویر پایگاه داده اعمال شده و نتایج با یکدیگر در شکل (۱۶) مقایسه شده است. برای مشخص کردن میزان عملکرد، نقاط یافته‌شده توسط هریک از الگوریتم‌ها با نقاط تعیین‌شده در پایگاه داده مقایسه شده و میزان تشابه مکان‌های تشخیص داده‌شده محاسبه می‌شود. هریک از توصیفگرها ویژگی‌های منحصربه‌فردی از بلوک‌ها را استخراج کرده‌اند که می‌توان آن‌ها را مورد مقایسه قرار داد.

همان طور که در شکل (۱۵) مشاهده می‌شود، توصیفگر HOG و SIFT از دیگر توصیفگرها درصد تشخیص بهتری دارد. توصیفگر HOG نسبت به توصیفگر SIFT به میزان

۲درصد و نسبت به توصیفگر Zernike به میزان ۴درصد تشخیص بهتری در نقاط جعل‌شده دارد.

۵ـ۲. بررسی میزان تشخیص جعل توسط ترکیب توصیفگرهای SIFT، KAZE، Zernike و HOG

در این بخش برخلاف آزمایش گذشته، تمامی ابعاد ویژگی‌ها با یکدیگر در تشخیص نقاط جعل استفاده و ترکیباتی از این ویژگی‌ها در نظر گرفته و نتایج نیز محاسبه شده است. ترکیب توصیفگرها سبب می‌شود تا چندین ویژگی منحصربه‌فرد با یکدیگر در تشخیص مکان جعل شرکت کنند. هیچ‌یک از ابعاد این توصیفگرها حذف نشده‌اند؛ در نتیجه با ترکیب آن‌ها حجم محاسبات نیز بیشتر می‌شود.

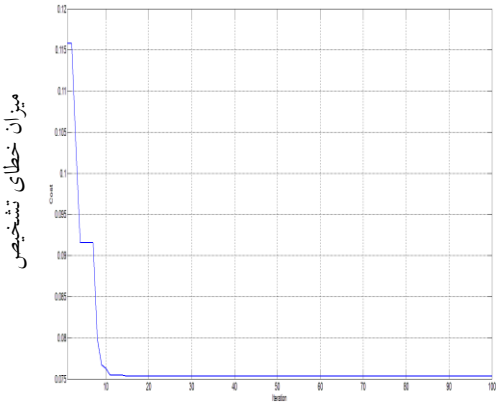


شکل (۱۶): مقایسهٔ درصد تشخیص ترکیب‌هایی از توصیفگرها

همان طور که در شکل (۱۶) مشاهده می‌شود، ترکیب تمامی ابعاد ویژگی‌ها نیز می‌تواند عملکرد سیستم را تغییر دهد. نتایج نشان می‌دهد ترکیب تمامی توصیفگرها با یکدیگر سبب می‌شود که عملکرد سیستم به میزان ۳درصد نسبت به بهترین توصیفگر آزمایش قبل (HoG) بهبود یابد.

۵ـ۳. بررسی عملکرد الگوریتم ژنتیک بر انتخاب ویژگی‌های مناسب با استفاده از توصیفگرهای SIFT، KAZE، Zernike و HOG

الگوریتم ژنتیک برای انتخاب ویژگی‌های مؤثر بر تشخیص نقاط بهتر جعل‌شده در تصویر استفاده شده است. همان طور که بیان شد، تعداد کروموزوم‌ها در این بخش برای هر نسل ۱۰۰ عدد در نظر گرفته شد. هریک از کروموزوم‌ها از ۴۰ ژن تشکیل شده‌اند. هرکدام از این ژن‌ها نشان‌دهندهٔ احتمال انتخاب ابعاد آن است. هدف انتخاب کمترین تعداد ویژگی برای کاهش خطای تشخیص نقاط جعل است. شکل (۱۷) بهترین عملکرد هر نسل را نشان می‌دهد. همان طور که در شکل (۱۷) مشاهده می‌شود، الگوریتم ژنتیک توانسته مؤثرترین ویژگی‌ها برای تشخیص نقاط جعل را با در نظر گرفتن میزان محاسبات و میزان خطای تشخیص بیابد.



شکل (۱۷): یافتن بهترین جواب برای مسئلهٔ انتخاب ویژگی

در ادامه، جدول (۸) ویژگی‌های انتخاب‌شده را نشان می‌دهد.

همان طور که در جدول (۹) مشاهده می‌شود، الگوریتم ژنتیک در فضای جست‌وجوی خود، مقادیری را به دست آورده است که میزان خطای تشخیص را به ۹۶/۹۴٪ می‌رساند. این ویژگی‌ها شش عدد است که نسبت به تمامی ویژگی‌های در نظر گرفته‌شده کمتر می‌باشد، در نتیجه حجم محاسبات نیز کم شده است. نتایج نشان می‌دهد میزان تشخیص جعل تصاویر با این ویژگی‌ها به میزان ۰/۶٪ در درستی تشخیص تأثیر دارد و به میزان ۱۵ برابر، حجم محاسبات را کاهش می‌دهد.

جدول (۸): نمونهٔ ارزش ژن انتخاب ویژگی

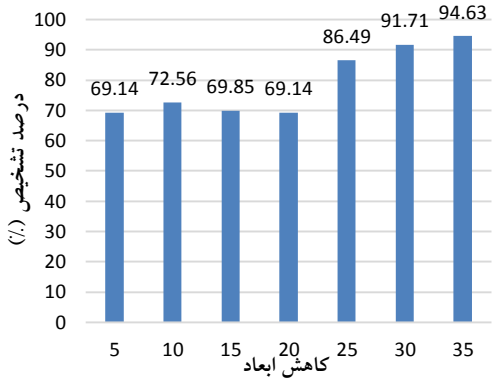
ویژگی	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
ارزش	۰/۲۳	۰/۰۵	۰/۵۳	۰/۶۸	۰/۲۱	۰/۲۰	۰/۱۸	۰/۲۶	۰/۲۶	۰/۵۵
ویژگی	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**
ارزش	۰/۷۱	۰/۲۴	۰/۷۵	۰/۶۴	۰/۲۶	۰/۰۹	۰/۶۷	۰/۰۹	۰/۱۸	۰/۴۳

جدول (۹): ویژگی‌های به‌دست‌آمده از خروجی الگوریتم ژنتیک

نوع ویژگی	Zernike	HOG	KAZE	SIFT	تعداد ویژگی‌ها	درصد خطای تشخیص
انتخاب‌شده	–	۱-۳-۴-۷	–	۳-۴	۶	۳/۰۶

۵ـ۴. بررسی عملکرد روش تحلیل مؤلفهٔ اصلی برکاهش ابعاد داده‌های استخراج شده از توصیفگرهای SIFT، KAZE، Zernike و HOG

همان طور که در شکل (۱۸) مشاهده می‌شود، به‌ازای Pهای مختلف، میزان تشخیص نقاط جعل بررسی شده است. این شکل نشان می‌دهد هرچه میزان کاهش ابعاد بیشتر باشد، میزان عملکرد تشخیص نیز کاهش می‌یابد. بهترین میزان تشخیص در کاهش ابعاد تمامی توصیفگرها به میزان ۹۴/۶۳٪ است.



شکل (۱۸): درصد تشخیص به‌ازای ابعاد کاهش‌یافته

۶. نتیجه‌گیری

جعل کپی-انتقال تصویر که بخش یا بخش‌هایی از یک تصویر در همان تصویر کپی می‌شوند، یکی از روش‌های مرسوم در جعل تصاویر است. در این مقاله برخی از توصیفگرها مانند SIFT، KAZE، Zernike و HOG در جهت آشکارسازی این نوع جعل مورد ارزیابی قرار گرفتند. نتایج نشان داد توصیف‌گر HOG نسبت به دیگر روش‌ها عملکرد بهتری از خود نشان می‌دهد. این عملگر توانسته است با دقت ۹۳/۵۹٪ نقاط جعل را بیابد. به‌علاوه نتایج نشان داد ترکیب کردن این توصیفگرها سبب افزایش عملکرد تشخیص می‌شود. اما از طرفی، حجم محاسبات و سرعت تشخیص نیز کاهش می‌یابد. در ادامه، از الگوریتم ژنتیک به‌عنوان انتخاب‌کنندهٔ بهترین ویژگی‌ها استفاده شد. نتایج نشان داد که می‌توان با انتخاب شش ویژگی به درصد تشخیص ۹۶/۹۴٪ دست یافت. همچنین با استفاده از تحلیل مؤلفهٔ اصلی نیز در صورت کاهش ابعاد به ۳۵ بعد، می‌توان درصد تشخیص ۹۴/۶۳٪ را به دست آورد.

مراجع

[1] Warif N. B. A., Wahab A. W. A., Idris M. Y. I., Ramli R., Salleh R., Shamshirband S., and Choo K. R., "*Copy-move forgery detection: Survey, challenges and future directions*", J. Netw. Comput. Appl., vol. 75, pp. 259–278, 2016.

[2] Yang F., Li J., Lu W., and Weng J., "*Copy-move forgery detection based on hybrid features*", Eng. Appl. Artif. Intell., vol. 59, pp. 73–83, 2017.

[3] Oreski S. and Oreski G., "*Genetic algorithm-based heuristic for feature selection in credit risk assessment*", Expert Syst. Appl., vol. 41, no. 4, pp. 2052–2064, 2014.

[4] Espejo P. G., Ventura S., and Herrera F., "*A survey on the application of genetic programming to classification*", IEEE Trans. Systems, Man, and Cybernetics, Part C, vol. 40, no. 2, pp. 121–144, 2010.

[5] Poon B., Amin M. A., and Yan H., "*Improved methods on pca based human face recognition for distorted images*", in International Multi-Conference of Engineers and Computer Scientists, Hong Kong, vol. 1, 2016.

[6] Ng S. C., "*Principal component analysis to reduce dimension on digital image*", Procedia Computer Science, vol. 111, pp. 113–119, 12 2017.

[7] Mohan M. and Preetha V., "*Gabor filter hog based copy move forgery detection*", in IOSRJournal of Electronics and Communication Engineering (IOSR-JECE), 2017, pp. 41–45.

[8] Amerini I., Ballan L., Caldelli R., Bimbo A. D., and Serra G., "*A siftbased forensic method for copy-move attack detection and transformation recovery*", IEEE Trans. Information Forensics and Security, vol. 6, no. 3-2, pp. 1099–1110, 2011.

[9] Alcantarilla P. F., Bartoli A., and Davison A. J., "*KAZE features*", in Computer Vision - ECCV 2012 - 12th European Conference on Computer Vision, Florence, Italy, October 7-13, 2012, Proceedings, Part VI, 2012, pp. 214–227.

[10] Ryu S., Lee M., and Lee H., "*Detection of copy-rotate-move forgery using zernike moments*", in Information Hiding - 12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010, Revised Selected Papers, 2010, pp. 51–65.

[11] Zhao Y., Wang S., Zhang X., and Yao H., "*Robust hashing for image authentication using zernike moments and local features*", IEEE Trans. Information Forensics and Security, vol. 8, no. 1, pp. 55–63, 2013.

[12] Muhammad G. and Hussain M., "*Passive detection of copy-move image forgery using undecimated wavelets and zernike moments*", International journal on information, vol. 16, pp. 1343–4500, 05 2013.

[13] Conotter V., "*Active and passive multimedia forensics*", Ph.D. dissertation, University of Trento, 2011.

[14] Al-Sawadi M. S., "*Automatic detection of copy-move image forgery based on clustering technique*", Master's thesis, King Saud University, 2013.

[15] Popescu A. C. and Farid H., "*Exposing digital forgeries by detecting duplicated image regions*", Department of Computer Science, Dartmouth College, Tech. Rep., 2004.

[16] Zimba M. and Xingming S., "*Dwt-pca (evd) based copy-move image forgery detection*", International Journal of Digital Content Technology and its Applications, vol. 5, pp. 251–258, 01 2011.

[17] Kang X. and Wei S., "*Identifying tampered regions using singular value decomposition in digital image forensics*", in International Conference on Computer Science and Software Engineering, CSSE 2008, Volume 3: Grid Computing / Distributed and Parallel Computing / Information Security, December 12-14, 2008, Wuhan, China, 2008, pp. 926–930.

[18] Davarzani R., Yaghmaie K., Mozaffari S., and Tapak M., "*Copy-move forgery detection using multiresolution local binary patterns*", Forensic science international, vol. 231, pp. 61–72, 09 2013.

[19] Christlein V., Riess C., and Angelopoulou E., "*On rotation invariance in copy-move forgery detection*", in 2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010, pp. 1–6.

[20] Espejo P. G., Ventura S., and Herrera F., "*A survey on the application of genetic programming to classification*", IEEE Trans. Systems, Man, and Cybernetics, Part C, vol. 40, no. 2, pp. 121–144, 2010.

[21] Shabanifard M., Shayesteh M. G., and Akhaee M. A., "*Forensic detection of image manipulation using the zernike moments and pixel-pair histogram*", IET Image Processing, vol. 7, no. 9, pp. 817–828, December 2013.

[22] Cao Y., Gao T., Fan L., and Yang Q., "*A robust detection algorithm for copy-move forgery in digital images*", Forensic Science International, vol. 214, no. 1, pp. 33 – 43, 2012.

[23] Sreelakshmy I. and Kovoor B., *Hybrid Method for Copy-Move Forgery Detection in Digital Images*, 01 2019, pp. 119–127.

[24] Wang C., Zhang Z., and Zhou X., "*An image copy-move forgery detection scheme based on A-KAZE and SURF features*", Symmetry, vol. 10, no. 12, p. 706, 2018.

[25] Lee J., Chang C., and Chen W., "*Detection of copy-move image forgery using histogram of orientated gradients*", Inf. Sci., vol. 321, pp. 250–262, 2015.

[26] Zhang Z., Wang G., Bian Y., and Yu Z., "*A novel model for splicing detection*", in Fifth International Conference on Bio-Inspired Computing: Theories and Applications, BIC-TA 2010, University of Hunan, Liverpool Hope University, Liverpool, United Kingdom / Changsha, China, September 8-10 and September 23-26, 2010, 2010, pp. 962–965.

[27] Amerini I., Ballan L., Caldelli R., Bimbo A. D., and Serra G., "*A siftbased forensic method for copy-move attack detection and transformation recovery*", IEEE Trans. Information Forensics and Security, vol. 6, no. 3-2, pp. 1099–1110, 2011.

[28] Pan X. and Lyu S., "*Detecting image region duplication using SIFT features*", in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2010, 14-19 March 2010, Sheraton Dallas Hotel, Dallas, Texas, USA, 2010, pp. 1706–1709.

[29] Amerini I., Ballan L., Caldelli R., Bimbo A. D., Tongo L. D., and Serra G., "*Copy-move forgery detection and localization by means of robust clustering with j-linkage*", Signal Process. Image Commun., vol. 28, no. 6, pp. 659–669, 2013.

[30] Costanzo A., Amerini I., Caldelli R., and Barni M., "*Forensic analysis of SIFT keypoint removal and injection*", IEEE Trans. Information Forensics and Security, vol. 9, no. 9, pp. 1450–1464, 2014.

[31] Lynch G., Shih F. Y., and Liao H. M., "*An efficient expanding block algorithm for image copy-move forgery detection*", Inf. Sci., vol. 239, pp. 253–265, 2013.

[32] Pan X. and Lyu S., "*Region duplication detection using image feature matching*", IEEE Trans. Information Forensics and Security, vol. 5, no. 4, pp. 857–867, 2010.

[33] Ketenci S. and Ulutas G., "*Copy-move forgery detection in images via 2d-fourier transform*", in 36th International Conference on Telecommunications and Signal Processing, TSP 2013, Rome, Italy, 2-4 July, 2013, 2013, pp. 813–816.

[34] Kang X., Stamm M. C., Peng A., and Liu K. J. R., "*Robust median filtering forensics using an autoregressive model*", IEEE Trans. Information Forensics and Security, vol. 8, no. 9, pp. 1456–1468, 2013.

[35] Le-Tien T., Phan-Xuan H., Nguyen Chinh T., and Do-Tieu T., "*Image forgery detection: A low computational-cost and effective data-driven model*", International Journal of Machine Learning and Computing, vol. 9, pp. 181–188, 04 2019.