Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

تکنیک‌های تشخیص جعل کپی-جابجایی مبتنی بر روش‌های سنتی در تصاویر دیجیتال

مریم عطائی قهفرخی[۱]، آذر محمودزاده [۲*]

۱- گروه مهندسی برق، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران
mari.attaie1994@gmail.com
۲- گروه مهندسی برق، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران
azar_mahmoodzadeh@yahoo.com

چکیده: جعل تصویر، یکی از زمینه‌های بسیار پر کاربرد در پردازش تصویر است که به صورت گسترده مورد توجه و مطالعه پژوهشگران قرار گرفته است. انواع مختلفی برای جعل تصویر دیجیتال موجود است که جعل کپی-جابجایی یکی از نمونه‌های رایج است که تشخیص این نوع جعل بسیار حائز اهمّیّت است. در این مقاله، ضمن معرفی مفاهیم جعل کپی-جابجایی تصویر، به بررسی مراحل، دسته‌بندی روش‌های تشخیص و سوگیری تحقیقات در این زمینه پرداخته شده‌است. این مقاله می‌تواند راهگشای پژوهشگران پردازش تصویر در فرآیند تشخیص جعل کپی-جابجایی باشد. اهتمام نویسندگان بر این بوده است که همه جنبه‌های این فرآیند مورد کاوش قرار گیرد.

واژه های کلیدی: جعل کپی-جابجایی تصویر، شناسایی جعل، پردازش تصویر، تصویر دیجیتال.

Copy-Move Forgery Detection Techniques based on Traditional Methods in Digital Images

Maryam Attaie Gahfarkhi [1], Azar Mahmoodzadeh[2*]

[1] Department of Electrical Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran
mari.attaie1994@gmail.com
[2] Department of Electrical Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran
Azar.mahmoodzadeh@iau.ac.ir

Abstract:
Image forgery is one of the most widely used fields in image processing, which has been widely studied and studied by researchers. There are different types of digital image forgery, copy-move forgery is one of the common examples, and it is very important to recognize this type of forgery. In this review article, while introducing the concepts of copy-move image forgery, the steps, classification of detection methods and research bias in this field have been discussed. This article can open the way for image processing researchers in the process of detecting copy-move forgery. The authors' effort has been to explore all aspects of this process.
Keywords: Copy-Move Image Forgery, Forgery Detection, Image Processing, Digital Image.

نوع مقاله: پژوهشی
تاریخ ارسال مقاله: ۱۴۰۲/۰۱/۰۵ تاریخ پذیرش مقاله: ۱۴۰۲/۰۲/۱۱ تاریخ چاپ مقاله: ۱۴۰۲/۰۳/۱۲
DOI: 00.00000/0000

* نویسنده‌ی مسئول؛ نشانی: ایران – شیراز –دانشگاه آزاد اسلامی شیراز – دانشکده مهندسی – گروه مهندسی برق

۱- مقدمه

محتوای دیجیتال همچون تصاویر، ویدئوها و فایل‌های صوتی، هر روز در شبکه‌های اجتماعی به طور گسترده استفاده می‌شوند که تصاویر، محبوب‌ترین منابع اشتراکی می‌باشند. در سال‌های اخیر با توسعه نرم افزارهای پیشرفته پردازش تصویر، تصاویر را می‌توان به راحتی بدون باقی ماندن ردپای محسوس جعل کرد. بنابراین، شناسایی خودکار تصاویر دستکاری شده برای کاربران عملی دشوار است [۱, ۲]. در نتیجه ابزارهای تشخیص جعل تصاویر دیجیتالی از اهمیّت ویژه‌ای برخوردار است.

روش‌های جعل به‌طورکلی به دو دسته عمده، روش‌های فعال و روش‌های غیرفعال تقسیم می‌شوند [۳]. روش‌های فعال، ویژگی‌های مبهم را از تصاویر بازیابی می‌کنند. روش‌هایی که از کیفیت ذاتی تصویر برای شناسایی جعلیات استفاده می‌کنند، شامل تکنیک‌های غیرفعال هستند که به دنبال کشف ناهنجاری‌ها در متغیرهای آماری، تفاوت‌ها در رنگ و بافت، و فشرده‌سازی مضاعف JPEG هستند. اخیرا روش‌های غیرفعال به طور گسترده استفاده می‌شود.

جعل کپی-جابجایی تصویر، یکی از روش‌های غیرفعال است که در این نوع جعل، بخش‌هایی (شی یا فرد) از تصویر کپی می‌شود و به منطقه دیگری از همان تصویر یا تصویر دیگر و با یا بدون دستکاری(تبدیل هندسی) گذاشته می‌شود. این روش یکی از متداول‌ترین و ساده‌ترین نوع جعل می‌باشد که در سال‌های اخیر مورد توجه محققان زیادی قرار گرفته است که این نشان دهنده اهمیّت به این موضوع می‌باشد. با این حال، تاکنون مقاله مروری به زبان فارسی ارائه نشده است. همچنین مقالات انگلیسی اندکی در این زمینه وجود دارد که عمدتاً به بررسی تعداد معدودی از روش‌های تشخیص جعل کپی-جابجایی پرداخته‌اند[۱-۳] . از طرف دیگر مقالات مروری که اخیرا چاپ شده فقط به نوع خاصی از روش‌های تشخیص جعل کپی-جابجایی پرداخته‌اند [۴-۶]. اهمیّت و کاربرد روزافزون تشخیص جعل کپی جابجایی نشان می‌دهد که هر پنج سال یک‌بار باید یک مقاله مروری در این زمینه نوشته شود تا بتواند دانشمندان در جهت ارتقا عملکرد فرآیند تشخیص خطای کپی-جابجایی راهنمایی کند. چنین مقالاتی می‌توانند راهگشای محققان در انتخاب مناسب و بهره‌گیری از این الگوریتم‌ها در کاربردهای مورد علاقه‌شان باشد. موارد ذکر شده، انگیزه بخش نگارش این مقاله در خصوص تشخیص جعل کپی-جابجایی بوده است. هدف این مقاله، بررسی انواع جعل، تشریح مراحل تشخیص جعل کپی-جابجایی تصویر، بررسی روش‌های تشخیص جعل کپی-جابجایی تصویر، تشریح دیتابیس موجود و معیارهای ارزیابی پرداخته می‌شود.

سازمان‌دهی مقاله به این صورت است که در بخش دوم به بررسی انواع جعل تصاویر دیجیتال، در بخش سوم به شرح مراحل تشخیص جعل کپی-جابجایی و در بخش چهارم، به بررسی روش‌های تشخیص جعل کپی-جابجایی پرداخته می‌شود. دیتابیس‌های رایج، معیارهای ارزیابی، و رویکردهای جدید به ترتیب در بخش پنجم، ششم، و هفتم، و در نهایت به جمع‌بندی در بخش هشتم پرداخته می‌شود.

۲- انواع جعل تصاویر دیجیتال

جعل تصاویر دیجیتال را به طور کلی می‌توان به پنج دسته، جعل کپی-جابجایی تصویر، پیوند زدن تصویر، روتوش کردن تصویر، مورفولوژی و بهبود تصاویر تقسیم کرد (شکل ۱) [۶]. جعل کپی-جابجایی تصویر، یکی از رایج‌ترین انواع جعل تصاویر دیجیتال است [۷].

۳- مراحل تشخیص جعل کپی-جابجایی

تشخیص جعل کپی-جابجایی به طور کلی از پنج مرحله اصلی تشکیل شده است که این مراحل در همه روش‌های تشخیص جعل کپی-جابجایی تقریبا یکسان می‌باشد [۷] که در ادامه هر یک از این مراحل به طور مختصر توضیح داده می‌شود.

پیش‌پردازش[1]: در هر گونه از روش‌های تشخیص جعل کپی-جابجایی، مرحله پیش‌پردازش تصویر وجود دارد که شامل عملیاتی مانند چیدن[2] و تبدیل تصویر رنگی به خاکستری می‌باشد.

استخراج ویژگی[3]: در هر گونه از روش‌های تشخیص جعل کپی-جابجایی، ویژگی‌های از مناطقی از تصویر که آنتروپی بالا[4] دارند شناسایی و استخراج می‌شوند.

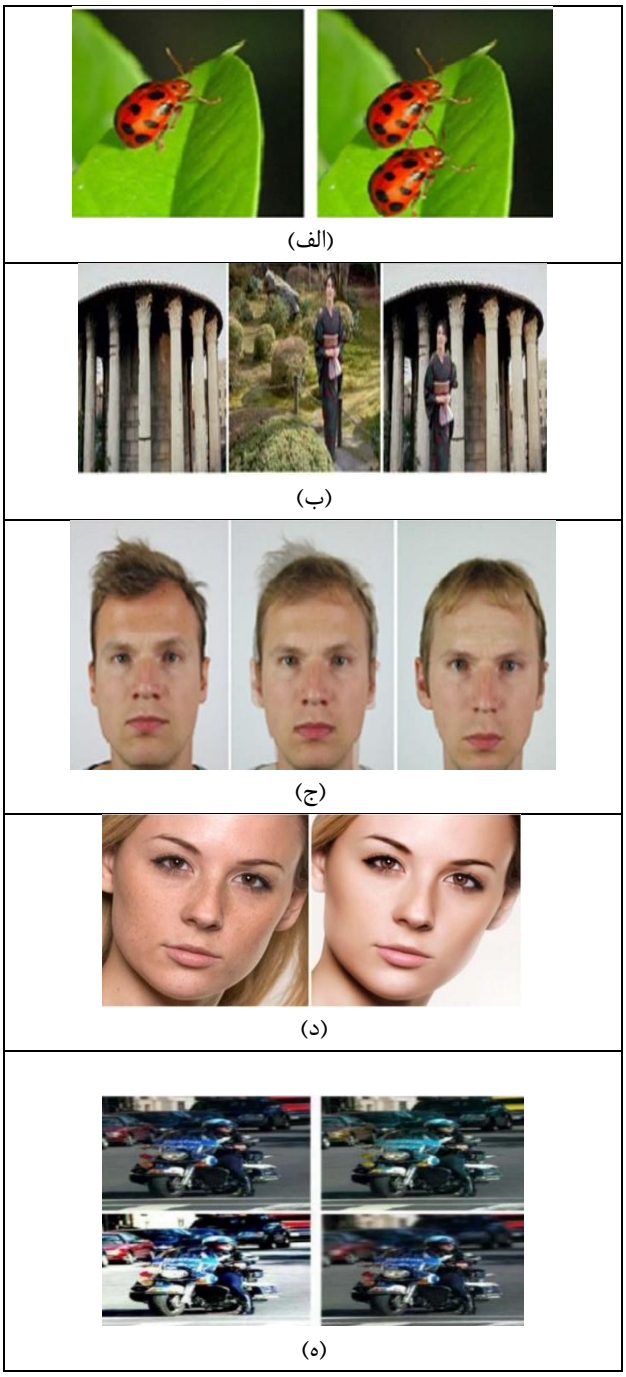
تطبیق[5] : بردارهای ویژگی استخراج شده در هر روش، برای یافتن مناطق جعل کپی‌شده تطبیق داده می‌شود. شباهت بالا بین دو توصیف‌گر ویژگی به عنوان یک نشانه برای منطقه کپی شده است.

فیلتر کردن[6]: فیلترینگ جهت کاهش تطبیق‌های اشتباه استفاده می‌شود. پیکسل‌های همسایه اطراف نواحی جعل معمولاً شدت روشنایی مشابه دارند که می‌تواند منجر به تطبیق‌های اشتباه و در نهایت تشخیص جعل اشتباه شود.

۴- بررسی روش‌های تشخیص جعل کپی جابجایی

روش‌های گوناگونی جهت تشخیص جعل کپی-جابجایی تصویر وجود دارد که به طور کلی می‌توان به دو دسته، تشخیص جعل مبتنی بر روش‌های سنتی و روش‌های مبتنی بر یادگیری ماشین دسته‌بندی کرد [۹, ۱۰]. روش‌های سنتی به دو دسته، روش‌های مبتنی بر نقاط کلیدی و روش‌های تشخیص جعل مبتنی بر بلوک می‌باشد.

[1]Pre-processing
[2]Cropping
[3]Feature Extraction
[4]High Entropy
[5]Matching
[6]Filtering



(الف)

(ب)

(ج)

(د)

(ه)

شکل (۱): انواع جعل تصاویر دیجیتال [۶] (الف) جعل کپی-جابجایی (تصویر سمت چپ: تصویر معتبر، تصویر سمت راست: تصویر جعل کپی-جابجایی)، (ب) پیوند زدن (تصاویر سمت چپ و مرکز: تصاویر معتبر، تصویر سمت راست: تصویر پیوند)، (ج) مورفولوژی (تصاویر سمت چپ و مرکز: تصاویر معتبر، تصویر سمت راست: مورفولوژی)، (د) روتوش تصویر (تصویر سمت چپ: تصویر معتبر، تصویر سمت راست: توبر روتوش شده)، (ه) بهبود تصویر (تصاویر سمت چپ: تصویر معتبر، تصاویر سمت راست: تصویر بهبود یافته از جهت تغییر رنگ پس زمینه)

۴-۱- تشخیص جعل کپی-جابجایی مبتنی بر نقاط کلیدی

در روش تشخیص جعل کپی-جابجایی مبتنی بر نقاط کلیدی، نیازی به تقسیم تصویر به بلوک نیست. در این روش‌ها ابتدا نقاط ویژگی شناسایی می‌شوند. سپس برای هر یک از ویژگی‌های شناسایی شده، توصیفگر ایجاد می‌شود و در نهایت فرآیند تطبیق برای شناسایی مناطق جعل انجام می‌شود [۸]. در این روش‌ها، تکنیک‌های استخراج ویژگی و تطبیق از مراحل مهم می‌باشد [۹]. در ادامه، به شرح چند الگوریتم مهم رایج استخراج ویژگی و سپس روش‌های مهم تطبیق پرداخته می‌شود.

۴-۱-۱- بررسی الگوریتم‌های استخراج ویژگی در روش-های تشخیص جعل کپی-جابجایی مبتنی بر نقاط کلیدی

در این بخش به بررسی الگوریتم‌های رایج استخراج ویژگی همچون تبدیل ویژگی مقیاس ثابت و الگوریتم SURF، الگوریتم MIFT، الگوریتم ORB، الگوریتم KAZE و الگوریتم A-KAZE پرداخته می‌شود.

- ***الگوریتم SIFT***

الگوریتم تبدیل ویژگی مقیاس ثابت در سال ۲۰۰۴ توسط لاوو معرفی شد [۱۰]. ویژگی‌های شناسایی شده در این الگوریتم، نسبت به تغییرات مقیاس و چرخش ثلبت هستند و نسبت به تغییر زاویه و تغییرات شدت روشنایی مقاوم هستند. در ادامه به بررسی الگوریتم SIFT و نسخه‌های بهبودیافته آن در جعل کپی-جابجایی استفاده شده پرداخته می‌شود.

در [۱۱] از الگوریتمSIFT و خوشه‌بندی سلسله مرتبه‌ای[1] به ترتیب جهت شناسایی و تطبیق ویژگی‌ها برای شناسایی نواحی چندگانه جعل استفاده شده است. در [۱۲] از الگوریتم SIFT وSURF جهت شناسایی ویژگی‌ها و از فاصله اقلیدوسی برای تطبیق ویژگی‌ها بهره گرفته شد. در [۱۳] ابتدا از الگوریتم SIFT جهت شناسایی ویژگی‌ها و سپس از روش تطبیق جدیدی بر اساس الگوریتمSIFT جهت تطبیق نواحی جعل استفاده‌شده است. این روش نسبت به روش‌های کلاسیک دیگر [۱۴, ۱۵] عملکرد مناسب‌تری از نظر زمان اجرا و نرخ مثبت درست[2] و نرخ مثبت اشتباه[3] دارد. در [۱۶] از الگوریتم RKEM-SIFT و خوشه‌بندی سلسله مرتبه‌ای به ترتیب جهت شناسایی و تطبیق ویژگی‌ها استفاده شده که این روش برای شناسایی نواحی جعل به طور موثر عمل می‌کند. در [۱۷] از الگوریتم SIFT، گشتاور ثابت و الگوریتم رشد ناحیه به ترتیب جهت شناسایی، تطبیق ویژگی‌ها و شناسایی نواحی جعل کپی-جابجایی استفاده شده است. این روش نسبت به روش‌های [۱۳, ۱۸] دقّت عملکرد مناسب‌تری دارد. در [۱۹] به مقایسه

[1] Hierarchical Clustering
[2] True-Positive Rate
[3] False-Positive Rate

للگوریتم های SIFT، SURF و HOG[1] در جعل کپی-جابجایی پرداخته شد که نشان می‌دهد الگوریتم SIFT نسبت به دو الگوریتم دیگر از دقّت بالاتری برخوردار است.

- **الگوریتم SURF**

SURF یک آشکارساز ویژگی محلی مقاوم است که اولین بار توسط هربرت بای[2] و همکارانش در سال ۲۰۰۶ ارائه شده است [۲۰] که می‌تواند در کارهای بینایی ماشین مانند بازشناسی یا بازیابی شیء استفاده شود. SURF از اندازه‌گیری سریع ماتریس هسیان[3] برای آشکارساز و توصیف‌گر مبتنی بر توزیع استفاده می‌کند. SURF مشابه SIFT نسبت به چرخش و مقیاس ثابت است، اما در یک زمان ثابت، SURF می‌تواند سریع‌تر عمل کند. در ادامه به بررسی الگوریتم SURF و نسخه‌های بهبودیافته آن در جعل کپی-جابجایی استفاده شده پرداخته می‌شود.

در [۲۱] از الگوریتمSURF و رویکرد نزدیکترین همسایه[4] جهت شناسایی نقاط کلیدی و تطبیق میان آنها استفاده می‌شود که این روش برای شناسایی نواحی جعل چندگانه با تغییرات چرخش و محوشدگی مناسب است. در [۲۲]، رویکرد جدیدی براساس الگوریتم SURF و PCET جهت شناسایی نواحی جعل کپی- جابجایی ارائه شده است. در این روش، ابتدا تصویر به بلوک‌های غیر هم‌پوشان تقسیم می‌شوند و سپس نقاط کلیدی توسط الگوریتم SURF از هر بلوک استخراج می‌شوند و در نهایت با توصیفگر PCET و تطبیق 2gNN جهت شناسایی نواحی جعل کپی-جابجایی استفاده می‌شود. در [۲۳]، روش جدیدی جهت جعل کپی-جابجایی تصویر پیشنهاد شده است. ابتدا، الگوریتم SURF و BRISK به ترتیب جهت شناسایی ویژگی‌ها و توصیفگرها استفاده شده است و سپس الگوریتم تطبیق 2NN جهت تطبیق به‌کار گرفته شده است. این رویکرد در کاهش نرخ شناسایی اشتباه موثر است. در [۲۴]، از الگوریتم SURF جهت توصیف نقاط کلیدی استفاده شده است که سبب کاهش زمان اجرا و افزایش دقت در فرآیند تشخیص جعل کپی-جابجایی شده است. در [۲۵]، الگوریتم SURF جهت شناسایی ویژگی‌ها در فرآیند تشخیص جعل کپی-جابجایی به‌کار گرفته شده است. این روش سبب به طور موثر نواحی جعل با تغییرات مقیاس، چرخش و محوشدگی را شناسایی می‌کند.

- **الگوریتم FAST**

الگوریتم FAST[5] برای شناسایی گوشه در تصویر توسط روستن[6] در سال ۲۰۰۸ معرفی شد [۲۶]. این الگوریتم نسبت به تغییرات چرخش ثابت می‌باشد و نسبت به تغییرات جزئی مقیاس پایداری مناسبی دارد. در ادامه به شرح جزییات این الگوریتم پرداخته می‌شود.

۱-یک پنجره دایره‌ای با ۱۶ پیکسل اطراف هر پیکسل مورد بررسی در نظر گرفته می‌شود.

۲-یک مقدار آستانه شدت روشنایی (T) در نظر گرفته می‌شود.

۳-ابتدا مقدار شدت روشنایی پیکسل های ۱و ۵ و۹و ۱۳ نسبت به آستانه مورد بررسی قرار خواهد گرفت.

۴- اگر حداقل سه تا از چهار پیکسل I_1, I_5, I_9, I_{13} مقدار شدت روشنایی آن بالاتر یا پایین‌تر از آستانه نباشد، در این مورد پیکسل مورد نظر به عنوان گوشه در نظر گرفته نمی‌شود. در غیر این صورت اگر حداقل سه تا از پیسکل‌ها بالاتر یا پایین‌تر از آستانه باشد، پس برای ۱۲ پیکسل دیگر مقدار شدت روشنایی آن نسبت به آستانه بررسی می‌شود.

۵- این فرآیند برای همه‌ی پیکسل ها در تصویر مورد بررسی قرار خواهد گرفت.

در [۲۷]، از الگوریتم SIFT و FAST جهت شناسایی نقاط کلیدی در نواحی جعل کپی-جابجایی استفاده شده است. الگوریتم SIFT برای شناسایی نقاط کلیدی در مناطق هموار و الگوریتم FAST برای شناسایی نقاط کلیدی در مناطق بافت به کار گرفته شده است که این روش از دقت بهتری و پیچیدگی محاسباتی کمتری برخوردار است.

- **الگوریتم ORB**

الگوریتم ORB از شناساگر FAST و توصیف‌گر BRIEF تشکیل شده است که نقاط کلیدی FAST، جهت ندارد. الگوریتم FAST و BRIEF هم عملکرد خوب و هم هزینه محاسباتی کمتری دارد. الگوریتم ORB نسبت به تغییرات چرخش ثابت و نویز مقاوم است. در ادامه به بررسی الگوریتم ORB در جعل کپی-جابجایی استفاده شده پرداخته می‌شود.

در [۲۸]، الگوریتم ORB جهت شناسایی و توصیف ویژگی‌ها برای فرآیند تشخیص جعل کپی-جابجایی استفاده شده است. در [۲۹]، رویکرد جدیدی مبتنی بر الگوریتم ORB جهت جعل کپی-جابجایی استفاده شده است که از الگوریتم ORB جهت شناسایی و توصیف ویژگی‌ها و از K نزدیک‌ترین همسایه مبتنی بر فاصله همینگ جهت تطبیق استفاده شده است. در [۳۰]، از الگوریتم ORB جهت استخراج و توصیف ویژگی‌ها و از تطبیق‌گر Brute Force و فاصله همینگ جهت تطبیق به‌کار گرفته شده است. این روش در برابر تغییرات رنگی، شدت روشنایی نواحی جعل بسیار مناسب می‌باشد و از زمان اجرای کمتری برخوردار است. در [۳۱]، از الگوریتم ORB جهت شناسایی و توصیف ویژگی‌ها در جعل کپی-جابجایی به کار گرفته شده است که این رویکرد دقت بالاتر و زمان اجرای کمتری دارد. در[۳۲]، الگوریتم ORB جهت شناسایی و توصیف ویژگی‌ها، فاصله همینگ برای تطبیق و الگوریتم RANSAC جهت حذف تطبیق‌های نادرست به‌کار گرفته شده است. این روش در برابر تبدیل‌های هندسی نواحی جعل عملکرد موثرتری دارد.

[1] Histogram Oriented Gradient
[2] Herbert Bay
[3] Hessian
[4] Nearest Neighbor
[5] Features from Accelerated Segment Test
[6] Rosten

- **الگوریتم MIFT**

الگوریتم MIFT نسخه توسعه یافته الگوریتم SIFT در مرحله توصیفگر می‌باشد که توسط گوا در سال ۲۰۰۹ ارائه شده است [۳۳]. این الگوریتم در مرحله استخراج ویژگی‌ها مشابه الگوریتم SIFT می‌باشد امّا در مرحله توصیفگر نسبت به تبدیلات انعکاس آینه ثابت می‌باشند. این الگوریتم علاوه بر اینکه نسبت به تغییرات مقیاس و چرخش ثابت و مقاوم به تغییر زاویه است، نسبت به انعکاس آینه ثابت می‌باشند. در ادامه به بررسی الگوریتم MIFT و نسخه‌های بهبود یافته آن در جعل کپی- جابجایی پرداخته می‌شود.

در [۳۴]، الگوریتم MIFT بهبودیافته جهت شناسایی نقاط کلیدی در جعل کپی-جابجایی استفاده شده است که این روش در شناسایی نواحی چندگانه جعل دقت مناسبی دارد. در [۳۵]، روش جدیدی مبتنی بر الگوریتم MIFT برای شناسایی نواحی جعل کپی-جابجایی ارائه شده است. در این روش، ابتدا ویژگی‌ها توسط الگوریتم MIFT شناسایی می‌شود و سپس الگوریتم RANSAC جهت حذف تطبیق‌های نادرست استفاده شده است. در [۳۶]، الگوریتم MIFT برای شناسایی نواحی جعل کپی-جابجایی استفاده شده است. این روش نسبت به SIFT توانایی بیشتر در تشخیص جعل کپی-جابجایی دارد اما این روش در نواحی مسطح عملکرد مناسبی ندارد. در [۳۷]، تشخیص نواحی جعل کپی –جابجایی توسط الگوریتم MIFT ارائه شده است. در [۳۸]، جعل کپی- جابجایی تصویر توسط رویکرد جدیدی مبتنی بر MIFT پیشنهاد شده است. در این روش، ابتدا تصویر به بلوک‌های غیر هم‌پوشان تقسیم می‌شود و سپس ویژگی‌ها از هر بلوک توسط الگوریتم SIFT و MIFT استخراج می‌شود. این روش نسبت نواحی جعل با تغییرات مقیاس، چرخش، نویز، تبدیلات انعکاس آینه ثابت می‌باشند.

- **الگوریتم KAZE**

الگوریتم KAZE توسط آلکانتریلا در سال ۲۰۱۲ پیشنهاد شده است [۳۹]. ابتدا ویژگی‌ها توسط فضای مقیاس غیرخطی شناسایی می‌شوند و سپس برای هر ویژگی، یک جهت تعیین می‌شود. این ویژگی‌ها نسبت به تغییرات مقیاس و چرخش ثلبت می‌باشند. در ادامه به بررسی الگوریتم KAZE در جعل کپی-جابجایی پرداخته می‌شود.

در [۴۰]، عملکرد الگوریتم SIFT، الگوریتم SURF و الگوریتم KAZE برای بررسی جعل کپی-جابجایی استفاده شده است. الگوریتم SURF نسبت به دو الگوریتم دیگر SIFT، KAZE سریعتر است اما الگوریتم SIFT نسبت به دو الگوریتم دیگر از دقت بهتری برخوردار است. الگوریتم KAZE دقت بهتری نسبت به SURF دارد اما سرعت بیشتری نسبت به SURF دارد. در [۴۱]، از الگوریتم KAZE جهت شناسایی نقاط کلیدی و از الگوریتم RANSAC جهت حذف تطبیق‌های نادرست در فرآیند تشخیص جعل کپی-جابجایی استفاده شده است. در [۴۲]، عملکرد الگوریتم‌های همچون SURF، KAZE، BRISK و هریس جهت شناسایی نقاط کلیدی در فرآیند تشخیص جعل کپی-جابجایی به‌کار گرفته شده است که الگوریتم KAZE دقت و صحت بهتری نسبت به الگوریتم‌های دیگر دارد. در [۴۳]، الگوریتم KAZE و الگوریتم SIFT جهت شناسایی ویژگی‌ها برای شناسایی نواحی چندگلنه جعل به‌کار گرفته شده است که این روش در برابر اعوجاج‌های مقیاس، چرخش و نویز عملکرد موثرتری دارد.

- **الگوریتم A-KAZE**

الگوریتم A-KAZE نسخه توسعه یافته الگوریتم KAZE می‌باشد که توسط آلکانتریلا در سال ۲۰۱۳ معرفی شده است [۴۴]. این الگوریتم نسبت به الگوریتم KAZE سرعت بهتری دارد. ویژگی‌ها در روش A-KAZE توسط ماتریس هسیان شناسایی می‌شوند و سپس نقاطی که مقدار اکسترمم آنها و مقدار اکسترمم هسیان آنها از مقدار آستانه بیشتر باشد به عنوان نقاط کلیدی (ویژگی‌ها) در نظر گرفته می‌شوند. در ادامه به بررسی الگوریتم AKAZE در جعل کپی-جابجایی پرداخته می‌شود. در [۴۵]، شناساگر FAST، AKAZE جهت استخراج ویژگی‌ها و الگوریتم SIFT و DAISY جهت توصیف ویژگی‌ها جهت شناسایی نواحی جعل پیشنهاد شده است. این رویکرد نسبت به روش‌های دیگر با کاهش نرخ شناسایی اشتباه برخوردار است. در [۴۶]، شناسایی ویژگی‌ها توسط الگوریتم AKAZE، تطبیق توسط فاصله همینگ و g2NN برای شناسایی نواحی جعل چندگانه استفاده شده است. در [۴۷]، ویژگی‌ها توسط الگوریتم‌های AKAZE و SIFT استخراج و تطبیق توسط g2NN انجام شده است. این روش به طور موثر نواحی جعل چندگانه با تغییرات مقیاس، چرخش و نویز شناسایی می‌کند. در [۴۸]، الگوریتم‌های SURF بهبودیافته و AKAZE جهت شناسایی ویژگی‌ها در فرآیند جعل کپی-جابجایی پیشنهاد شده است.

۴-۱-۲- بررسی روش‌های تطبیق در تشخیص جعل کپی-جابجایی مبتنی بر نقاط کلیدی

در این بخش به بررسی روش‌های رایج تطبیق همچون نزدیک‌ترین همسایه و کلاسترینگ پرداخته می‌شود.

- **نزدیک‌ترین همسایه**

تکنیک نزدیکترین همسایه شباهت بین فاصله نقاط ویژگی از هر نقطه کلیدی را نسبت به یکدیگر محاسبه می‌کند. سپس فاصله نقاط کلیدی که کمتر از آستانه از پیش تعیین شده باشند، تطبیق داده می‌شود. تکنیک‌های نزدیک‌ترین همسایه برای رویکرد مبتنی بر نقطه کلیدی به چهار نوع، [۱۶] g2NN، 2NN، Best Bin First و روش‌های دیگر تقسیم می‌شوند که روش g2NN برای تشخیص جعل چندگانه کپی-جابجایی مناسب است [۳۰]. یکی از مشکلات این روش‌ها، ایجاد تعداد زیادی تطبیق‌های نادرست می‌باشد.

- **کلاسترینگ**

در تکنیک‌های کلاسترینگ (خوشه‌بندی)، اشیاء مشابه در یک دسته (خوشه) و اشیاء مختلف در یک دسته متفاوت قرار می‌گیرند. خوشه‌بندی سلسله مراتبی تجمعی، یک نمونه رایج تکنیک خوشه‌بندی

در تشـــخیص جعل کپی-جابجایی اســـت. از مشـــکلات این روش، تطبیق‌های نادرست می باشد.

۴-۲- تشخیص جعل کپی- جابجایی مبتنی بر بلوک

در روش‌های مبتنی بر بلوک، ابتدا تصـــویر به بلوک‌های مربعی یا دایره‌ای هم‌اندازه تقســـیم می‌شـــود که ممکن اســـت روی یکدیگر همپوشانی داشته باشند یا نداشته باشند [۵۲]. سپس ویژگی‌های هر بلوک شناسایی شده و بردار ویژگی به صورت یک ماتریس لغوی مرتب شـده و جفت بلوک‌های مشـابه تطبیق داده می‌شـود تا مناطق کپی-جابجایی شـناسـایی شـوند و در نهایت می‌توان از فیلترها و روش‌های مناسب جهت حذف تطبیق‌های نادرست برای بهبود دقت نواحی جعل اســتفاده کرد. در این روش‌ها به طور گســترده از الگوریتم‌های تبدیل کسـینوسـی گسـسـته، روش‌های مبتنی برگشـتاور ثابت، بافت شـدت روشـــنایی و روش مبتنی بر تبدیل ویولت دوتایی جهت شـــناســـایی ویژگی‌ها و از الگوریتم‌های همبستگی ، فاصله اقلیدسی و مرتب‌سازی، جهت تطبیق استفاده می‌شود.

۴-۲-۱- بررسی الگوریتم‌های استخراج ویژگی در روش‌های تشخیص جعل کپی-جابجایی مبتنی بر بلوک

در این بخش، برخی روش‌های رایج جهت شـناسـایی ویژگی هر بلوک شرح داده می‌شود. در ادامه به شرح هر یک از آنها پرداخته می‌شود.

- ***تبدیل کسینوسی گسسته***

در بسیاری از روش‌های تشخیص جعل کپی- جابجایی مبتنی بر بلوک از تبدیل کسـینوسـی گسـسـته (DCT)[1] اسـتفاده شـده اسـت. DCT یک روش تبدیل ریاضی است که می‌تواند هر پیکسل از یک تصویر در دامنه فضایی را به ضرائب DCT در حوزه فرکانس تبدیل کند. اکثر اطلاعات سیگنال تمایل دارند در چند مؤلفه فرکانس پایین DCT متمرکز شوند. در [۴۹]، جعل کپی-جابجایی مبتنی بر تبدیل کسـینوسـی گسـسـته پیشـنهاد شـده اسـت. ابتدا، تصـاویر به بلوک‌های هم‌پوشـان تقسـیم می‌شـود. سـپس تبدیل کسـینوس گسـسـته اسـتفاده می‌شـود و ضـرایب تبدیل کسـینوس گسـسـته به صـورت زیگزاگ مرتب می‌شـوند و تطبیق مبتنی بر نزدیک‌ترین همسایه انجام می‌شود. این رویکرد در شناسایی نواحی جعل چندگانه موثر می‌باشد.

در [۵۰]، جعل کپی-جابجایی با اسـتفاده از تبدیل کسـینوسـی گسـسـته ارائه شـده اسـت. در این رویکرد، ابتدا تصـاویر به بلوک‌های هم‌پوشـان با اندازه یکسـان تقسـیم می‌شـود و تبدیل کسـینوسـی گسـسـته برای هر بلوک محاسـبه می‌شـود و سـپس مرتب‌سـازی لغوی برای ضـرایب تبدیل کسـینوسـی گسسـته انجام شود و در نهایت از نزدیک‌ترین همسایه جهت تطبیق استفاده می‌شود.

در [۵۱]، رویکرد مبتنی بر تبدیل کسـینوسـی گسـسـته برای جعل کپی-جابجایی ارائه شـده اسـت. در این روش، ابتدا تصـاویر خاکسـتری به بلوک‌های با اندازه یکسـان تقسـیم می‌شـود و سـپس تبدیل کسـینوسـی گســسـته برای هر بلوک به‌کار گرفته می‌شـود و در نهایت Gaussian RBF kernel PCA برای ضرایب فرکانسی تبدیل کسـینوسـی گسـسـته اســـتفاده می‌شـــود. این روش نســـبت به تغییرات مقیاس، چرخش، محوشدگی، فشردگی، نویز و تبدیل غیرخطی مقاوم است.

در [۵۲]، جعل کپی-جابجایی توسـط تبدیل کسـینوسـی گسـسـته و تبدیل ویولیت گســسـته اسـتفاده شـده اسـت. در این روش پس از بلوک‌بندی تصویر، تبدیل کسـینوسـی گسـسـته و تبدیل ویولیت گسـسـته به‌کار گرفته می‌شود. سـپس همبسـتگی جهت تطبیق انجام می‌شـود که تصویر باینری ایجاد می‌شـود و نواحی سـیاه نشـان‌دهنده جعل می‌باشـد که موقعیت نواحی جعل توسط شناساگر کنی بدست می‌آید. این روش از دقت مناسبی برخوردار است.

- ***روش مبتنی بر تبدیل ویولیت گسسته***[2]

در روش مبتنی بر تبدیل ویولیت گســسـته، ابتدا تصـویر با اسـتفاده از تبدیل ویولیت گســسـته تا مقیاس یک تجزیه شـده و تنها از زیرباند HH1 و LL1 استفاده می‌شود. زیرباند LL1 یک برآورد از تصویر است که برای شـــناســـایی نواحی تکراری بهتر می‌باشـــد که با اعمال فیلتر پایین‌گذر در جهت عمودی و افقی به دســـت می‌آید و به مؤلفه‌های فرکانس پایین ورودی اشـــاره دارد. همچنین زیرباند HH1 نویز موجود در تصـویر را کدگذاری می‌کند که شـامل اطلاعات فرکانس بالا اسـت و پس از اعمال فیلتر بالاگذر در جهت عمودی و افقی به دست می‌آید.

در [۵۳]، تشخیص جعل کپی-جابجایی توسط تبدیل ویولیت گسسته و همبسـتگی فاز انجام شـده اسـت که این روش از نظر سـرعت عملکرد موثری دارد. در [۵۴]، زیر باند LL1 از تبدیل ویولیت گســسـته جهت تشخیص نواحی جعل از تصویر اسـتفاده شـده اسـت که این روش سـبب کاهش پیچیدگی محاسباتی و افزایش سرعت می‌شود. در [۵۵]، تبدیل ویولیت گسـسـته جهت تجزیه تصویر و شـناسـایی نواحی جعل پیشـنهاد شـده اسـت. این روش نسـبت به تبدیل فوریه در آنالیز محتوای تصـویر بسـیار مناسـب‌تر اسـت. در [۵۶]، رویکرد جهت تشـخیص جعل کپی-جابجایی پیشـنهاد شـده اسـت. در این روش، ابتدا تصـویر توسـط تبدیل ویولیت گسـسـته تجزیه می‌شـود و سـپس تصـویر به بلوک‌های هم‌پوشـان تقسـیم می‌شـود و در نهایت با اسـتفاده از مرتب‌سـازی لغوی نواحی جعل کپی-جابجایی شناسایی می‌شود.

- **روش مبتنی بر گشتاورهای ثابت Zernike**

روش‌های مبتنی بر گشتاورهای ثابت Zernike به چرخش نواحی جعل کپی‌شـــده، ثابت می‌باشـــد [۱]. در این روش، تصـــویر به بلوک‌های هم‌پوشـان تقسـیم می‌شـود. اندازه گشـتاور Zernike هر بلوک به عنوان بردار ویژگی در نظر گرفته می‌شـود. این روش در برابر تغییرات مقیاس و تبدیل آفین نواحی جعل عملکرد موثری ندارد [۵۷, ۵۸].

[1] Discrete Cosine Transform

[2] Discrete Wavelet Transform

در [۵۹]، روش گشتاورZernike مبتنی بر تبدیل هارمونیک دایره‌ای و تبدیل فوریه ملین جهت استخراج ویژگی‌ها برای تشخیص نواحی جعل کپی-جابجایی ارائه شده است. در [۶۰]، روش گشتاور ثابت Zernike جهت تشخیص نواحی جعل کپی-جابجایی پیشنهاد شده است. این روش نسبت به به چرخش و نویز مقاوم است. در [۶۱]، روش گشتاور ثابت fractional Zernike جهت تشخیص نواحی جعل کپی-جابجایی ارائه شده است.

۴-۲-۲- بررسی روش‌های تطبیق در تشخیص جعل کپی-جابجایی مبتنی بر بلوک

در این بخش، به بررسی روش‌های رایج تطبیق در تشخیص جعل کپی-جابجایی مبتنی بر بلوک همچون همبستگی، فاصله اقلیدسی و مرتب‌سازی پرداخته می‌شود. در ادامه به شرح جزییات آنها پرداخته می‌شود.

- **همبستگی**

در این روش میزان تشابه بین بلوک‌ها محاسبه شده و حداکثر شباهت‌ها به عنوان موارد مشابه در نظر گرفته می‌شود. معمولاً از ضرایب همبستگی برای تعیین نواحی جعلی پس از مرتب‌سازی استفاده می‌شود. هرچند که ضرایب همبستگی را می‌توان به طور مستقل و بدون مرتب‌سازی در روش‌های تطبیق مبتنی بر بلوک استفاده کرد. در این روش ممکن است نواحی با تشابه میزان شدت روشنایی، به اشتباه تطبیق داده شود که سبب تطبیق‌های نادرست و در نهایت تشخیص نادرست نواحی جعل می‌گردد.

- ***فاصله اقلیدسی***

این روش، فواصل بین بلوک‌ها را اندازه می‌گیرد و بلوک‌های مشابه را تطبیق می‌دهد. فاصله اقلیدسی، مشابه روش همبستگی، برای تعیین مناطق دستکاری (جعل) شده پس از فرآیند مرتب‌سازی استفاده می‌شود. یکی از مشکلات این روش، ایجاد تطبیق‌های چندگانه می‌باشد.

- **مرتب‌سازی**

یکی از روش‌های رایج و مهم تطبیق جهت تشخیص جعل کپی-جابجایی، عمل مرتب‌سازی بردار ویژگی جفت بلوک‌های مشابه می‌باشد. هدف از مرتب‌سازی داده، چیدمان داده‌ها در قالبی خاص است. الگوریتم مرتب‌سازی روشی برای چیدمان داده‌ها با ترتیبی خاص تعیین می‌کند. اغلب ترتیب‌های رایج به صورت ترتیب عددی یا الفبایی هستند. اهمّیّت مرتب‌سازی در این نکته است که جستجوی داده‌ها در صورت مرتب بودن می‌تواند تا سطح بالایی بهینه‌سازی شود. در فرایند تشخیص جعل کپی-جابجایی، معمولاً پس از مرتب‌سازی، عمل جستجو در ماتریس ویژگی انجام می‌شود تا بردارهای مشابه در مجاورت هم قرار گیرند و تطبیق سریع‌تر و ساده‌تر صورت گیرد.

بنابراین تعیین روش مرتب‌سازی مناسب در سرعت الگوریتم و هزینه‌های محاسباتی آن تأثیر به سزایی دارد.

۴-۳- تشخیص جعل کپی-جابجایی مبتنی بر یادگیری ماشین

یادگیری عمیق یکی از موضوعات روز است که کاربرد گسترده‌ای در زمینه‌های مختلف دارد. عملکرد روش‌های مبتنی بر یادگیری عمیق نسبت به روش‌های مبتنی بر نقاط کلیدی و مبتنی بر بلوک بهتر می‌باشد [۵۷]. در [۶۲]، روش dual branch CNN جهت تشخیص جعل کپی-جابجایی پیشنهاد شده است که این روش از دقت و سرعت بالایی برخوردار است. در [۶]، روش مبتنی بر شبکه عصبی پیچشی جهت تشخیص جعل کپی-جابجایی ارائه شده است که در این روش بر روی دیتابیس MICC-F220 به دقّت ۱۰۰ درصد می‌رسد. در [۶۳]، روش جدید شبکه عصبی پیچشی مبتنی بر عمیق جهت تشخیص نواحی جعل ارائه شده است. در این روش از ۳۰ فیلتر بالاگذر به عنوان وزن‌های اوّلیه در شبکه عصبی پیشنهادی استفاده می‌شود. در [۶۴]، با استفاده از شبکه عصبی پیچشی عمیق[1] و بخش‌بندی یک روش برای تشخیص نواحی جعل کپی-جابجایی پیشنهاد شده است. در [۶۵]، ویژگی‌ها توسط معماری ResNet جهت شناسایی نواحی جعل ارائه شده است.

۵- پایگاه داده

تشخیص جعل کپی-جابجایی، یک شاخه جدید در پردازش تصویر می‌باشد. تعدادی پایگاه داده استاندارد برای ارزیابی روش‌ها ایجاد شده است که در ادامه به معرفی چند پایگاه داده رایج پرداخته می‌شود.

- **مجموعه CASIA**

مجموعه داده‌های CASIA محبوب‌ترین مجموعه جهت شناسایی جعل تصویر می‌باشد. دو نسخه از مجموعه داده‌های CASIA به نام CASIA v1 و CASIA v2 وجود دارد [۶۶]. نسخه اوّل این مجموعه شامل ۸۰۰ تصویر معتبر و ۹۲۱ تصویر جعلی می‌باشد. نسخه دوم مجموعه شامل ۷۲۰۰ تصویر معتبر و ۵۱۲۳ تصویر جعل می‌باشد. هر دو مجموعه شامل تصاویر طبیعی، حیوانات و فضای داخلی می‌باشند که اندازه نواحی جعل با اندازه‌های مختلف از کوچک به بزرگ می‌باشد. نواحی جعل شامل اعوجاج‌های هندسی و رادیومتریکی می‌باشد که رزلوشن پایینی دارند.

- **مجموعه Forensic**

پایگاه داده Forensic در اولین چالش IEEE Forensics توسط کمیته فنی امنیت و اطلاعات قانونی در سال ۲۰۱۳ منتشر شد . این مجموعه داده شامل ۴۵۰ تصویر آموزشی و ۷۰۰ تصویر آزمایشی به اندازه ۱۵×۲۰۱۸ است.

[1] deep convolutional neural network

- **مجموعه CoMoFoD**

مجموعه CoMoFoD شامل تصاویر جعل کپی-جابجایی می‌باشد. این پایگاه داده شامل ۲۰۰ تصویر کوچک با اندازه ۵۱۲×۵۱۲ و ۶۰ تصویر بزرگ با اندازه ۳۰۰۰×۲۰۰۰ می‌باشد و مقدار نواحی جعل از ۰/۱۱ تا ۱۷/۳۴ درصد تصاویر است [۶۷]. این مجموعه برای ایجاد تصویر جعل کپی- جابجایی از اعوجاج‌های همچون انتقال، چرخش، تغییرات مقیاس، فشرده‌سازی JPEG، محوشدگی، اضافه کردن نویز و کاهش رنگ استفاده می‌کند.

- **مجموعه GRIP**

مجموعه CRIP شامل ۸۰ تصویر کپی-جابجایی و ۸۰ تصویر معتبر است [۶۸]. تمام تصاویر این پایگاه داده فقط دارای یک منطقه نواحی جعل می‌باشد. تصاویر جعل فقط شامل حرکت انتقالی می‌باشد و تغییرات مقیاس و چرخش ندارد.

- **مجموعه COVERAGE**

مجموعه COVERAGE، یک مجموعه جعل کپی-جابجایی با اشیا واقعی می‌باشند [۶۹]. شش نوع عملیات همچون انتقال، تغییر مقیاس، تغییر چرخش، تبدیل فرم، تغییرات روشنایی و ادغام برای ایجاد تصاویر جعل کپی- جابجایی استفاده شده است.

- **مجموعه MICC-F600**

مجموعه MICC-F600 شامل ۴۴۰ تصویر معتبر و ۱۶۰ تصویر جعل کپی-جابجایی می‌باشد [۱۳]. تصاویر جعل کپی- جابجایی در این مجموعه بسیار مبتدی می‌باشد که دستکاری را می‌توان به راحتی توسط چشم انسان تشخیص داد.

- **مجموعه FAU**

مجموعه FAU شامل ۴۸ تصویر معتبر می‌باشد و از هر تصویر معتبر، یک تصویر جعل کپی-جابجایی ایجاد شده است [۷۰]. اعوجاج‌های همچون فشرده‌سازی JPEG، نویز، تغییرات مقیاس و چرخش برای ایجاد دستکاری تصاویر استفاده شده است. دستکاری تصاویر در این مجموعه بسیار ماهرانه انجام شده است که تصاویر جعل هم مشابه تصاویر معتبر می‌باشد.

- **مجموعه MICC-F220**

مجموعه MICC-F220 شامل ۱۱۰ تصویر معتبر و ۱۱۰ تصویر جعلی می‌باشد [۱۳]. این مجموعه شامل تصاویر طبیعی می‌باشد. وضوح تصاویر از ۴۸۰×۷۲۲ به ۶۰۰×۸۰۰ پیکسل‌ها متغییر است و اندازه پچ جعلی به طور متوسط ۱/۲ درصد کل تصویر را پوشش داده است.

۶- معیارهای ارزیابی

مهم‌ترین فاکتور در ارزیابی روش‌های تشخیص جعل، توانایی آن‌ها در شناسایی تصویر معتبر از جعلی می‌باشد. با این حال، قدرت و دقّت یک الگوریتم به درست تشخیص دادن ناحیه جعل نیز بسیار قابل توجه است، به ویژه هنگامی که تشخیص چشمی جعل امکان‌پذیر نباشد. بنابراین، وقتی یک الگوریتم تشخیص جعل کپی- جابجایی ارزیابی می‌شود، عملکرد تشخیص بایستی در دو سطح تحلیل شود. در ادامه به معرفی چند تا از این معیارهای ارزیابی رایج پرداخته می‌شود.

۶-۱- معیارهای ارزیابی در سطح پایگاه داده

هدف از معیارهای ارزیابی در سطح پایگاه داده اینست که چه تعداد از تصاویر جعلی یا معتبر تشخیص داده می‌شود. در این معیارها، تعداد تصاویر پایگاه داده ارزیابی می‌شود. در ادامه به شرح چند معیار ارزیابی رایج در سطح پایگاه داده بررسی می‌شود.

• دقّت تشخیص

دقّت تشخیص مطابق فرمول (۱) محاسبه می‌شود.

$$\text{precision}=\frac{T_P}{T_P+F_P} \quad (۱)$$

در این رابطه، T_P تعداد تصاویر جعل‌شده که به درستی به عنوان تصویر جعل شناسایی شده است و F_P تعداد تصاویر معتبر که به اشتباه به عنوان تصویر جعل شناسایی شده است.

• فراخوانی

فراخوانی مطابق فرمول (۲) محاسبه می‌شود.

$$Recall=\frac{T_P}{T_{P+F_N}} \quad (۲)$$

در این رابطه، T_P تعداد تصاویر جعل‌شده که به درستی به عنوان تصویر جعل شناسایی شده است و F_N تعداد تصاویر جعل‌شده که به اشتباه به عنوان تصویر معتبر شناخته شده است.

• F1

معیار F1 مطابق فرمول (۳) محاسبه می‌شود.

$$F1=2\frac{precision\times Recall}{precision+Recall} \quad (۳)$$

۶-۲- معیارهای ارزیابی در سطح پیکسل

هدف از معیارهای ارزیابی در سطح پیکسل اینست که چه تعداد از پیکسل‌ها به صورت صحیح جعلی یا معتبر تشخیص داده می‌شود. در این معیارها، یک تصویر به تنهایی ارزیابی می‌شود. در ادامه به شرح چند معیار ارزیابی رایج در سطح پیکسل پرداخته می‌شود.

• دقّت

دقّت مطابق فرمول (۴) محاسبه می‌شود.

$$\text{precision}=\frac{T_P}{T_P+F_P} \quad (۴)$$

در این رابطه، T_P تعداد پیکسل‌های جعل‌شده که به درستی به عنوان پیکسل جعل شناسایی شده است و F_P تعداد پیکسل‌های معتبر که به اشتباه به عنوان پیکسل جعل شناسایی شده است.

• فراخوانی

معیار فراخوانی مطابق فرمول (۵) محاسبه می‌شود.

$$Recall=\frac{T_P}{T_{P+F_N}} \quad (۵)$$

در این رابطه، T_P تعداد پیکسل‌های جعل‌شده که به درستی به عنوان پیکسل جعل شناسایی شده است و F_N تعداد پیکسل جعل‌شده که به اشتباه به عنوان پیکسل معتبر شناخته شده است.

• میانگین هارمونیک

میانگین هارمونیک ترکیب دقّت و فراخوانی می‌باشد که مطابق فرمول (۶) محاسبه می‌شود.

$$F1 = 2\frac{precision \times Recall}{precision + Recall} \quad (۶)$$

• نرخ دقّت تشخیص در سطح پیکسل

نرخ دقّت تشخیص در سطح پیکسل معیاری است که برای تعیین دقّت و مقاوم بودن عملکرد الگوریتم در سطح پیکسل ارائه شده است. این معیار مطابق فرمول (۷) محاسبه می‌شود.

$$DAR = \frac{|\varphi_S \cap \bar{\varphi}_S| + |\varphi_T \cap \bar{\varphi}_T|}{|\varphi_S| + |\varphi_T|} \quad (۷)$$

φ_S نواحی کپی، $\overline{\varphi_S}$ نواحی کپی شناسایی شده، همچنین φ_T و $\bar{\varphi}_T$ به ترتیب نواحی جعل شده و نواحی جعل تشخیص داده شده، هستند.

• نرخ تشخیص اشتباه در سطح پیکسل

نرخ تشخیص اشتباه در سطح پیکسل نشان می‌دهد که در یک الگوریتم تشخیص جعل چند درصد از پیکسل‌هایی که جعلی نیستند، به اشتباه جعلی تشخیص داده می‌شود. نرخ تشخیص اشتباه در سطح پیکسل مطابق رابطه (۸) محاسبه می‌شود.

$$FPR = \frac{|\overline{\varphi_S} - \varphi_S| + |\bar{\varphi}_T - \varphi_T|}{|\overline{\varphi_S}| + |\overline{\varphi_T}|} \quad (۵)$$

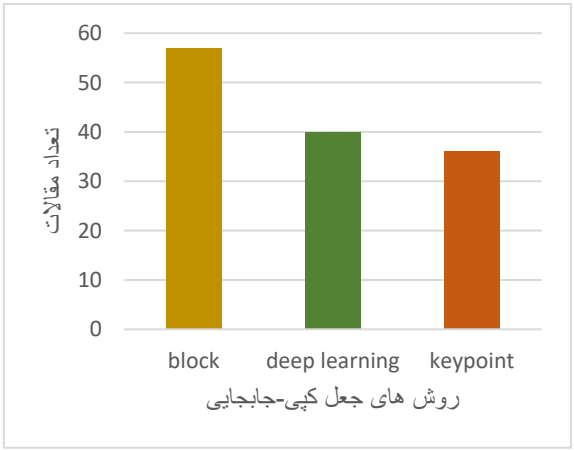
در این رابطه، $|\overline{\varphi_S} - \varphi_S|$ تفاضل نواحی از پیکسل‌ها را مشخص می‌کند که کپی شده و کپی نیز تشخیص داده شده، $|\bar{\varphi}_T - \varphi_T|$ تفاضل نواحی از پیکسل‌ها را مشخص می‌کند که جعلی می‌باشد و جعلی نیز تشخیص داده شده است.

۷- رویکردهای جدید

با توجه به تحقیق‌های زیادی که جهت تشخیص جعل کپی-جابجایی انجام شده است امّا هنوز به دلیل متنوع بودن نوع تبدیل‌های هندسی، رادیومتریک و آفین جهت کپی نواحی جعل، یک روش عمومی و کامل جهت تشخیص جعل وجود ندارد. پس برای تشخیص نواحی جعل کپی- جابجایی باید به نوع تبدیل‌ها جهت کپی نواحی جعل و تعداد نواحی جعل هم توجه کرد. بر این اساس بررسی‌هایی بین روش‌های مبتنی بر نقاط کلیدی، روش‌های مبتنی بر بلوک و روش‌های مبتنی بر یادگیری عمیق در محدوده‌ی سال‌های (۲۰۱۵-۲۰۲۳) در پایگاه IEEE مورد بررسی قرار گرفته است (شکل (۲)). با توجه به این بررسی می‌توان نتیجه گرفت که اخیرا روش‌های مبتنی بر نقاط کلیدی کمتر از روش‌های دیگر کاربرد دارد که این نشان می‌دهد که در این روش چالش کمتری وجود دارد. روش‌های مبتنی بر یادگیری عمیق بیشتر از روش‌های مبتنی بر نقاط کلیدی کاربرد دارد امّا روش‌های مبتنی بر بلوک بیشترین کاربرد در تشخیص نواحی جعل کپی- جابجایی دارد که نشان‌دهنده بیشترین چالش در این زمینه می‌باشد. چالش‌های موجود در روش‌های مبتنی بر بلوک نسبت به تبدیل‌های هندسی مقاوم نمی‌باشند که اخیرا با ترکیب با روش‌های مبتنی بر نقاط کلیدی یا بهبود جزیی هر یک از روش‌های مبتنی بر بلوک توانستند در این زمینه عملکرد خوبی داشته باشند و به همین دلیل امروزه بهبود این روش‌ها بیشترین تعداد مقالات دارند. از طرف دیگر، روش‌های مبتنی بر یادگیری عمیق به طور گسترده در زمینه‌های دیگر پردازش تصویر کاربرد گسترده‌ای دارد امّا این روش‌ها معمولاً به اندازه تصویر ثابت و تعداد زیادی داده‌های آموزشی و آزمایشی در تشخیص جعل کپی-جابجایی نیاز دارند. بنابراین، نتایج تشخیص روش‌های مبتنی بر یادگیری عمیق کاملاً به کیفیت داده‌های آموزشی بستگی دارد. به طور خلاصه، روش‌های موجود مبتنی بر یادگیری عمیق هنوز هم برای تشخیص جعل کپی- جابجایی خوب عمل نمی‌کنند. روش‌های مبتنی بر نقاط کلیدی با توجه به اینکه الگوریتم‌های بسیاری نسبت به تبدیل‌های هندسی ثابت می‌باشند، اخیرا چالش جهت بهبود این الگوریتم‌ها در زمینه جعل کپی-جابجایی بسیار کم می‌باشد و به همین دلیل اخیرا تعداد مقالات در بهبود این زمینه کم می‌باشد.

۸- جمع‌بندی

تصاویر دیجیتال به طور گسترده در زمینه‌های مختلف همچون پزشکی، صنعت روزنامه، جنایی، سنجش از دور و غیره کاربرد دارند. بنابراین موثق بودن این تصاویر بسیار مهم می‌باشد. امروزه روش‌های گوناگونی جهت جعل تصاویر دیجیتال وجود دارد که جعل کپی-جابجایی تصویر یکی از رایج‌ترین و ساده‌ترین جعل‌ها می‌باشد که تشخیص اینگونه جعل مورد توجه محققان متعددی قرار گرفته است. در این مقاله، ضمن معرفی مفاهیم جعل کپی-جابجایی تصویر، به بررسی مراحل، دسته‌بندی روش‌های تشخیص و سوگیری تحقیقات در این زمینه ارائه شد. از ویژگی‌های دیگر این مقاله، مشخص کردن رویکردهای تحقیقات آینده در این زمینه است. مقالات این حوزه نشان می‌دهد، هنوز



شکل (۲): نمودار تعداد مقالات برحسب روش‌های مختلف جعل کپی-جابجایی

چالش‌هایی در روش‌های مبتنی بر بلوک و روش‌های مبتنی بر یادگیری عمیق وجود دارد که بهبود این روش‌ها در ارتقا دقّت تشـــخیص جعل کپی-جابجایی بسیار حائز اهمّیّت است.

مراجع

[1] B. Soni, P. K. Das, and D. M. Thounaojam, "CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection," *IET Image Processing*, vol. 12, pp. 167-178, 2018.

[2] A. Dixit and R. Gupta, "Copy-Move Image Forgery Detection a Review," *International Journal of Image, Graphics and Signal Processing*, vol. 8, p. 29, 2016.

[3] M. A. Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," in *2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14)*, 2014, pp. 1-5.

[4] N. T. Pham and C.-S. Park, "Toward Deep-Learning-Based Methods in Image Forgery Detection: A Survey," *IEEE Access*, vol. 11, pp. 11224-11237, 2023.

[5] A. Bensaad, K. Loukhaoukha, and S. Sadoudi, "Keypoint-based copy-move forgery detection in digital images: a survey," in *2022 7th International Conference on Image and Signal Processing and their Applications (ISPA)*, 2022, pp. 1-6.

[6] K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, "An efficient CNN model to detect copy-move image forgery," *IEEE Access*, vol. 10, pp. 48622-48632, 2022.

[7] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on keypoint based copy-move forgery detection methods on image," *Procedia Computer Science*, vol. 85, pp. 206-212, 2016.

[8] B. Ustubioglu, G. Tahaoglu, and G. Ulutas, "Detection of audio copy-move-forgery with novel feature matching on Mel spectrogram," *Expert Systems with Applications*, vol. 213, p. 118963, 2023.

[9] N. Kumar and T. Meenpal, "Salient keypoint-based copy–move image forgery detection," *Australian Journal of Forensic Sciences*, vol. 55, pp. 331-354, 2023.

[10] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, pp. 91-110, 2004.

[11] Y. Fan, Y.-S. Zhu, and Z. Liu, "An improved SIFT-based copy-move forgery detection method using T-linkage and multi-scale analysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, pp. 399-408, 2016.

[12] R. C. Pandey, S. K. Singh, K. Shukla, and R. Agrawal, "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," in *2014 9th International conference on industrial and information systems (ICIIS)*, 2014, pp. 1-6.

[13] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *IEEE transactions on information forensics and security*, vol. 6, pp. 1099-1110, 2011.

[14] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*, pp. 1-11, 2004.

[15] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *Proceedings of Digital Forensic Research Workshop*, 2003.

[16] Z. H.-N. a. M. Nasri, "Copy-Move Image Forgery Detection Using Redundant Keypoint Elimination Method," *in Cryptographic and Information Security Approaches for Images and Videos, S. Ramakrishnan, Ed. Boca Raton: CRC Press*, pp. 773-797, 2019.

[17] C.-C. Chen, W.-Y. Lu, and C.-H. Chou, "Rotational copy-move forgery detection using SIFT and region growing strategies," *Multimedia Tools and Applications*, pp. 1-16, 2019.

[18] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 507-518, 2014.

[19] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016, pp. 706-710.

[20] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer vision–ECCV 2006*, ed: Springer, 2006, pp. 404-417.

[21] M. F. Hashmi, V. Anand, and A. G. Keskar, "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms," in *2014 international conference on computer and communication technology (ICCCT)*, 2014, pp. 147-152.

[22] C. Wang, Z. Zhang, Q. Li, and X. Zhou, "An image copy-move forgery detection method based on SURF and PCET," *IEEE Access*, vol. 7, pp. 170032-170047, 2019.

[23] M. Bilal, H. A. Habib, Z. Mehmood, T. Saba, and M. Rashid, "Single and multiple copy–move forgery detection and localization in digital images based on the sparsely encoded distinctive features and DBSCAN clustering," *Arabian Journal for Science and Engineering*, vol. 45, pp. 2975-2992, 2020.

[24] A. Badr, A. Youssif, and M. Wafi, "A robust copy-move forgery detection in digital image forensics using SURF," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 2020, pp. 1-6.

[25] R. Rakhi, A. J. Sundararaj, R. C. Joy, and J. J. Winston, "Effective Detection of Copy Move Forgery Using Surf," in *2023 4th International Conference on Signal Processing and Communication (ICSPC)*, 2023, pp. 306-310.

[26] E. Rosten, R. Porter, and T. Drummond, "Faster and better: A machine learning approach to corner detection," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, pp. 105-119, 2008.

[27] B. Fatima, A. Ghafoor, S. S. Ali, and M. M. Riaz, "FAST, BRIEF and SIFT based image copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 81, pp. 43805-43819, 2022.

[28] G. Muzaffer, O. Makul, B. Ustubioglu, and G. Ulutas, "Copy move forgery detection using gabor filter and orb," in *Proc. 2016International Conf. Image Process. Prod. Comput. Sci*, 2016, pp. 23-29.

[29] V. Mehta, A. K. Jaiswal, and R. Srivastava, "Copy-move image forgery detection using DCT and ORB feature set," in *Futuristic Trends in Networks and Computing Technologies: Second International Conference, FTNCT 2019, Chandigarh, India,*

[45] A. Dixit and S. Bag, "Composite attacks-based copy-move image forgery detection using AKAZE and FAST with automatic contrast thresholding," *IET Image Processing*, vol. 14, pp. 4528-4542, 2020.
[46] X. Zhou and Q. Shi, "Multiple copy-move forgery detection based on density clustering," *Pattern Recognition and Image Analysis*, vol. 31, pp. 109-116, 2021.
[47] C. S. Prakash, P. P. Panzade, H. Om, and S. Maheshkar, "Detection of copy-move forgery using AKAZE and SIFT keypoint extraction," *Multimedia Tools and Applications*, vol. 78, pp. 23535-23558, 2019.
[48] S. K. Narasimhamurthy, V. K. Mahadevachar, and R. K. T. Narasimhamurthy, "A Copy-Move Image Forgery Detection Using Modified SURF Features and AKAZE Detector," *International Journal of Intelligent Engineering & Systems*, vol. 16, 2023.
[49] S. Kumar, J. Desai, and S. Mukherjee, "A fast DCT based method for copy move forgery detection," in *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*, 2013, pp. 649-654.
[50] E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco, and L. J. García Villalba, "Copy-move forgery detection technique based on discrete cosine transform blocks features," *Neural Computing and Applications*, vol. 33, pp. 4713-4727, 2021.
[51] M. A. S. Kumar, "IMAGE FORENSIC FOR DIGITAL IMAGE COPY MOVE FORGERY DETECTION," *IMAGE*, vol. 52, 2023.
[52] A. Shankar, P. Swetha, and B. Ramu, "Image Forgery Detection Method for Copy-Move and Splicing Attacks Using DCT, DWT And Correlation," *Journal of Pharmaceutical Negative Results*, pp. 3878-3883, 2022.
[53] S. Khan and A. Kulkarni, "Reduced time complexity for detection of copy-move forgery using discrete wavelet transform," *International Journal of Computer Applications*, vol. 6, pp. 31-36, 2010.
[54] S. Mushtaq, R. A. Khan, S. A. Lone, A. Moon, and M. Qadri, "Improved Complexity in Localization of Copy-Move Forgery Using DWT," in *International Conference on Computing, Communications, and Cyber-Security*, 2022, pp. 825-839.
[55] R. Ashraf, M. S. Mehmood, T. Mahmood, J. Rashid, M. W. Nisar, and M. Shah, "An efficient forensic approach for copy-move forgery detection via discrete wavelet transform," in *2020 International Conference on Cyber Warfare and Security (ICCWS)*, 2020, pp. 1-6.
[56] P. Yadav and Y. Rathore, "Detection of copy-move forgery of images using discrete wavelet transform," *International Journal on Computer Science and Engineering*, vol. 4, p. 565, 2012.
[57] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *International workshop on information hiding*, 2010, pp. 51-65.
[58] B. Patel and S. Degadwala, "A Survey Paper on Image forgery detection Using Pseudo Zernike Moment," 2020.
[59] S. Velmurugan and T. Subashini, "Patch-match based detection of copy-move forgeries using rotation invariant features," *Materials Today: Proceedings*, vol. 33, pp. 4686-4690, 2020.
November 22–23, 2019, Revised Selected Papers 2, 2020, pp. 532-544.
[30] Z. Xue, L. Tian, and C. Li, "Passive Image Copy–Move Forgery Detection Based on ORB Features," in *Recent Developments in Intelligent Computing, Communication and Devices: Proceedings of ICCD 2019 5*, 2021, pp. 312-317.
[31] K.-T. Huynh, T.-N. Ly, and T. Le-Tien, "ORB for Detecting Copy-Move Regions with Scale and Rotation in Image Forensics," in *Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications: 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25–27, 2020, Proceedings 7*, 2020, pp. 358-372.
[32] Y. Zhu, X. Shen, and H. Chen, "Copy-move forgery detection based on scaled ORB," *Multimedia Tools and Applications*, vol. 75, pp. 3221-3233, 2016.
[33] X. Guo, X. Cao, J. Zhang, and X. Li, "Mift: A mirror reflection invariant feature descriptor," in *Asian Conference on Computer Vision*, 2009, pp. 536-545.
[34] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery," *Machine vision and applications*, vol. 25, pp. 451-475, 2014.
[35] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Improving the detection and localization of duplicated regions in copy-move image forgery," in *2013 18th international conference on digital signal processing (DSP)*, 2013, pp. 1-6.
[36] V. Agarwal and V. Mane, "Reflective SIFT for improving the detection of copy-move image forgery," in *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2016, pp. 84-88.
[37] V. Dhania and H. B. KP, "Improving Digital Image Forgery Detection Using MIFT Features and Adaptive Over Segmentation," 2016.
[38] A. J. Mariyal, "AN EFFICIENT IMAGE FORGERY DETECTION USING SIFT AND MIFT."
[39] P. F. Alcantarilla, A. Bartoli, and A. J. Davison, "KAZE features," in *European conference on computer vision*, 2012, pp. 214-227.
[40] A. Rani and A. Jain, "Copy-Move Image Forgery Detection Using SURF, SIFT, and KAZE," in *Proceedings of 3rd International Conference on Machine Learning, Advances in Computing, Renewable Energy and Communication: MARC 2021*, 2022, pp. 719-726.
[41] D. Vaishnavi, G. Balaji, and D. Mahalakshmi, "KAZE feature based passive image forgery detection," in *First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018*, 2019, pp. 333-340.
[42] A. Kaur, S. Walia, and K. Kumar, "Comparative analysis of different keypoint based copy-move forgery detection methods," in *2018 Eleventh International Conference on Contemporary Computing (IC3)*, 2018, pp. 1-5.
[43] F. Yang, J. Li, W. Lu, and J. Weng, "Copy-move forgery detection based on hybrid features," *Engineering Applications of Artificial Intelligence*, vol. 59, pp. 73-83, 2017.
[44] P. Alcantarilla, J. Nuevo, and A. Bartoli, "Fast explicit diffusion for accelerated features in nonlinear scale spaces british machine vision conference (BMVC)," ed: Bristol, 2013.

[60] K. A. Tatkare and M. Devare, "Novel Method to Detect Multiple Cloning in Targeted Image Invariant to Rotation," in *Computing in Engineering and Technology: Proceedings of ICCET 2019*, 2020, pp. 65-74.

[61] B. Chen, M. Yu, Q. Su, H. J. Shim, and Y.-Q. Shi, "Fractional quaternion Zernike moments for robust color image copy-move forgery detection," *IEEE Access*, vol. 6, pp. 56637-56646, 2018.

[62] N. Goel, S. Kaur, and R. Bala, "Dual branch convolutional neural network for copy move forgery detection," *IET Image Processing*, vol. 15, pp. 656-665, 2021.

[63] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE international workshop on information forensics and security (WIFS)*, 2016, pp. 1-6.

[64] Abhishek and N. Jindal, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation," *Multimedia Tools and Applications*, vol. 80, pp. 3571-3599, 2021.

[65] B. Ahmed, T. A. Gulliver, and S. alZahir, "Image splicing detection using mask-RCNN," *Signal, Image and Video Processing*, vol. 14, pp. 1035-1042, 2020.

[66] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in *2013 IEEE China summit and international conference on signal and information processing*, 2013, pp. 422-426.

[67] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—New database for copy-move forgery detection," in *Proceedings ELMAR-2013*, 2013, pp. 49-54.

[68] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy–move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2284-2297, 2015.

[69] B. Wen, Y. Zhu, R. Subramanian, T.-T. Ng, X. Shen, and S. Winkler, "COVERAGE—A novel database for copy-move forgery detection," in *2016 IEEE international conference on image processing (ICIP)*, 2016, pp. 161-165.

[70] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, pp. 1841-1854, 2012.