بسم الله الرحمن الرحيم

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی هوش مصنوعی

احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند

نگارنده: انعام هلالات

استاد راهنما

دکتر منصور فاتح

اساتید مشاور

دکتر محسن رضوانی

دکتر علیرضا تجری

خرداد ماه ۱۴۰۰

فرم شماره (3) صورتجلسه نهایی دفاع از پایان نامه دوره کارشناسي ارشد

با نام و یاد خداوند متعال، ارزیابی جلسه دفاع از پایان نامه کارشناسي ارشد خانم **انعام هلالات** با شماره دانشجویی **9717264** رشته **کامپیوتر** گرایش **هوش‌مصنوعی و رباتیک** تحت عنوان **احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند** که در تاریخ **400/03/24** با حضور هیأت محترم داوران در دانشگاه صنعتي شاهرود برگزار شد به شرح ذیل اعلام می‌گردد:

الف) درجه عالی: نمره 19-20 ☐ ب) درجه خیلی خوب: نمره 18/99 – 18 ☑
ج) درجه خوب: نمره17/99– 16☐ د) درجه متوسط: نمره 14-15/99 ☐
ه) کمتر از 14 غیر قابل قبول و نیاز به دفاع مجدد دارد ☐
نوع تحقیق: نظري √ عملي ☐

عضو هیأت داوران	نام ونام خانوادگي	مرتبهٔ علمي	امضاء
1- استاد راهنمای اول	دکتر منصور فاتح	استادیار	
2- استاد مشاور	دکتر محسن رضوانی	دانشیار	
3- استاد مشاور	دکتر علیرضا تجری	استادیار	
4- استاد داور اول	دکتر مرتضی زاهدی	استادیار	
5- استاد داور دوم	دکتر اسماعیل طحانیان	استادیار	
6- نماینده تحصیلات تکمیلي	محسن فرهادی	مربی	

نام و نام خانوادگی رئیس دانشکده: دکتر علیرضا الفی

تاریخ و امضاء و مهر دانشکده:

تقدیم به:

خدایی که آفرید

جهان را، انسان را، علم را، معرفت را، عشق را

و به کسانی که عشقشان را در وجودم دمید.

و

پدر و مادر عزیز و مهربانم

که در سختی‌ها و دشواری‌های زندگی، همواره یاوری دلسوز و فداکار و پشتیبانی محکم و مطمئن برایم بوده‌اند؛

از نگاهشان صلابت، از رفتارشان محبت

و از صبرشان ایستادگی را آموختم.

و

برادر و خواهرم

که وجودشان شادی بخش و صفایشان مایه آرامش من است.

تشکر و قدردانی و سپاس از:

اکنون پس از اتمام دوره کارشناسی ارشد بر خود لازم می‌دانم آیین قدردانی را بجا آورده و از تمامی کسانی که به نحوی مرا در به انجام رساندن این مهم یاری داده‌اند تشکر نمایم.

به اساتید ارجمندم جناب آقای **دکتر منصور فاتح**، **دکتر محسن رضوانی** و **دکتر علیرضا تجری** که با راهنمایی‌هایشان مرا در مراحل مختلف انجام رساله یاری کرده‌اند کمال سپاس گزاری خود را ابراز می‌دارم. از اساتید محترم هیئت داوران که با انتقادات و راهنمایی‌های مفیدشان در هنگام ارائه موضوع پایان نامه و جلسه دفاعیه سهم موثری در بالابردن کیفیت پایان نامه اینجانب داشته‌اند کمال سپاس و تشکر را دارم. همچنین تقدیر و سپاس از تمامی اساتید کامپیوتر که در طی دوره کارشناسی ارشد از دانش آن‌ها بهره برده‌ام را بر خود لازم می‌دانم.

در انتها لازم است مراتب تشکر و قدردانی خود را از خانواده‌ام که در طی مراحل مختلف تحصیل یار و یاور من بوده‌اند ابراز نمایم.

انعام هلالات

خرداد ماه ۱۴۰۰

تعهدنامه

اینجانب **انعام هلالات** دانشجوی دوره کارشناسی ارشد رشته **کامپیوتر گرایش هوش مصنوعی** دانشکده کامپیوتر دانشگاه صنعتی شاهرود نویسنده پایان‌نامه **احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند** تحت راهنمائی **دکتر منصور فاتح، دکتر محسن رضوانی، دکتر علیرضا تجری** متعهد می‌شوم.

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان‌نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می‌باشد و مقالات مستخرج با نام «دانشگاه صنعتی شاهرود» و یا « Shahrood University of Technology» به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تأثیرگذار بوده‌اند در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا چینی‌جاهای آن‌ها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

تاریخ

امضای دانشجو

چکیده

امروزه ایجاد تجهیزات تصویربرداری جدید و امکان پردازش و ویرایش آسان تصاویر، منجر به تولید حجم زیادی از تصاویر جعلی می‌شود. لذا روش‌های جرم‌کاوی تصویر برای تشخیص تصاویر جعلی معرفی شده‌اند. روش‌های مبتنی بر فرمت، می‌توانند جعل را در تصویر فشرده، شناسایی کنند. این روش‌ها عمدتا در فرمت تصویری JPEG به کار می‌روند. در میان فرمت‌های تصویری، فرمت JPEG از فراوانی و کاربرد بیشتری برخوردار است، به همین دلیل غالب موارد جعل تصاویر در این فرمت انجام می‌شود. در این رساله، روش جدیدی برای احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه شده است. برای جعل تصویر، ابتدا تصویر خروجی دوربین به نرم‌افزار مربوطه منتقل شده و سپس تغییرات لازم بر روی آن انجام می‌شود. یکی از مهم‌ترین پارامترهای تشخیص جعل تصاویر، منبع تصویر است. یعنی باید مشخص کرد که تصویر موردنظر، از دوربین اخذ شده یا در نرم‌افزاری مورد تغییر قرار گرفته است. جعل یا تغییر در تصاویر به کمک نرم‌افزارهای مختلفی از جمله فتوشاپ انجام می‌شود. یکی از راه‌کارهای شناسایی نرم‌افزار تغییر دهنده‌ی تصویر استفاده از اطلاعات سرآیند است. هر دوربین یا نرم‌افزار، ردپایی از خود در سرآیند تصویر بجای می‌گذارد که به کمک این ردپا امکان شناسایی مدل دوربین یا نرم‌افزار تغییر دهنده‌ی تصویر وجود دارد. در این رساله، الگوریتم جدیدی برای آشکارسازی جعل در جرم‌شناسی تصاویر با استفاده از اطلاعات سرآیند تصویر JPEG معرفی می‌شود. در این روش ابتدا با توجه به دادگان کاربردی در سرآیند تصویر JPEG، نوع نرم‌افزار ویرایشگر یا مدل دوربین را شناسایی کنیم و سپس با توجه به دیگر اطلاعات موجود در سرآیند نیز نرم‌افزار ویرایشگر و مدل دوربین را باری دیگر شناسایی کنیم و سپس در صورت عدم تطابق اطلاعات، سرآیند تغییر یافته را شناسایی کنیم.

نتایج ارزیابی روش‌های پیشنهاد شده با پایگاه داده جمع‌آوری شده نشان دادند که روش پیشنهادی احراز هویت تصویر، به‌خوبی انجام شده است و قابلیت استفاده در سیستم‌های عملیاتی را دارد. همچنین در روش پیشنهادی هرگونه ویرایش عکس با فتوشاپ به‌راحتی و بدون ابهام قابل شناسایی است.

کلیدواژه: جرم‌کاوی، احراز اصالت، پردازش تصویر، تشخیص جعل، تصویر JPEG

پیش‌گفتار

گسترش اینترنت، پیشرفت فناوری و ارائه تجهیزات تصویربرداری جدید و امکان پردازش و ذخیره‌سازی تصاویر در تجهیزاتی همانند دوربین و برنامه‌های موجود در اکثر تلفن‌های همراه، مزایای چشمگیر و غیرقابل انکاری به همراه آورده است که از آن مزایا می‌توان به ثبت خاطرات و لحظات به‌یادماندنی زندگی، ثبت وقایع مهم و مخابره خبرها، اشتراک‌گذاری اطلاعات، داشتن نسخه پشتیبان از مدارک ارزشمند،کاهش فضای فیزیکی مورد نیاز برای نگهداری اسناد و ابداع مجلات دیجیتالی اشاره کرد. در چندین سال اخیر با متداول شدن دوربین‌های تصویربرداری و مجهز شدن تلفن‌های همراه به این دوربین‌ها، امکان استفاده از مدارک تصویری محکمه پسند این نوید را می‌داد که این امکانات تصویر-برداری، موجب احقاق حق بهتر انسان‌ها شوند و از تضییع حقوق آن‌ها جلوگیری کنند؛ اما متاسفانه در این روزها، تهیه و ارائه برخی فناوری‌های دیجیتال مانند نرم‌افزارهای ویرایش عکس و فیلم، اعتماد و انتظارات پیشین از این فناوری‌های تصویری را کاهش داده‌اند؛ تاحدی که گاهی حتی بر عکس عمل می‌کنند؛ زیرا این نرم‌افزارهای ویرایش تصویر می‌توانند تصاویری باقابلیت واقعیت نمایی[۱] بالا تولید نمایند. تصاویر دستکاری شده[۲] همه‌روزه و به‌صورت فزاینده‌ای تولید می‌شوند و به‌منظور کلاه‌برداری و منافع شخصی افراد قانون گریز، ارائه می‌شوند. البته باید این نکته را نیز مدنظر داشت که این دستکاری‌ها از منظر برخی کاربردها مانند آگهی‌های تبلیغاتی همچنین تجارت الکترونیک مطلوب و مناسب هستند.

اصطلاح دستکاری عمدی هنگامی برای تصویر به کار می‌رود که به‌منظور کتمان یک واقعیت باشد و با حذف بخش‌هایی از تصویر، پنهان یا اضافه کردن بخش‌هایی به آن منجر به اشتباه انداختن ناظر و یا القای باور غلط از یک صحنه انجام شود؛ وگرنه به انجام عملیات پردازش تصویری مانند ارتقای کنتراست،[۳] بهبود رنگ[۴] یا روشنایی[۵] تصویر، گفته نمی‌شود.

---

۱. Reality
۲. Tampered
۳. Contrast
۴. Color Enhancement
۵. Illumination Enhancement

لیست مقالات مستخرج از پایان نامه

۱-

۲-

۳-

فهرست مطالب

فهرست جداول **خ**

فهرست اشکال **د**

فهرست کلمات اختصاری **ر**

فهرست علائم و نشانه‌های اختصاری **ز**

فصل۱ : مقدمه **۱**

۱-۱ مقدمه ۲

۱-۲ تاریخچه جعل ۲

۱-۳ شرح مسئله ۴

۱-۴ چالش‌های مهم تحقیق ۵

۱-۵ اهداف تحقیق ۸

۱-۶ سوالات و فرضیه‌ها ۸

۱-۷ دلایل ضرورت تحقیق ۹

۱-۸ نوآوری‌ها ۹

۱-۹ ساختار پایان‌نامه ۱۰

فصل۲ : کارهای پیشین **۱۱**

۲-۱ مقدمه ۱۲

۲-۲ روش‌های تشخیص دستکاری تصویر ۱۲

۲-۳ تکنیک‌های تشخیص تصویر نامعتبر ۱۲

۲-۳-۱ تکنیک‌های مبتنی بر پیکسل ۱۳

۲-۳-۱-۱ کپی و انتقال ۱۳
۲-۳-۱-۲ نمونه‌برداری مجدد (تغییر اندازه، کشش، چرخش) ۱۴
۲-۳-۱-۳ چسباندن ۱۶
۲-۳-۱-۴ آماری ۱۸
۲-۳-۲ تکنیک‌های مبتنی بر فرمت ۱۹
۲-۳-۲-۱ مضاعف JPEG ۱۹
۲-۳-۲-۲ چندی‌سازی JPEG ۱۹
۲-۳-۲-۳ مسدود کردن JPEG ۲۱
۲-۳-۳ تکنیک‌های مبتنی بر دوربین ۲۲
۲-۳-۳-۱ آرایه فیلتر رنگ ۲۲
۲-۳-۳-۲ حسگر نویز ۲۲
۲-۳-۴ تکنیک‌های مبتنی بر فیزیک محیطی ۲۳
۲-۳-۵ تکنیک‌های مبتنی بر هندسه ۲۴
۲-۳-۵-۱ نقطه اصلی ۲۴
۲-۴ مقایسه روش‌های تشخیص جعلی تصویر منفعل ۲۵
۲-۵ جمع‌بندی ۲۸
فصل۳ : تعاریف و مفاهیم مبنایی **۳۱**
۳-۱ مقدمه ۳۲
۳-۲ فشرده‌سازی JPEG ۳۲
۳-۳ مراحل فشرده‌سازی JPEG ۳۳
۳-۴ توضیحات کلی راجع به استاندارد JPEG ۳۵
۳-۴-۱ حالت‌های مختلف کدینگ ۳۵

۳-۴-۱-۱ کدینگ رشته‌ای مبتنی بر DCT ۳۶
۳-۴-۱-۲ روش‌های مختلف کدینگ مبتنی بر آنتروپی ۳۶
۳-۴-۱-۳ دقت هر نمونه ۳۷
۳-۴-۲ کوچک‌ترین واحد کد شده (MCU) ۳۷
۳-۴-۳ فرمت‌های فشرده‌سازی JPEG ۳۷
۳-۴-۴ پارامترها، شاخص‌ها، قطعات شاخص و قطعات کد شده مبتنی بر آنتروپی ۳۹
۳-۵ بررسی ترتیب اجزاء اصلی فایل JPEG در حالت‌های کدینگ رشته‌ای ۴۲
۳-۵-۱ سرآیند فریم ۴۴
۳-۵-۲ سرآیند اسکن ۴۶
۳-۵-۳ جدول‌ها و قطعات شاخص متفرقه ۴۹
۳-۵-۳-۱ جدول کوانتیزاسیون ۵۰
۳-۵-۳-۲ جدول هافمن ۵۱
۳-۵-۴ دادگان کاربردی (نرم‌افزاری) ۵۲
۳-۵-۴-۱ قالب تبادل فایل JPEG (JFIF) ۵۳
۳-۵-۴-۲ قالب فایل تصویری تعویض‌پذیر (EXIF) ۵۴
۳-۵-۴-۳ دادگان کاربردی فتوشاپ ۵۵
۳-۵-۴-۴ دادگان کاربردی APP14 ..... ۵۵
۳-۵-۵ تعریف تعداد سطرها (DNL) ۵۵
۳-۶ جمع‌بندی ۵۶
فصل۴ : روش پیشنهادی **۵۷**
۴-۱ مقدمه ۵۸
۴-۲ روش پیشنهادی احراز هویت تصاویر JPEG ۵۸

۴-۲-۱ بررسی و استخراج اطلاعات مهم سرآیند تصاویر JPEG: ۶۰
۴-۲-۱-۱ آشنایی با نرم‌افزارهای استخراج، تولید و ویرایش سرآیند JPEG و استفاده از آن‌ها ۶۰
۴-۲-۲ عدم وجود دادگان کاربردی در اطلاعات سرآیند تصویر JPEG ۶۱
۴-۲-۳ بررسی و استخراج اطلاعات مهم دادگان کاربردی (نرم‌افزاری) ۶۱
۴-۲-۳-۱ قالب تبادل فایل JPEG (JFIF) ۶۲
۴-۲-۳-۲ قالب فایل تصویری تعویض‌پذیر (EXIF) ۶۲
۴-۲-۳-۳ دادگان کاربردی فتوشاپ ۶۴
۴-۲-۳-۴ دادگان کاربردی APP14 ۶۴
۴-۲-۴ استخراج امضای تصویر از روی جدول کوانتیزاسیون و کدینگ هافمن ۶۴
۴-۲-۵ انطباق امضای تصویر با اطلاعات سرآیند تصویر JPEG ۷۰
۴-۳ داده‌کاوی اطلاعات سرآیند ۷۱
۴-۴ ترتیب متداول بخش‌های مختلف در فایل JPEG ۷۱
۴-۵ تهیه دادگان و داده‌کاوی آن‌ها ۷۲
۴-۶ تولید دادگانی از سرآیندها ۷۲
۴-۷ جمع‌بندی ۷۳
فصل۵ : پیاده‌سازی و ارزیابی نتایج **۷۵**
۵-۱ مقدمه ۷۶
۵-۲ مجموعه داده ۷۷
۵-۳ ابزارهای مورد استفاده برای پیاده‌سازی ۷۷
۵-۴ ارزیابی نتایج ۷۸
۵-۴-۱ تفاوت تصویر اصلی با تصویر ذخیره شده در نرم‌افزار فتوشاپ ۷۸

۵-۴-۲ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Paint ۸۰
۵-۴-۳ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار متلب ۸۰
۵-۴-۴ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار ACDSee Pro ۸۱
۵-۴-۵ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Program4pc-Photo Editor ۸۲
۵-۴-۶ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار GIMP ۸۲
۵-۴-۷ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Corel AfterShot Pro ۸۳
۵-۴-۸ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Capture NX ۸۳
۵-۴-۹ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Corel Painter ۸۴
۵-۴-۱۰ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Adobe Photoshop Light room ۸۵
۵-۵ داده‌کاوی اطلاعات سرآیند: ۸۵
۵-۵-۱ داده‌کاوی بر روی زیر نمونه‌برداری در پایگاه داده ۸۶
۵-۵-۲ داده‌کاوی بر روی دادگان کاربردی (نرم‌افزاری) ۸۷
۵-۵-۳ داده‌کاوی بر روی شاخص آغاز فریم (SOF) ۹۱
۵-۵-۴ داده‌کاوی قطعه شاخص سرآیند فریم (SOF) ۹۳
۵-۵-۵ داده‌کاوی بر روی جدول کوانتیزاسیون (DQT) ۹۴
۵-۵-۶ داده‌کاوی قطعه شاخص تعریف شروع مجدد (DRI) ۹۴
۵-۵-۷ داده‌کاوی جداول هافمن (DHT) ۹۵
۵-۶ مقایسه روش پیشنهادی با روش‌های مبتنی بر فرمت ۹۵
۵-۷ جمع‌بندی ۹۶
فصل۶ : نتیجه‌گیری و پیشنهادها برای کارهای آتی **۹۷**
۶-۱ مقدمه ۹۸

۲-۶ نتیجه‌گیری و پیشنهادها برای کارهای آتی ۹۸

پیوست **۱۰۰**

مراجع **۱۰۹**

واژه‌نامه مرتب بر اساس حروف الفبای انگلیسی **۱۱۲**

واژه‌نامه مرتب بر اساس حروف الفبای فارسی **۱۱۸**

فهرست جداول

جدول ۲-۱: مقایسه روش‌های مبتنی بر پیکسل در تشخیص جعلی تصویر منفعل ۲۵
جدول ۲-۲: مقایسه روش‌های مبتنی بر فیزیک محیطی در تشخیص جعلی تصویر منفعل ۲۶
جدول ۲-۳: مقایسه روش‌های مبتنی بر هندسه در تشخیص جعلی تصویر منفعل..... ۲۷
جدول ۲-۴: مقایسه روش‌های مبتنی بر فرمت در تشخیص جعلی تصویر منفعل ۲۷
جدول ۲-۵: مقایسه روش‌های مبتنی بر دوربین در تشخیص جعلی تصویر منفعل ۲۸
جدول ۳-۱: فرآیند انکدینگ معمولی مبتنی بر DCT.....۳۶
جدول ۳-۲: انواع شاخص‌های فایل JPEG [۵۱]. ۴۱
جدول ۳-۳: پارامترهای موجود در سرآیند فریم، اندازه هر یک (برحسب بیت) و مقادیر مجاز آن‌ها.....۴۶
جدول ۳-۴: پارامترهای موجود در سرآیند اسکن، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها... ۴۹
جدول ۳-۵: پارامترهای موجود در بخش تخصیص جدول کوانتیزاسیون، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها ۵۱
جدول ۳-۶: پارامترهای موجود در بخش تخصیص جدول هافمن، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها ۵۲
جدول ۳-۷: پارامترهای موجود در بخش دادگان کاربردی، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها..... ۵۳
جدول ۳-۸: اطلاعات JFIF..... ۵۴
جدول ۳-۹: پارامترهای موجود در بخش تعریف تعداد سطرها، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها ۵۶
جدول ۴-۱: قابلیت نرم‌افزار EXIFTOOL برای ویرایش و تولید بخش‌های سرآیند تصاویر.....۶۱
جدول ۵-۱: شرایط نمونه‌برداری..... ۸۷
جدول ۵-۲: مقایسه روش پیشنهادی با روش‌های مبتنی بر فرمت در تشخیص جعلی تصویر منفعل.....۹۶

فهرست اشکال

شکل۱-۱: نمونه‌هایی از تصاویر جعلی در سال‌های دور ۳
شکل ۱-۲: نمونه‌هایی از تصاویر جعلی در سال‌های دور ۳
شکل ۱-۳: طبقه‌بندی رویکردهای جعل تصویر ۷
شکل ۳-۱: مراحل فشرده‌سازی به روش JPEG ۳۴
شکل ۳-۲: نمایش مراحل ذخیره‌سازی یک تصویر نمونه به روش JPEG ۳۵
شکل ۳-۳: نمایش حالت کدینگ رشته‌ای (دنباله‌ای) مبتنی بر DCT ۳۶
شکل ۳-۴: توصیف کلی و سرتاسری قسمت‌های مهم فایل JPEG در فرمت Interchange ۴۳
شکل ۳-۵: اجزاء و ترتیب قرارگیری بایت‌ها در داخل سرآیند فریم ۴۴
شکل ۳-۶: اجزاء و ترتیب قرارگیری بایت‌ها در داخل سرآیند فریم ۴۸
شکل ۳-۷: قطعات شاخص متفرقه ۴۹
شکل ۳-۸: تخصیص جدول کوانتیزاسیون ۵۰
شکل ۳-۹: تخصیص جدول هافمن ۵۲
شکل ۳-۱۰: دادگان کاربردی ۵۳
شکل ۳-۱۱: تعریف تعداد سطرها ۵۶
شکل ۴-۱: چارت مراحل روش پیشنهادی ۵۹
شکل ۴-۲: جدول کوانتیزاسیون استاندارد ۶۵
شکل ۴-۳: جدول کوانتیزاسیون متناسب با دوربین Canon – Canon PowerShot G1 (Superfine) با نمونه‌برداری رنگ ۱×۲ ..... ۶۵
شکل ۴-۴: جدول کوانتیزاسیون متناسب با نرم‌افزار Photoshop – (Save For Web 070) با نمونه‌برداری رنگ ۱×۱ ..... ۶۶
شکل ۴-۵: جداول کدینگ هافمن استاندارد ۶۷
شکل ۴-۶: جداول کدینگ هافمن استاندارد تصویر بندانگشتی ۶۸
شکل ۴-۷: جداول کدینگ هافمن بهینه Canon – Canon PowerShot SX260 HS ۶۸
شکل ۴-۸: جداول کدینگ هافمن متناسب با دوربین Canon PowerShot SX700 HS ۶۹
شکل ۴-۹: جداول کدینگ هافمن متناسب با نرم‌افزار فتوشاپ Adobe Photoshop CS5 Windows ۶۹
شکل ۵-۱: اطلاعات دادگان کاربردی JFIF تصویر اصلی ۷۸
شکل ۵-۲: بخشی از اطلاعات EXIF تصویر مشکوک به جعل ۷۸
شکل ۵-۳: اطلاعات دادگان کاربردی تصویر مشکوک به جعل ۷۹
شکل ۵-۴: قطعه DRI در اطلاعات سرآیند تصویر مشکوک به جعل ۷۹

شکل ۵-۵: قطعه APP13 و APP14 و DRI در اطلاعات سرآیند تصویر بندانگشتی مشکوک به جعل. ۸۰
شکل ۵-۶: اطلاعات بخش تصویر بندانگشتی در تصویر اصلی ۸۰
شکل ۵-۷: قطعه COM در اطلاعات سرآیند تصویر مشکوک به جعل ۸۱
شکل ۵-۸: قطعه APP1 در اطلاعات سرآیند تصویر اصلی ۸۱
شکل ۵-۹: حالت کدینگ تصاعدی ۸۲
شکل ۵-۱۰: بخشی از اطلاعات EXIF تصویر اصلی ۸۳
شکل ۵-۱۱: بخشی از اطلاعات EXIF تصویر مشکوک به جعل ۸۴
شکل ۵-۱۲: بخشی از اطلاعات EXIF تصویر مشکوک به جعل ۸۵
شکل ۵-۱۳: نمونه‌برداری ۴:۲:۰ ..... ۸۶
شکل ۵-۱۴: فراوانی دادگان کاربردی در تمام تصاویر پایگاه داده ۸۸
شکل ۵-۱۵: فروانی دادگان کاربردی در تصاویر بدون فتوشاپ در پایگاه داده ۸۹
شکل ۵-۱۶: فروانی پارامترهای JFIF ۸۹
شکل ۵-۱۷: فراوانی پارامترهای EXIF ۹۰
شکل ۵-۱۸: فراوانی فرمت ذخیره‌سازی اطلاعات در EXIF ۹۰
شکل ۵-۱۹: فراوانی وجود تصویر بندانگشتی ۹۱
شکل ۵-۲۰: فراوانی اندازه‌های تصویر بندانگشتی ۹۱
شکل ۵-۲۱: فراوانی انواع فشرده‌سازی در تصاویر JPEG ۹۲
شکل ۵-۲۲: فراوانی انواع فشرده‌سازی در تصاویر بندانگشتی JPEG ۹۳
شکل ۵-۲۳: پارامترهای قطعه شاخص سرآیند اسکن در حالت فشرده‌سازی Baseline DCT ۹۳
شکل ۵-۲۴: سه جز مختلف پارامترهای قطعه شاخص سرآیند فریم در تصویر اصلی در حالت فشرده سازی Baseline DCT ۹۳
شکل ۵-۲۵: کل قطعه شاخص سرآیند فریم در تصویر در حالت فشرده‌سازی Baseline DCT ۹۴
شکل ۵-۲۶: دو مورد پر کاربرد کل قطعه شاخص سرآیند فریم در حالت فشرده‌سازی Baseline DCT۹۴
شکل ۵-۲۷: کل قطعه شاخص سرآیند فریم در تصویر بندانگشتی در حالت فشرده‌سازی Baseline DCT ۹۴
شکل ۵-۲۸: پارامترهای قطعه شاخص تعریف شروع مجدد ۹۵
شکل ۵-۲۹: فراوانی جداول هافمن ۹۵

فهرست کلمات اختصاری

عنوان	کلمه اختصاری
نقشه‌های ویژگی درهم‌پیچیده افزودنی	Augmented Convolutional Feature Maps (ACFM)
نقشه‌های ویژگی درهم‌پیچیده افزودنی	Augmented Convolutional Feature Maps (ACFM)
شبکه‌های عصبی درهم‌پیچیده	Convolutional Neural Networks (CNNs)
آرایه فیلتر رنگ	Color Filter Array (CFA)
تعریف تعداد سطرها	Define Number of LinesD (DNL)
شاخص معرف جدول هافمن	Define Huffman Table Marker (DHT)
شاخص معرف جدول کوانتیزاسیون	Define Quantization Table Marker (DQT)
بازه شروع مجدد تعریف شده	Defind Restart Interval (DRI)
انتهای تصویر	End of Image (EOI)
قالب فایل تصویری تعویض‌پذیر	Exchangeable Image File Format (EXIF)
ماشین یادگیری افراطی	Extreme Learning Machine (ELM)
موقعیت مکانی	Global Positioning System (GPS)
هویت بین‌المللی تجهیزات تلفن همراه	International Mobile Equipment Identity (IMEI)
راهنمای فایل تصویر	Image File Directory (IFD)
گروه مشترک متخصصان عکاسی	Joint Photographic Experts Group (JPEG)
قالب تبادل فایل JPEG	JPEG File Interchange Format (JFIF)
شرکت خدمات مهندسی الکترونیک در ژاپن	Japanese Electronics Industry Development Association (JEIDA)
حافظه کوتاه مدت	Long Short-Term Memory (LSTM)
آنالیز تبعیض آمیز خطی	Linear Discriminant Analysis (LDA)
کوچک‌ترین واحد کد شده	Minimum Coded Unit (MCU)
باقیمانده فیلتر میانه	Median Filtering Residual (MFR)
تحلیل مؤلفه‌های اصلی	Principal Component Analysis (PCA)
توابع چگالی احتمال	Probability Density Functions (PDFs)
کدگذاری طول گام	Run Length Encoding (RLE)
آغاز تصویر	Start of Image (SOI)
آغاز فریم	Start Of Frame (SOF)
آغاز اسکن	Start Of Scan (SOS)
خود کدگذار پشته‌ای	Stacked Auto-Encoders (SAE)
ماشین بردار پشتیبان	Support Vector Machine (SVM)
الگوی نویز حسگر	Sensor Pattern Noise (SPN)

فهرست علائم و نشانه‌های اختصاری

عنوان	علامت اختصاری
موقعیت بالای بیت تخمینی در دنباله	Ah
چهار بیت پرارزش‌تر بایت	MSB
چهار بیت کم‌ارزش‌تر بایت	LSB
حالت کدینگ رشته‌ای معمولی (Baseline) مبتنی بر DCT (و کدینگ هافمن)	SOF_0
طول سرآیند فریم	Lf
دقت نمونه	P
تعداد سطرها	Y
تعداد نمونه‌ها	X
تعداد مؤلفه‌های تصویری موجود در فریم	Nf
معرف مؤلفه	C_i
فاکتور نمونه‌برداری افقی	H_i
فاکتور نمونه‌برداری عمودی	V_i
انتخاب‌گر آدرس جدول کوانتیزاسیون	Tq_i
طول سرآیند اسکن	Ls
تعداد مؤلفه‌های تصویری داخل یک اسکن	Ns
انتخاب‌گر مؤلفهٔ اسکن	Cs_j
انتخاب‌گر آدرس جدول مربوط به کدینگ آنتروپی DC	Td_j
انتخاب‌گر آدرس جدول مربوط به کدینگ آنتروپی AC	Ta_j
محل شروع انتخاب طیفی یا تخمین‌گر	Ss
پایان انتخاب طیفی	Se
موقعیت پائین بیت تخمینی در دنباله یا تخمین نقطه‌ای	Al
طول جدول کوانتیزاسیون	Lq
دقت المان‌های موجود در جدول کوانتیزاسیون	Pq
معرف آدرس جدول کوانتیزاسیون	Tq
المانی از جدول کوانتیزاسیون	Q_K
طول جدول هافمن	Lh
کلاس (گروه) جدول	Tc
معرف آدرس جدول هافمن	Th
تعداد کدهای هافمن دارای طول i	L_i
مقدار اختصاص یافته به هر کد هافمن	$V_{i,j}$
طول بخش داده‌گان کاربردی	Lp
بایت‌های داده‌گان کاربردی	Ap_i
طول قطعه شاخص تعریف تعداد سطرها (بر حسب بایت)	Ld
تعداد سطرها	NL

فصل۱ : مقدمه

۱-۱ مقدمه

امروزه هر پیشرفتی در دنیای دیجیتال امکان‌پذیر است، استفاده از تصاویر روز به‌روز در زندگی ما بیشتر می‌شود و انگیزه ایجاد تصاویر دستکاری‌شده نیز به‌طور هم‌زمان افزایش می‌یابد [۱]. پیشرفت فن‌آوری‌های تصویربرداری دیجیتال منجر به توسعه دوربین‌ها و اسکنرهای دیجیتال با هزینه کم و کیفیت وضوح بالا شده است. تصاویر دیجیتال می‌توانند توسط انواع فن‌آوری‌ها از جمله دوربین‌های دیجیتال، اسکنرها و نرم‌افزارهای گرافیکی تولید شوند و به‌طور گسترده، در تصویربرداری پزشکی، اجرای قانون و بانکداری استفاده شوند [۲]. تصاویر دیجیتال را با دستگاه‌های سخت‌افزاری کم هزینه و ابزارهای نرم‌افزاری به‌راحتی و بدون هیچ گونه مدرکی می‌توان ویرایش و اصلاح کرد [۳]. انتشار نرم‌افزار برای تولید تصاویر دیجیتالی دستکاری شده، به‌طور چشم‌گیری افزایش یافته است [۲، ۴]. امروزه استفاده از فیلم یا تصاویر دیجیتال به‌عنوان مدرکی برای مبارزه با جرائم فیزیکی و سایبری، جرم‌شناسی[۱] چندرسانه‌ای شامل تأیید و شناسایی دوربین منبع، طبقه‌بندی تصاویر مبدا گرا، تأیید صحت، تشخیص جعل،[۲] احراز هویت[۳] و غیره بسیار حائز اهمیت است [۵]. ایجاد تصاویر جعلی برای پنهان کردن برخی از اطلاعات مفید تصویر نیز روز به‌روز ساده‌تر شده و در حال افزایش است. امروزه با پیشرفت فناوری دیجیتال و حرکت آن به‌سوی دنیای مگا پیکسل،[۴] امکان تشخیص تصاویر جعلی وجود دارد [۱]. جرم-شناسی دیجیتال برای اعتبار بخشی به تصاویر دیجیتال پدید آمده است [۶].

برای جعل تصاویر باید ابتدا تصویر خروجی دوربین را به نرم‌افزار مربوطه منتقل کرد و سپس تغییرات لازم را بر روی آن انجام داد. یکی از مهم‌ترین پارامترهای تشخیص جعل تصاویر، منبع تصویر است. یعنی باید مشخص کرد که تصویر موردنظر، از دوربین اخذ شده یا در نرم‌افزاری مورد تغییر قرار گرفته است. ما در این رساله قصد داریم تا به بررسی این مسئله بپردازیم.

در ادامه این فصل، در بخش‌های بعدی به تاریخچه جعل تصویر، شرح مسئله، چالش‌های احراز هویت تصاویر، هدف از انجام پژوهش، معرفی مسائل و فرضیات موجود در احراز هویت تصاویر، دلایل ضرورت پژوهش و نوآوری خواهیم پرداخت.

۱-۲ تاریخچه جعل

تصاویر حاصل از عکس‌برداری، اعتبار و صحت قانونی خود را به دلیل جعل تصاویر از دست داده‌اند. تنها طی چند دهه گذشته، در تصاویر به نسبت زیادی دستکاری و جعل رخ داده است. با ظهور

---

۱. Forensics
۲. Forgery Detection
۳. Authentication
۴. Megapixels

دوربین‌های دیجیتال با تفکیک‌پذیری بالا، رایانه‌های شخصی قدرتمند و نرم‌افزارهای ویرایش عکس ماهرانه، دستکاری و جعل عکس‌ها و تصاویر، معمول‌تر و رایج‌تر شده است. البته تعدادی از تصاویر که در سال‌های دور و در اواسط دهه ۱۸۰۰ دستکاری شده‌اند. در شکل ۱-۱ یک نمونه تصویر جعلی را مشاهده می‌کنید. این عکس یک نمونه تصویر جعلی مربوط به سال ۱۸۶۴ بود که در خلال جنگ آمریکا گرفته شده بود. با تلاش محققان مربوط به جعل تصویر، مشخص شد این عکس، ترکیبی از سه عکس مختلف است که ماهرانه با یکدیگر ترکیب شده بودند [۷].

شکل۱-۱: نمونه‌هایی از تصاویر جعلی در سال‌های دور

نمونه تصویر جعلی دیگر در شکل ۱-۲ مربوط به سال ۱۸۶۵ است که به رهبران جنگ داخلی آمریکا باز می‌گردد که عکس ژنرال شرمان و یارانش را نشان می‌داد. در این تصویر، ژنرال فرانچزپی‌بیلر[۱] حضور نداشت و بعدا به‌عکس اضافه شد [۷].

شکل۱-۲: نمونه‌هایی از تصاویر جعلی در سال‌های دور

۱. Frances P. Biller

۳-۱ شرح مسئله

شناسایی تغییر در تصاویر یکی از مهم‌ترین مباحث جرم‌شناسی تصویری است. یکی از مهم‌ترین تغییرات موجود در تصویر ناشی از جعل در تصاویر است. انواع جعل در تصاویر شامل، فشرده‌سازی مجدد[۱]تصویر، تار کردن[۲] ترکیب دو یا چند تصویر، کپی بخشی از یک تصویر، حذف بخشی از یک تصویر و ویرایش و دستکاری[۳]یک عکس هستند.

جعل یا تغییر در تصاویر به کمک نرم‌افزارهای مختلفی از جمله فتوشاپ[۴]انجام می‌شود. یکی از راه‌کارهای شناسایی نرم‌افزار تغییر دهنده‌ی تصویر استفاده از اطلاعات سرآیند[۵]است. هر دوربین یا نرم‌افزار، ردپایی از خود در سرآیند تصویر بجای می‌گذارد که به کمک این ردپا امکان شناسایی مدل دوربین یا نرم‌افزار تغییر دهنده‌ی تصویر وجود دارد.

بخشی از سرآیند تصاویر JPEG شامل اطلاعات EXIF و JFIF است که اطلاعاتی اضافی از تصویر JPEG را در اختیار کاربر قرار می‌دهد [۸]. اولین ردپای استفاده از نرم‌افزارهای ویرایش تصویر در این بخش‌ها به چشم می‌خورد و با تحلیل مناسب این بخش‌ها می‌توان نرم‌افزار ویرایشگر تصویر را شناسایی کرد.

گاهی افرادی که جعل در تصاویر را انجام می‌دهند این اطلاعات اضافی را حذف می‌کنند تا نرم‌افزار ویرایشگر مشخص نشود. اما این ردپا در برخی دیگر از اجزای سرآیند مانند ماتریس کوانتیزاسیون[۶]یا کدینگ هافمن[۷]وجود دارد که قابل حذف نیست.

برای جعل تصاویر باید ابتدا تصویر خروجی دوربین را به نرم‌افزار مربوطه منتقل کرد و سپس تغییرات لازم را بر روی آن انجام داد. یکی از مهم‌ترین پارامترهای تشخیص جعل تصاویر، منبع تصویر است. یعنی باید مشخص کرد که تصویر موردنظر، از دوربین اخذ شده یا در نرم‌افزاری مورد تغییر قرار گرفته است. ما در این رساله قصد داریم آخرین منبع تصویر را مشخص نماییم. سپس با توجه به آخرین منبع عکس می‌توان مشخص کرد که تصویر متعلق به دوربین است یا در نرم‌افزار ویرایشگر تصویر ذخیره شده است.

در میان فرمت‌های تصویری، فرمت JPEG از فراوانی و کاربرد بیشتری برخوردار است. غالب موارد جعل تصاویر روی این فرمت انجام می‌شود. فرمت JPEG با سیستم‌عامل‌های مختلف سازگار است. این فرمت فشرده‌سازی[۸] مناسبی دارد و استفاده فراوانی توسط کاربران دارد [۹]. از این‌رو در این رساله، احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند انجام خواهد شد.

---

۱. Recompressed
۲. Blur
۳. Tampered
۴. Photoshop
۵. Header
۶. Quantization Table
۷. Huffman Coding
۸. Compression

۱-۴ چالش‌های مهم تحقیق

به‌طور مشخص می‌توان مسائل زیر را به‌عنوان چالش احراز هویت تصاویر اشاره نمود:

۱. ایجاد تصویر JPEG با اطلاعات سرآیند متمایز: دوربین‌های متفاوت سرآیندهای متفاوتی برای تصاویر JPEG ایجاد می‌کنند. از این‌رو، تحلیل‌های جرم‌شناسی باید مبتنی به دادگانی از متنوع‌ترین انواع دوربین باشد تا نتایج مناسبی را به ارمغان آورد [۱۰].

۲. پنهان کردن آثار دستکاری اطلاعات سرآیند تصویر: کسی که تصاویر را جعل می‌کند، می‌تواند با استخراج امضای دوربین، تغییر تصویر و سپس ذخیره مجدد تصویر با فرمت EXIF مناسب و کلیه پارامترهای مناسب از جمله: اندازه تصویر، جدول کوانتیزاسیون تصویر، کدینگ هافمن تصویر، اندازه تصویر بندانگشتی[۱] جدول کوانتیزاسیون تصاویر بندانگشتی و کدینگ هافمن تصویر بندانگشتی، اثر دستکاری آن‌ها را پنهان کند. اگرچه قطعا این امکان‌پذیر است، اما در حال حاضر فراتر از حد نرم‌افزارهای مشهور ویرایش عکس است [۱۰].

۳. احراز هویت تصویر JPEG به کمک اطلاعات سرآیند: امضای دوربین شامل: جدول کوانتیزاسیون، کدینگ هافمن، اطلاعات دادگان کاربردی (نرم‌افزاری) است که از سرآیند تصویر JPEG استخراج می‌شود، از این امضا برای تأیید اعتبار تصویر دیجیتال استفاده می‌شود. با مقایسه این امضا با امضای دوربین‌های معتبر و شناخته شده، منبع عکس شناسایی می‌شود. اما این روش در برابر عکس‌برداری مجدد با دوربین اصلی از عکس جعل شده که اطلاعات سرآیند را بازسازی می‌کند، آسیب‌پذیر است [۱۰].

۴. تغییرات مداوم فن‌آوری دستگاه‌های تولید تصویر: قدرت تحلیل جرم‌شناسی در توانایی به دست آوردن امضا از طیف گسترده‌ای از دوربین‌ها و تلفن‌های همراه نهفته است. با توجه به اینکه دائماً دوربین‌ها و تلفن‌های همراه جدید منتشر خواهد شد، چالش‌های مهمی را ایجاد می‌کند. برای پیگیری این تغییرات مداوم، نیاز به تداوم ساخت پایگاه داده از تصاویر و اطلاعات دوربین است [۱۰].

۵. کاهش عملکرد شناسایی مدل دوربین به دلیل عملیات پس پردازش تصاویر: الگوریتم‌های زیادی برای شناسایی مدل دوربین پیشنهاد شده است. اما عملکرد این روش‌ها در صورتی که تصویر در معرض پس پردازش[۲] باشد، به میزان قابل ملاحظه‌ای کاهش می‌یابد. کاهش در عملکرد روش‌های شناسایی مدل دوربین، در عملیاتی مانند تغییر اندازه[۳] نمونه‌برداری مجدد[۴] و فشرده‌سازی JPEG بیشتر بروز می‌کند. این تخریب عملکرد یک مشکل مهم است، زیرا وب‌سایت‌های اشتراک‌گذاری عکس برخط[۵] و برنامه‌های رسانه‌های اجتماعی غالباً تصاویر را تغییر اندازه می‌دهند یا آن‌ها را دوباره فشرده می‌کنند.

---

۱. Thumbnail

۲. post-processing

۳. Resizing

۴. Resampling

۵. Online

برای اینکه رویکردهای شناسایی مدل دوربین در سناریوهای دنیای واقعی کار کنند، باید روش‌هایی ابداع شوند تا آن‌ها را نسبت به این عملیات رایج پس پردازش قوی‌تر کند [۱۱].

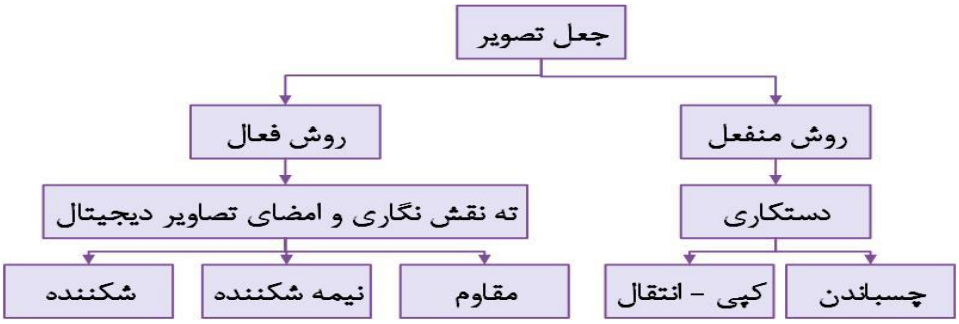
۶. متمایز بودن فرآیند تولید تصویر در دوربین‌ها: شناسایی مدل دوربین‌ها در کاربردهایی از جمله تشخیص جعل تصویر ضروری است. عملیات و مراحل ثبت تصویر برای کلیه دوربین‌های دیجیتال متداول است، اما جزئیات پردازش دقیق از یک تولیدکننده در هر مرحله تا مرحله دیگر در مدل‌های مختلف دوربین همان شرکت متفاوت است [۱۲].

۷. تغییر مفهوم معنایی تصویر: مفهوم معنایی[۱] یک تصویر، با بهره‌گیری از روش‌های دستکاری[۲] مانند چسباندن[۳] اشیا یک تصویر با تصاویر دیگر و همچنین حذف اشیائی از تصویر به‌راحتی قابل تغییر است. همچنین با ظهور ابزارهای پیشرفته ویرایش تصویر، می‌توان یک تصویر را از جهت‌های مختلف دستکاری کرد [۱۳]. انواع دستکاری تصاویر به دو دسته طبقه‌بندی می‌شود: (۱) تغییر در تصویر با حفظ محتوا[۴] و (۲) تغییر در تصویر بدون حفظ محتوا[۵][۱۴]. نوع اول دستکاری (به‌عنوان مثال، فشرده‌سازی، تار شدن و تقویت کنتراست[۶] عمدتاً به دلیل پس پردازش اتفاق می‌افتد که هیچ محتوای معنایی را تغییر نمی‌دهند و کمتر مخرب محسوب می‌شوند. نوع دوم (به‌عنوان مثال، کپی- انتقال[۷] چسباندن و حذف جسم) محتوای تصویر را به‌طور دلخواه تغییر داده و مفهوم معنایی را به‌طور قابل توجهی تغییر می‌دهد [۱۴]. دستکاری تغییر محتوا می‌تواند اطلاعات غلط یا گمراه‌کننده را به تصویر اضافه کند. به‌تازگی، تشخیص دستکاری در تصویر یا فیلم بدون حفظ محتوای آن، مورد توجه زمینه‌های مختلف علمی، امنیتی و نظارتی قرار گرفته است. شناسایی این دستکاری‌ها به دلیل اینکه نواحی دستکاری شده تصاویر از نظر بصری آشکار نیستند به مسئله‌ای چالش برانگیز تبدیل شده است [۱۳].

۸. دستکاری تصویر با روش‌های فعال و غیرفعال: جعل تصویر دیجیتال در شکل ۱-۳ به دو گروه اصلی با عنوان رویکردهای فعال[۸] و منفعل[۹] طبقه‌بندی شده است. در روش فعال، پیش‌پردازش‌هایی[۱۰] مانند تعبیه نقش‌نگاری[۱۱] یا امضاها بر روی تصویر اعمال می‌شود. با این حال، این کار باعث محدود شدن کاربرد آن‌ها می‌شود [۱]. در صورتی که بتوان اطلاعات ویژه‌ای را از تصویر دیجیتال استخراج کرد، می‌توان تشخیص داد که تصویر دستکاری شده است. همچنین دستکاری غیرفعال با تجزیه و تحلیل تصویر خام بر اساس آمار و معنی‌های مختلف محتوای تصویر تشخیص داده می‌شود [۱].

---

۱. Semantic Meaning
۲. Manipulation
۳. Splicing
۴. Content-preserving
۵. Content-changing
۶. Contrast Enhancement
۷. Copy-move
۸. Active
۹. Passive
۱۰. Pre-processing
۱۱. Watermark



شکل ۱-۳: طبقه‌بندی رویکردهای جعل تصویر

تأیید صحت یا دستکاری در یک تصویر معین بدون هیچ‌گونه اطلاعات قبلی یا هر نوع تعبیه نقش‌نگاری[۱] به‌عنوان تشخیص جعلی منفعل[۲]شناخته شده است [۱۵, ۱۶]. در تشخیص جعل فعال[۳] نیاز به کدهای امنیتی تعبیه شده یا امضا در زمان ایجاد تصویر وجود دارد [۱۷, ۱۸]. تکنیک‌های شناسایی جعل فعال بر اساس استراتژی‌هایی[۴]مانند ته نقش‌نگاری دیجیتال[۵]و امضای دیجیتال دوربین استفاده شده است [۱۹, ۲۰]. مهم‌ترین اشکال در تکنیک‌های فعال این است که آن‌ها به نوع خاصی از دوربین دیجیتال احتیاج دارند [۲۱].

۹. اختصاص ابزارهای جرم‌شناسی به قالب تصویر خاص و روش دستکاری خاص: در تشخیص تصاویر جعلی دیجیتال، تشخیص حضور تصاویر دستکاری شده از اهمیت قابل توجهی برخوردار است. مشکل اکثر مقالات این است که ویژگی‌های خاصی از تصاویر دستکاری شده برمبنای یک روش دستکاری خاص را (مانند کپی-انتقال[۶] چسباندن[۷]و غیره) شناسایی کرده‌اند. این بدان معنی است که این روش‌ها در مقابل روش‌های مختلف دستکاری قابل اعتماد نیست. علاوه بر این، از نظر محلی‌سازی[۸]ناحیه دستکاری‌شده، بیشتر کارها فقط به دلیل بهره‌برداری از آثار فشرده‌سازی مضاعف[۹] تصاویر JPEG را هدف قرار داده‌اند. با این حال، در واقعیت، ابزارهای جرم‌شناسی دیجیتال نباید به هر قالب تصویری اختصاص داشته باشد و همچنین باید مکانی از تصویری که اصلاح شده است محلی‌سازی شود [۱۲].

۱۰. تشخیص تصاویر جعلی به روش کور: به‌طور کلی روش‌های کور[۱۰]در تشخیص تصاویر جعلی، برای تأیید صحت داده‌های چندرسانه‌ای از اثرانگشت‌های آماری[۱۱]و بدون دسترسی به منبع اصلی استفاده می‌کنند. یعنی این روش‌ها مبتنی بر روش خاصی از جعل یا مدل خاصی از دوربین نیستند و ویژگی‌های

۱. Watermark Embedded
۲. Passive Forgery Detection
۳. Active Forgery Detection
۴. Strategies
۵. Digital Watermarking
۶. Copy-Move
۷. Splicing
۸. Localize
۹. Double Compression
۱۰: Blind
۱۱: Statistical Fingerprints

کلی آماری تصاویر را لحاظ می‌کنند. با این حال چنین اثر انگشت‌های غیرقابل تصوری ممکن است با دستکاری‌های مختلف از بین بروند [۲۲].

۱۱. **شناسایی مدل دوربین:** حل مشکل شناسایی مدل دوربین می‌تواند به یک متخصص تحلیل و ارزیابی موارد غیرقانونی (به‌عنوان مثال، صحنه‌های عمل تروریستی و غیره) کمک کند. با شناسایی مدل دوربین تصویر یا نرم‌افزار ویرایشگر تصویر می‌توان تصاویر جعلی را شناسایی کرد [۲۳, ۲۴].

به‌طور کلی چالش‌های انواع روش‌های تشخیص جعل تصویر بیان شد. در روش احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند فقط با چالش‌های شش و ده مواجه نیستیم. در این تحقیق، به کمک روش احراز هویت تصاویر JPEG با اطلاعات سرآیند، چالش‌های یک، سه، چهار و یازده را مرتفع ساختیم.

۱-۵ اهداف تحقیق

در این رساله قصد داریم که ابتدا با توجه به اطلاعات کاربردی در سرآیند تصویر JPEG، نوع نرم‌افزار ویرایشگر یا مدل دوربین را شناسایی کنیم و سپس با توجه به دیگر اطلاعات موجود در سرآیند نیز نرم‌افزار ویرایشگر و مدل دوربین را شناسایی کنیم و سپس اطلاعات استخراج شده را باهم تطبیق دهیم و تا حد امکان تغییرات در سرآیند را شناسایی کنیم.

تصاویر JPEG می‌توانند از ساختارهای مختلفی برای فشرده‌سازی و کدینگ استفاده نمایند. در سرآیند فایل JPEG یک قطعه وجود دارد که ساختار فشرده‌سازی و کدینگ را مشخص می‌کند. ۱۵ ساختار مختلف برای فشرده‌سازی تصویر به فرمت JPEG وجود دارد که کاربران غالبا تنها از دو ساختار اول آن برای فشرده‌سازی استفاده می‌کنند. متداول‌ترین فایل JPEG از فشرده‌سازی Baseline DCT و کدینگ هافمن استفاده می‌کند و بعد از آن فشرده‌سازی Extended DCT و کدینگ هافمن رواج دارد. با بررسی‌های انجام گرفته بیشتر فایل‌های JPEG موجود در فضای مجازی از فشرده‌ساز نوع اول بهره گرفته‌اند. از این‌رو در این رساله، احراز هویت تصاویر JPEG با فشرده‌سازی نوع اول بررسی خواهد شد. قطعه‌ی شاخص آغاز فریم (SOF0) مربوط به فایل JPEG نوع اول، با FFC0 شروع می‌شود و اگر در فایل JPEG از قطعه شاخص آغاز فریم با شاخص آغازین FFC1، FFC2، FFC3، FFC5، FFC6، FFC7، FFC8، FFC9، FFCA، FFCB، FFCD، FFCE، FFCF استفاده شود، نشان از این دارد که فایل JPEG مربوطه از روش‌های دیگر فشرده‌سازی استفاده نموده است و به‌عنوان فایل JPEG غیرمتداول معرفی می‌شود و بررسی جعل در مورد آن انجام نمی‌شود [۸].

۱-۶ سوالات و فرضیه‌ها

سوالات و فرضیه‌های این پژوهش عبارتند از:

- آیا تصویر JPEG نسبت به نسخه اصلی خود تغییر کرده است؟
- یک تصویر دیجیتالی معتبر است یا تغییر کرده است؟

- آیا می‌توان تصاویر دیجیتالی را به دستگاه خرید یا کلاس دستگاه‌های خرید خود پیوند داد؟
- آیا تصویر استفاده شده توسط کامپیوتر تولید شده است یا توسط دوربین گرفته شده است؟
- کدام یک از دوربین‌ها با کدام مدل تصویر را اخذ کرده‌اند؟

۱-۷ دلایل ضرورت تحقیق

همان‌طور که دانلود[۱] کپی، جعل و توزیع مجدد تصاویر دیجیتال در طول سال‌ها ساده‌تر می‌شود، تایید صحت تصویر نیز از اهمیت ویژه‌ای برخوردار است [۲۵]. در واقع تشخیص جعل تصویر بسیار دشوار شده است، زیرا تصاویر دستکاری شده اغلب از دید واقعی قابل تشخیص نیستند. با افزایش تعداد تصاویر دستکاری شده، تشخیص دستکاری تصاویر برای جلوگیری از ارائه اطلاعات گمراه‌کننده به بینندگان بسیار مهم است [۱۳]. در جرم‌شناسی دیجیتال، با توجه به ارائه اطلاعات برجسته در تصاویر و فیلم‌ها، تشخیص دستکاری تصاویر از اهمیت قابل توجهی برخوردار است [۲۶]. در عصر دیجیتال، حجم عظیمی از تصاویر جعلی در زمینه‌های رسانه‌های اجتماعی مانند فیس‌بوک[۲] یا فلیکر[۳] وجود دارد. توزیع تصاویر دستکاری شده می‌تواند بسیار آسان به اشتراک گذاشته شود و می‌تواند برای گمراه کردن بینندگان از حقیقت استفاده شود [۱۲]. تصاویر دیجیتالی به‌طور معمول به‌عنوان شواهد به دادگاه قانون معرفی می‌شوند. بنابراین، تأیید صحت تصاویر دیجیتال بسیار مهم و حیاتی است [۱۰، ۲۷]. از این‌رو، ارائه ابزارهای تحلیل تصویر و ارائه نتیجه به تحلیلگران اجرای قانون در شناسایی فعالیت‌های غیرقانونی، به‌شدت احساس می‌شود.

۱-۸ نوآوری‌ها

به‌طور کلی، نوآوری‌ها در این رساله به شرح زیر است:

۱) تهیه دادگانی ارزشمند از تصاویر JPEG با دوربین‌های متنوع.
۲) استخراج و تهیه دادگان جداول کوانتیزاسیون، کدینگ هافمن و دادگان کاربردی برای هر مدل دوربین.
۳) داده‌کاوی بر روی دادگان تهیه شده و تشخیص موارد پر کاربرد و موارد کم کاربرد در سرآیند.
۴) استخراج دقیق اطلاعات سرآیند تصویر JPEG با استفاده از چندین نرم‌افزار.
۵) بررسی اطلاعات جداول کوانتیزاسیون و کدینگ هافمن برای هر تصویر و تعیین مدل دوربین بر مبنای دادگان.
۶) بررسی اطلاعات دادگان کاربردی نرم‌افزاری و تعیین نرم‌افزار و تشخیص مغایرت‌ها در سرآیند

---

۱. Download
۲. Facebook
۳. Flickr

تصویر.

۹-۱ ساختار پایان‌نامه

در ادامه این رساله، در فصل دوم به سوابق کارهای مرتبط با تحقیق پرداخته شده و معایب و مزایای هر یک از آن‌ها بیان شده است. در فصل سوم به معرفی مفاهیم پایه و کاربردی احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند پرداخته شده است. همچنین در این فصل تاریخچه و فرآیند فشرده‌سازی تصاویر JPEG بازگویی شده است. به‌طور کلی در این فصل پس از بیان مفاهیم مرتبط با آشنایی سرآیند تصاویر JPEG، به بررسی اطلاعات دادگان کاربردی، انواع ماتریس‌های چندی‌سازی و جداول کدینگ هافمن و غیره پرداخته شده است. در فصل چهارم به معرفی روش پیشنهادی پرداخته شده است. در این فصل، برای تفکیک تصاویر اصلی از تصاویر حاصل از نرم‌افزارهای ویرایشگر تصویر، ویژگی‌های مناسبی ارائه شده است. با توجه به ویژگی‌های استخراج شده از تصاویر به دسته‌بندی آن‌ها پرداخته شده است. همچنین در این فصل روش پیشنهادی همراه با دادگان مورد استفاده بررسی شده و به معرفی ابزار مورد استفاده برای پیاده‌سازی پرداخته شده است. در فصل پنجم ارزیابی نتایج بررسی شده و نتایج حاصل از این تحقیق مورد واکاوی قرار گرفته است تا بهترین الگوریتم با بالاترین دقت مورد تایید قرار گیرد. در مرحله‌ی آزمون، تصاویری که در بخش آموزش نبوده‌اند را معیار قرار داده و به دسته‌بندی منبع این تصاویر پرداخته شده است. در نهایت در فصل ششم به نتیجه‌گیری و ارائه‌ی پیشنهادهایی برای کارهای آینده پرداخته شده است.

فصل ۲ : کارهای پیشین

۲-۱ مقدمه

در سال‌های اخیر جرم‌شناسی تصویر تلاش می‌کند صداقت و اصالت تصاویر دیجیتالی مورد استفاده در سیستم‌های اطلاعاتی و اجرای قانون را پیدا کند. شناسایی دوربین‌های مورد استفاده در ضبط تصاویر در کاربردهایی از جمله تشخیص جعل تصویر ضروری است [۳]. استاندارد JPEG پرمخاطب‌ترین قالب تصویری است که توسط دوربین‌های دیجیتال به کار رفته است [۱۰]. یک روش ساده برای شناسایی منبع تصویر در صورت وجود یک فرمت (به‌عنوان مثال JPEG و TIFF)، استفاده از اطلاعات EXIF در سرآیند تصویر است که شامل اطلاعات متنی در مورد نوع دوربین دیجیتالی و شرایطی (تاریخ و زمان، و غیره.) که در آن عکس گرفته شده است. در تصاویر JPEG، اطلاعات اضافی درباره منبع را می‌توان از جدول کوانتیزاسیون در سرآیند JPEG جمع‌آوری کرد [۲۸]. برای شناسایی نواحی دستکاری شده از مصنوعات باقیمانده از فشرده‌سازی‌های JPEG متعدد بهره‌برداری شده است [۲۹، ۳۰، ۳۱، ۳۲، ۳۳، ۳۴، ۳۵]. با این حال، این تکنیک‌ها فقط در قالب‌های JPEG قابل اجرا هستند [۱۲]. تعدادی چارچوب تشخیص جعل تصاویر در طول سال‌ها پیشنهاد شده است که تعدادی از آن‌ها راه‌حل‌های قابل توجهی را ارائه داده‌اند.

در ادامه این فصل به شرح روش‌های تشخیص تصویر جعلی و برخی پژوهش‌های انجام شده مرتبط با روش‌های تشخیص تصویر جعلی را به‌صورت اجمالی مورد بررسی قرار خواهیم داد. در جداول انتهای فصل برخی روش‌ها شرح داده شده در پژوهش‌ها مقایسه می‌شوند و در بخش آخر به جمع‌بندی خلاصه‌ای از مطالب گفته شده در این فصل خواهیم پرداخت.

۲-۲ روش‌های تشخیص دستکاری تصویر

به‌طور کلی، روش‌های تشخیص دستکاری تصویر دو نوع است: فعال [۳۶] و منفعل [۳۵، ۳۶]. در رویکردهای فعال، تصویر دیجیتال مستلزم پیش‌پردازش تصویر مانند تعبیه علامت‌گذاری یا تولید امضا است که کاربرد آن‌ها را در عمل محدود می‌کند. با این حال، روش‌های فعال برای استفاده عملی روزانه مطلوب نیست. تکنیک‌های منفعل به هیچ امضای دیجیتالی نیاز ندارند یا هر علامت مدنظر قرار می‌گیرند. رویکردهای منفعل که جمع‌آوری شواهد دستکاری از تصاویر خود را دارند، پتانسیل بالاتری برای استفاده عملی و توجه بیشتر در تحقیقات در زمینه پزشکی قانونی دارد. در سال‌های اخیر چندین تکنیک برای تشخیص تصویر منفعل ارائه شده است [۳۷، ۳۸].

۲-۳ تکنیک‌های تشخیص تصویر نامعتبر

تکنیک‌های تشخیص جعلی تصویر منفعل را به‌طور تقریبی می‌توان به پنج دسته تقسیم کرد:

- **روش‌های مبتنی بر پیکسل:**[۱] این روش‌ها به تشخیص ناهنجاری‌های آماری در سطح پیکسل، می‌پردازند.
- **روش‌های مبتنی بر فرمت:**[۲] این روش‌ها همبستگی‌های آماری را که توسط یک برنامه فشرده-سازی با اتلاف خاص انجام می‌شود، استفاده می‌کنند.
- **روش‌های مبتنی بر دوربین:**[۳] این روش‌ها با استفاده از آثار به‌جامانده در تصویر توسط لنز دوربین به تشخیص ناهنجاری می‌پردازند.
- **روش‌های مبتنی بر فیزیک محیطی:**[۴] این روش‌ها به‌طور صریح، مدل‌های مختلف و ناهماهنگی در تعامل سه بعدی بین اشیاء فیزیکی، نور و دوربین را مدل‌سازی و تشخیص می‌دهند.
- **روش‌های مبتنی بر هندسه:**[۵] این روش‌ها اندازه‌گیری اشیاء در جهان و موقعیت خود را نسبت به دوربین تشخیص می‌دهد.

در ادامه، چندین ابزار جرم‌شناسی را در هر یک از این دسته‌ها بررسی می‌کنم.

۱-۳-۲ تکنیک‌های مبتنی بر پیکسل

تکنیک‌های مبتنی بر پیکسل روی پیکسل‌های تصویر دیجیتال تاکید می‌کنند. این تکنیک‌ها به چهار نوع تقسیم می‌شوند که عبارتند از:

- کپی و انتقال[۶]
- نمونه‌برداری مجدد[۷](تغییر اندازه، کشش، چرخش)
- چسباندن[۸]
- آماری[۹]

۱-۱-۳-۲ کپی و انتقال

کپی و انتقال شایع‌ترین نوع جعل تصویر است و به‌عنوان تقلب و نسخه‌برداری شناخته شده است. در کپی- انتقال بخشی از تصویر کپی و در موقعیت دیگر در همان تصویر، جایگذاری می‌گردد. چنین دستکاری‌هایی ممکن است. هیچ نشانه محسوسی از تحریف به‌جا نگذارند که این موضوع، اعتماد به تصاویر دیجیتال را تحت تاثیر قرار می‌دهد. در این روش همبستگی پیکسل‌ها در کل تصویر دیجیتالی مورد بررسی قرار می‌گیرد.

---

۱. Pixel-Based
۲. Format Based
۳. Camera Based
۴. Physics Based
۵. Geometric Based
۶. Cloning
۷. Resampling
۸. Splicing
۹. Statistical

در مرجع [۲۲] برای مقابله با چالش تشخیص فیلترهای میانه[۱]از بلوک‌های تصویر کوچک و فشرده استفاده شده است. یک روش تشخیص فیلتر میانه بر اساس شبکه‌های عصبی درهم‌پیچیده[۲](CNN) با در نظر گرفتن ویژگی‌های فیلتر میانه، پیشنهاد شده است. شبکه CNN ویژگی‌های تصویر را به‌صورت خودکار یاد می‌گیرد. در زمینه تشخیص تصاویر جعلی، استفاده از فیلتر میانه به‌شدت لبه‌های تصویر و بافت‌ها را تحت تأثیر قرار می‌دهد. از طرفی استفاده از مدل‌های معمولی CNN به‌طور مستقیم (یعنی استفاده از پیکسل‌های تصویر خام به‌عنوان ورودی به CNN) منجر به عملکرد ضعیف می‌شود. بنابراین با اضافه کردن یک لایه فیلتر به مدل CNN معمولی تداخل ناشی از وجود لبه‌ها و بافت تصویر را سرکوب کرده‌اند. ارزیابی آزمایش‌ها با بانک اطلاعاتی تصویر مرکب از پنج پایگاه داده عبارتند از BOSSbase، UCID، BOSS RAW، Dresden و NRCS انجام شده است. نتایج نشان می‌دهد که پیشرفت‌های قابل توجهی به‌خصوص در تشخیص جعل برش و چسباندن به دست آورده‌اند.

۲-۱-۳-۲ نمونه‌برداری مجدد (تغییر اندازه، کشش، چرخش)

برای ساخت یک تصویر مرکب، ممکن است برای مطابقت مجبور به تغییر اندازه، کشش و یا چرخش قسمت یا قسمت‌هایی از تصویر، انجام گردد. این فرآیند مستلزم نمونه‌برداری مجدد از تصویر اصلی بر روی یک شبکه نمونه‌برداری جدید است که ارتباطات متناوب دوره‌ای بین پیکسل‌های همسایه را نشان می‌دهد. از آنجا که این همبستگی‌ها به‌طور طبیعی رخ نمی‌دهد، حضور آن‌ها می‌تواند برای شناسایی این دستکاری خاص استفاده شود [۴۱].

در مرجع [۱۱] روشی نوین مبتنی بر شبکه عصبی درهم‌پیچیده برای تشخیص تصاویر جعلی و مدل دوربین ارائه شده است. این روش در برابر نمونه‌برداری مجدد[۳]و فشرده‌سازی JPEG مقاوم است. برای تحقق این هدف، روشی به نام نقشه‌های ویژگی درهم‌پیچیده افزودنی[۴](ACFM) برای ادغام باقیمانده-های غیرخطی سطح پایین[۵]در CNN و استخراج ویژگی باقیمانده سطح پایین پیشنهاد شده است. از این ویژگی‌ها به‌صورت یک نقشه ویژگی‌های واحد استفاده می‌شود. سپس برای تقویت نقشه‌های ویژگی تولید شده، از یک لایه درهم‌پیچیده محدود و از یک استخراج کننده ویژگی باقیمانده غیرخطی[۶]مانند باقیمانده فیلتر میانه[۷](MFR) استفاده می‌شود. این لایه، که در ابتدا برای یادگیری ویژگی‌هایی جهت تشخیص جعل در تصویر ارائه شده است، قادر است به‌طور مشترک محتوای یک تصویر را سرکوب کرده و مجموعه متنوع تطبیقی باقیمانده‌های پیش‌بینی خطی[۸]را در حین آموزش CNN بیاموزد. نقشه ویژگی‌های تولید شده توسط هر دوی این لایه‌ها سپس ادغام می‌شوند و برای استخراج ویژگی‌های

---

۱. Median Filtering
۲. Convolutional Neural Networks (CNNs)
۳. Re-Sampling
۴. Augmented Convolutional Feature Maps (ACFM)
۵. Low-Level Nonlinear Residuals
۶. Nonlinear Residuals
۷. Median Filtering Residual (MFR)
۸. Linear Prediction Residuals

بعدی به لایه‌های درهم‌پیچیده سطح بالاتر منتقل می‌شوند. آزمایش‌ها روی مجموعه تصاویری از پایگاه داده تصویری درسدن[۱] انجام شده است. نتایج تجربی نشان می‌دهد که این روش می‌تواند به‌طور قابل ملاحظه‌ای عملکرد شناسایی مدل دوربین را در نمونه‌برداری مجدد و فشرده‌سازی مجدد تصاویر بهبود بخشد. همچنین CNN مبتنی بر ACFM و CNN مبتنی بر NonACFM بهتر از CNN هستند که فقط از ویژگی‌های MFR استفاده می‌کند. هنگامی که حجم تصاویر (کیفیت) با روش فشرده‌سازی JPEG نصف می‌شود، CNN پیشنهادی مبتنی بر ACFM به‌طور قابل توجهی عملکرد بهتری در شبکه‌های همولوگ[۲] خود دارد که از ویژگی‌های MFR استفاده نمی‌کند.

در مرجع [۴] آثاری را که به دلیل نمونه‌برداری مجدد (یک امضای مهم از تصاویر دستکاری شده) ایجاد شده را در نظر گرفته‌اند. این آثار هنگام ایجاد دستکاری‌های دیجیتال مانند مقیاس‌گذاری، چرخش یا چسباندن متداول است. دو روش برای شناسایی و محلی‌سازی دستکاری‌های تصویر[۳] بر اساس ترکیبی از ویژگی‌های نمونه‌برداری مجدد و یادگیری عمیق[۴] ارائه شده است. در روش اول، تبدیل رادون[۵] از ویژگی‌های نمونه‌برداری مجدد بر روی تکه‌های تصویر روی هم افتاده محاسبه می‌شود. از طبقه‌بندی کننده‌های یادگیری عمیق و یک مدل زمینه تصادفی شرطی گوسین[۶] برای ایجاد نقشه رنگی[۷] استفاده شده است. نواحی دستکاری شده با استفاده از روش تقسیم‌بندی تصادفی واکر[۸] واقع شده‌اند. در روش دوم، ویژگی‌های تغییر شکل مجدد بر روی تکه‌های تصویر همپوشانی محاسبه می‌شود. از یک شبکه مبتنی بر حافظه کوتاه مدت[۹] (LSTM)، برای طبقه‌بندی و محلی‌سازی استفاده می‌شود. عملکرد تشخیص یا محلی‌سازی هر دو روش با هم مقایسه شده است. نتایج تجربی نشان می‌دهد که هر دو روش در تشخیص و محلی‌سازی جعل تصویر دیجیتال مؤثر هستند. که هر دو شبکه عصبی درهم‌پیچیده و شبکه‌های مبتنی بر LSTM در بهره‌برداری از ویژگی‌های مجدد برای شناسایی نواحی آسیب‌دیده مؤثر هستند.

در مرجع [۱۳] یک معماری یکپارچه در راستای هدف محلی‌سازی نواحی دستکاری‌شده[۱۰] در سطح پیکسل[۱۱] برای دستکاری تغییر محتوی تصویر با اطمینان بالا ارائه شده است. در این معماری از یک مدل CNN-LSTM ترکیبی استفاده شده است که به‌طور موثر نواحی دستکاری شده و غیر دستکاری شده را طبقه‌بندی می‌کند. شبکه پیشنهادی از زمینه‌های پذیرش بزرگ‌تر (نقشه‌های مکانی[۱۲] و

---

۱. Dresden
۲. Homologue Networks
۳. Localize Image Manipulations
۴. Deep Learning
۵. Radon Transform
۶. Gaussian Conditional Random
۷. Heatmap
۸. Random Walker Segmentation
۹. Long Short-Term Memory (LSTM)
۱۰. Localize Tampered Region
۱۱. Pixel Level
۱۲. Spatial Maps

همبستگی دامنه فرکانس[۱]برای تحلیل ویژگی‌های تبعیض‌آمیز بین نواحی دستکاری و غیر دستکاری شده با ترکیب کدگذار[۲]و شبکه LSTM بهره می‌برد. یک تصویر به چندین بلوک یا تکه تقسیم می‌شود و سپس ویژگی‌های نمونه‌برداری مجدد از هر بلوک استخراج می‌شوند. از ویژگی‌های نمونه‌برداری مجدد برای ضبط آثار مانند از دست دادن کیفیت JPEG، افزایش نمونه‌برداری[۳]و کاهش نمونه‌برداری،[۴] چرخش و برش استفاده می‌شود. ویژگی‌های نمونه‌برداری مجدد تکه‌ها برای مشاهده انتقال بین تکه‌های دستکاری شده و غیر دستکاری شده در شبکه LSTM گنجانیده شده است. از شبکه LSTM برای یادگیری ارتباط بین بلوک‌های دستکاری شده و غیر دستکاری شده در حوزه فرکانس استفاده می‌شود. از معماری CNN برای طراحی یک شبکه کدگذار[۵]بهره‌برداری شده که نقشه ویژگی‌های مکانی اشیاء دستکاری شده را فراهم می‌کند. سرانجام، از شبکه کدگشا[۶]به‌منظور یادگیری نقشه‌برداری از نقشه‌های ویژگی‌های کدگذاری شده با وضوح پایین[۷]تا پیش‌بینی روش مبتنی بر پیکسل با استفاده از ماسک دودویی[۸]پیش‌بینی شده توسط لایه نهایی (softmax) برای محلی‌سازی در سطح پیکسل و تقسیم نواحی دستکاری شده از موارد غیر دستکاری شده بهره‌برداری می‌شود. علاوه بر این، یک مجموعه داده ترکیبی جدیدی ارائه شده است که شامل تعداد زیادی از تصاویر است. این مجموعه داده می‌تواند برای جامعه جرم‌شناسی رسانه[۹]مفید باشد. روش پیشنهادی قادر به محلی‌سازی دستکاری‌های تصویر در سطح پیکسل با دقت بالا است. در این روش تشخیص انواع مختلفی از دستکاری‌ها از جمله کپی و انتقال،[۱۰]حذف شی و چسباندن به‌صورت مؤثر انجام شده است. از طریق آزمایش دقیق بر روی سه مجموعه داده متنوع نشان داده شده است.

۳-۱-۳-۲ چسباندن

تکنیک‌های چسباندن تصویر به‌طور قابل توجهی تصویر اصلی را تغییر می‌دهند و شامل ترکیب بیش از یک تصویر می‌شوند که برای ایجاد یک تصویر دستکاری شده ترکیب شده‌اند. اگر دو تصویر با پس زمینه‌های مختلف به یکدیگر متصل شوند، بنابراین مرزها قابل تشخیص نیستند. کشف چسباندن در تصاویر، یک مشکل چالش برانگیز است که به‌موجب آن مناطق پیوستگی روش‌های مختلفی مورد بررسی قرار می‌گیرند. حضور لبه‌های تیز (یا تغییرات) بین مناطق مختلف و محیط اطراف آن‌ها سرنخ‌های ارزشمندی است که باعث می‌شود در تصویر، مورد تحقیق قرار گیرند. روش‌های تشخیص چسباندن و ادغام تصاویر را می‌توان تقریبا به دو دسته تقسیم کرد، شناسایی دستکاری مبتنی بر ناحیه و مبتنی بر

---

۱. Frequency Domain Correlation
۲. Encoder
۳. Upsampling
۴. Downsampling
۵. Encoder Network
۶. Decoder Network
۷. Low-Resolution
۸. Binary Mask
۹. Media Forensics Community
۱۰: Copy-Move

مرز. روش‌های مبتنی بر مرز، تغییرات نامنظم در مرزهای چسبانده شده را تشخیص می‌دهند. در روش‌های مبتنی بر ناحیه، سازگاری در مدل نسبی تصویر، بررسی می‌شود که در صورت تشخیص غیر کور، از تصویر اصلی و دستکاری شده برای شناسایی جعل، تخمین زده می‌شود [۶].

در مرجع [۴۲] از RX_myKarve به‌عنوان یک چارچوب بازسازی[۱]فایل جدید برای حل تعدادی از مشکلات بازیابی[۲]در تشخیص تصاویر جعلی از جمله حل مشکلات پیچیده تکه‌تکه شدن[۳]در ناحیه اسکن فایل‌های JPEG ارائه شده است. در این چارچوب برای بازیابی و تجمع مجدد[۴]فایل‌های JPEG، از طراحی اساسی RX_myKarve شامل ترکیبی از دو روش بازسازی مبتنی بر ساختار[۵]و بازسازی مبتنی بر محتوا[۶]استفاده می‌شود. در اجزای اصلی شناسایی اعتبار و تجمع مجدد، الگوریتم‌های یادگیری ماشین[۷]و الگوریتم‌های تکاملی[۸]اتخاذ می‌شوند. در تکنیک‌های شناسایی و اعتبار سنجی از یک ماشین یادگیری افراطی[۹]برای طبقه‌بندی خوشه‌های فایل تصاویرJPEG، شناسایی و فیلتر کردن داده‌های تصویر در ناحیه اسکن استفاده شده است. این طبقه‌بندی دقت بازسازی و زمان مرحله تجمع مجدد را بهبود می‌بخشد. تکنیک تجمع مجدد شامل یک الگوریتم ژنتیک[۱۰]برای بازسازی داده‌ها از قطعات تکه‌تکه شده به یک تصویر کامل است. نتایج نشان می‌دهد که چارچوب RX_myKarve قادر به بازسازی موارد مختلفی از تصاویر تکه‌تکه شده JPEG را با دقت بالا و قادر بازسازی عکس‌های کوچک که از تغییر شکل‌های پیچیده رنج می‌برند و بازیابی کامل تمام موارد در مجموعه داده DFRWS-2006 و DFRWS-2007 است.

در مرجع [۱۲] روش یادگیری عمیق برای یادگیری ویژگی‌های سلسله مراتبی[۱۱]دو مرحله‌ای به‌منظور شناسایی نواحی دستکاری شده تصاویر در قالب‌های مختلف تصویر ارائه شده است. در مرحله اول، از یک مدل خود کدگذار پشته‌ای[۱۲]برای یادگیری ویژگی‌های پیچیده هر تکه به‌طور اختصاصی برای توصیف نواحی دستکاری شده استفاده می‌شود. در مرحله دوم، برای تشخیص دقیق‌تر اطلاعات متنی هر تکه یکپارچه می‌شود. مزیت این روش این است که قابل استفاده در هر دو قالب تصویر JPEG و TIFF نیز هست. نتایج آزمایش نشان می‌دهد که روش پیشنهادی نواحی دستکاری شده را با دقت کلی ۹۱,۰۹٪ تشخیص می‌دهد.

در مرجع [۲۶] به توصیف فرآیند و توسعه چارچوبی سریع کارآمد و به‌راحتی قابل استفاده پرداخته شده است. این چارچوب برای ادغام Tensorflow Google با Apache Tika یک بستر ساده را فراهم

---

۱. Carving
۲. Recovery
۳. Fragmentation
۴. Reassembling
۵. Structure-Based
۶. Content-Based
۷. Machine learning
۸. Evolutionary
۹. Extreme Learning Machine (ELM)
۱۰. Genetic Algorithm
۱۱. Hierarchy Feature Learning
۱۲. Stacked Auto-Encoders (SAE)

می‌کند. این چارچوب استخراج محتوای متنی و غنی را ترکیب، سپس می‌تواند از طریق رابطهای جستجو و تجسم در معرض دید قرار گیرد. همچنین توانایی تحلیلگران را برای کشف محتوا جامع و متنوع موجود در تبلیغات اسلحه بهبود می‌بخشد. مدل ImageNet v3 یا Inception را با چارچوب Apache Tika ادغام کردند. هدف از انجام این کار طبقه‌بندی و تحلیل خودکار و کارآمد تشخیص تصاویر جعلی برای شناسایی فروش غیرقانونی سلاح‌های خودکار[۱] و سایر اشیاء خطرناک در وب است. این کار بر روی جرم‌شناسی ابر اطلاعات تصویر[۲] به‌عنوان جایگزینی برای تحلیل مبتنی بر پیکسل تصویر و تشخیص و شناسایی شیء متمرکز شده است. ارزیابی کیفی و کمی تکنیک‌های ادغام نشان می‌دهد که طبقه‌بندی و تشخیص تصاویر جعلی خودکار، در مقیاس بزرگ و قابل اعتماد تصویر می‌تواند به‌طور گسترده‌ای برای پاسخ به سؤالات مربوط به حوزه خاص مورد استفاده قرار گیرد و به‌صورت عمده تحلیل و بررسی شود. همچنین نتایج طبقه‌بندی تصویر خود را با توجه به پردازش خودکار مجموعه داده تصویر سلاح‌های Memex با استفاده از ادغام REST API ارزیابی کردند.

۴-۱-۳-۲ آماری[۳]

تصاویر دارای خواص آماری هستند. مدل آماری برای تشخیص همه نوع دستکاری‌های تصویری اولیه مانند، تغییر اندازه و فیلتر کردن، عکاسی از تصاویر کامپیوتری و شناسایی پیام‌های مخفی (نهان‌نگاری[۴]) استفاده می‌شود. به‌طور مثال از خواص آماری مثل واریانس محلی و یا میانگین محلی برای کشف جعل می‌توان استفاده نمود.

در مرجع [۱] برای تشخیص جعلی که از ناسازگاری‌های غیرقابل تشخیص[۵] در رنگ روشنایی تصاویر بهره می‌برد. اطلاعاتی از برآوردگرهای روشنایی[۶] مبتنی بر فیزیک و آماری در نواحی تصویر درج کردند. همچنین به تحلیل و استخراج ویژگی‌های مبتنی بر بافت، لبه و مقدار پیکسل از برآوردهای روشنایی پرداختند. سپس مقدارهای این ویژگی‌ها را محاسبه کردند و یک روش یادگیری ماشین برای تصمیم-گیری خودکار با این ویژگی‌ها ارائه دادند. طبقه‌بندی کننده ماشین بردار پشتیبان[۷] (SVM) آموزش داده شده، که از الگوی نویز ویژگی‌های آماری برای طبقه‌بندی بلوک‌های کوچک‌تر یک تصویر استفاده شود. با استفاده از طبقه‌بندی متافیوژن[۸] SVM عملکرد امیدوار کننده‌ای برای طبقه‌بندی به دست آوردند.

---

۱. Automatic Weapons
۲. Image Metadata Forensics
۳. Statistical
۴. Steganography
۵. Subtle Inconsistencies
۶. Illuminant Estimators
۷. Support Vector Machine (SVM)
۸. Meta-Fusion

۲-۳-۲ تکنیک‌های مبتنی بر فرمت

تکنیک‌های مبتنی بر فرمت، نوع دیگری از تکنیک‌های تشخیص جعل تصویر است. این‌ها بر اساس فرمت‌های تصویری هستند و عمدتا در فرمت JPEG کار می‌کنند. اگر تصویر فشرده شده باشد، تشخیص جعل بسیار دشوار است اما این تکنیک‌ها می‌توانند جعل را در تصویر فشرده، شناسایی کنند.

این تکنیک‌ها را می‌توان به سه نوع تقسیم کرد.

- تکنیک‌های چندی‌سازی JPEG[۱]
- تکنیک‌های JPEG مضاعف[۲]
- تکنیک‌های مسدود کردن JPEG[۳]

۲-۳-۲-۱ JPEG مضاعف

در مرجع [۲۷] برای تهیه یکپارچگی تصویر از روش مقایسه مقادیر هش[۴]استفاده شده است. برخی از اطلاعات دادگان کاربردی EXIF مانند: نام شرکت سازنده دوربین، مدل دوربین، اطلاعات تصویر بندانگشتی، درجه بزرگنمایی، موقعیت مکانی[۵] تاریخ و ساعت را از سرآیند تصاویرJPEG استخراج کردند. با مقایسه این اطلاعات با تصویر اصلی، تصاویر دستکاری شده، تشخیص داده شده‌اند. با استفاده از تکنیک نهان‌نگاری LSB[۶] هرگونه پیام پنهان در تصاویر، تشخیص داده شده‌اند.

در مرجع [۴۳] روشی ساده و کارآمد برای شناسایی منبع تصویر توسط اطلاعات دادگان کاربردی ذخیره شده در تصویر ارائه شده است. این روش در دو مرحله انجام می‌شود. مرحله اول مقدار هش IMEI (هویت بین‌المللی تجهیزات تلفن همراه[۷]) دستگاه را در دادگان کاربردی JPEG ذخیره می‌کند. مرحله دوم بررسی اطلاعات دادگان کاربردی است، دستگاه IMEI در دادگان کاربردی تصویر ذخیره شده است. پس از استخراج IMEI از دستگاه، از الگوریتم SHA برای هش IMEI استفاده کردند. از این‌رو هر تصویر دارای یک شناسه یکتا برای شناسایی منبع تصویر است.

۲-۳-۲-۲ چندی‌سازی JPEG

در مرجع [۴۴] یک مطالعه در مقیاس بزرگ از اطلاعات سرآیند تصاویر JPEG از تلفن‌های هوشمند اپل[۸]انجام شده است. تا تأثیر این پیشرفت در امکان انجام شناسایی منبع تصویر را بررسی کنند. هدف

---

۱. Quantization
۲. Double
۳. Blocking
۴. Hash
۵. Global Positioning System (GPS)
۶. Steganography
۷. International Mobile Equipment Identity (IMEI)
۸. Apple

پیوند یک تصویر به ساخت یک مدل دوربین خاص یا یک نرم‌افزار خاص از اطلاعات سرآیند تصاویر JPEG است. برای انجام این کار از یک روش یادگیری ماشین استفاده کردند. طبقه‌بندی نسخه سیستم-عامل تلفن‌های هوشمند را با یک جنگل تصادفی انجام می‌شود. همه ماتریس‌های چندی‌سازی که برای یک برنامه خاص یافت می‌شود را جمع‌آوری و بر اساس فرکانس نسبی مرتب کردند. سپس ماتریس چندی‌سازی مرتبط با پارامتر نام نرم‌افزار در اطلاعات دادگان کاربردی EXIF تصاویر را در همان ماتریس‌های چندی‌سازی جستجو کردند. بدین‌صورت توانستند از ماتریس‌های چندی‌سازی برای اثر انگشت استفاده کنند. تحلیل‌ها نشان می‌دهد که توسط اطلاعات دادگان کاربردی EXIF، و پارامترهای به کار رفته در الگوریتم کدگذاری JPEG، منبع معتبر تصویر را به‌صورت خودکار و سریع قابل تشخیص است. ارتباط یک تصویر با نسخه خاص از پشته نرم‌افزار[۱] مورد استفاده را می‌توان از اطلاعات سرآیند تصاویر JPEG یافت. از اطلاعات سرآیند تصاویر JPEG برای شناسایی موفقیت‌آمیز تصویر یک دوربین استفاده می‌شود. با توجه به تنوع بسته‌های نرم‌افزاری، طبقه‌بندی و شناسایی سخت‌افزار تلفن‌های هوشمند بسیار سخت‌تر از دوربین‌های سنتی است. با این حال، شناسایی پشته نرم‌افزار، به‌ویژه نسخه سیستم‌عامل و برنامه‌های انتخابی، به‌خوبی امکان‌پذیر است. محیط نرم‌افزاری غنی و پویا در تلفن‌های هوشمند امکان تنوع بسیار بیشتری از تنظیمات خاص دستگاه در اطلاعات سرآیند فراهم می‌کند. نسخه سیستم‌عامل به‌ویژه تأثیرگذار است، اما اغلب اوقات برنامه‌های خاصی نیز استفاده می‌شود و چندین برنامه خاص یا نسخه سیستم‌عامل باقابلیت اطمینان بالا قابل تشخیص است. تعداد ورودی‌های ابر اطلاعات EXIF[۲] یک ویژگی کاملاً قوی برای اثر انگشت[۳] است. مجموعه داده‌های جمع‌آوری شده از وب سایت فلیکر[۴] ارائه شده است. این مجموعه داده، ابتدا می‌نمایاند که اطلاعات دادگان کاربردی EXIF از تلفن‌های هوشمند باگذشت زمان در دستگاه‌های اپل تغییر می‌کند. این تغییر کمتر به سخت‌افزار اپل مرتبط است، اما بیشتر با تغییر نسخه در سیستم‌عامل آیفون[۵] و IOS ارتباط دارد. به‌عنوان ویژگی فقط از تعداد ورودی‌های ابر اطلاعات EXIF و مقدار ماتریس‌های چندی‌سازی JPEG، در آزمایش‌ها برای طبقه‌بندی خودکار تعیین منبع تصویر استفاده کردند. بررسی را در دو خانواده از ویژگی‌ها انجام شده است. تعداد ورودی‌های ابر اطلاعات EXIF مانند IFD0، IFD1، EXIFIFD و GPS موجود در راهنمای فایل تصویر[۶] (IFD)، ماتریس‌های چندی‌سازی JPEG و همچنین جداول کدینگ هافمن مورد بررسی قرار گرفت. اما در جداول کدینگ هافمن نشانگر اثر انگشت دیده نشد. نتایج نشان می‌دهد که در مجموعه داده جمع‌آوری‌شده جداول کدینگ هافمن در اکثر تصاویر مشابه هم هستند، به همین دلیل جداول کدینگ هافمن را در نظر نگرفتند.

---

۱. Software Stack
۲. Image Metadata
۳. Fingerprint
۴. Flickr
۵. IPhone
۶. Image File Directory (IFD)

در مرجع [۱۰] امضای[۱]متمایز دوربین را از جدول کوانتیزاسیون[۲]و کدینگ هافمن[۳]به همراه سایر داده‌ها از سرآیند تصویر JPEG استخراج کردند. توانستند از این امضا برای تأیید اعتبار تصاویر استفاده کنند. در این روش چندین ویژگی از اطلاعات سرآیند تصاویر JPEG را که قبلاً در نظر گرفته نشده بود را در نظر گرفتند. سه مؤلفه اول امضای دوربین ابعاد تصویر، جدول کوانتیزاسیون و کدینگ هافمن را از تصویر با وضوح کامل و تصویر بندانگشتی استخراج کردند. با شمارش تعداد ورودی‌های موجود در هر یک از این پنج راهنمای فایل تصویر نمایشی متراکم[۴]از انتخاب ابر اطلاعات EXIF تصویر استخراج کردند. بنابراین ۲۸۴ مقدار را از سرآیند تصویر با وضوح کامل، ۲۸۴ مقدار مشابه از سرآیند تصویر بندانگشتی و هشت مورد دیگر از اطلاعات دادگان کاربردی EXIF، به‌طور کلی ۵۷۶ مقدار استخراج کردند. این ۵۷۶ مقدار امضایی را به وجود می‌آورد که توسط آن‌ها هویت تصویر تایید می‌شود. همچنین امضا، ساخت و مدل دوربین را از اطلاعات دادگان کاربردی EXIF استخراج کردند و با امضاهای تصویر معتبر استخراج شده از همان ساخت و مدل دوربین مقایسه کردند. برای ارزیابی آزمایش‌ها از بانک اطلاعاتی فلیکر استفاده کرده‌اند. تمایز پارامترهای مورد استفاده فشرده‌سازی JPEG را در میان دوربین-ها از ساخت و مدل دوربین‌های مختلف تحت تنظیمات مختلف و وضوح کیفیت نسبت به نرم‌افزار ویرایش عکس را تعیین کردند. تعداد مقادیر یکتا برای هر ویژگی را مشخص کردند که شمارش EXIF یکتاترین است. پس از آن ابعاد تصویر، مولفه خاکستری جدول کوانتیزاسیون تصویر سپس مولفه خاکستری جدول کوانتیزاسیون تصاویر بندانگشتی، جداول کدینگ هافمن و ابعاد تصویر بندانگشتی از حداقل تمایز برخوردار هستند. در نهایت امضای نسخه‌های مختلف فتوشاپ از هر یک از ۹,۱۶۳ تنظیمات دوربین برای تعیین ویژگی متمایز آن‌ها مقایسه کردند. در این حالت، فقط از جدول‌های کوانتیزاسیون تصویر و تصویر بندانگشتی و کدینگ هافمن برای مقایسه استفاده کردند. هیچ همپوشانی بین هر نسخه یا کیفیت فتوشاپ و سازنده دوربین مشاهده نشد. این بدان معنی است که هرگونه ویرایش عکس با فتوشاپ به‌راحتی و بدون ابهام قابل شناسایی است. اما این روش در برابر عکس‌برداری مجدد با دوربین اصلی از عکس جعل شده که اطلاعات سرآیند را بازسازی می‌کند، آسیب‌پذیر است.

۳-۲-۳-۲ مسدود کردن JPEG

در مرجع [۴۵]، از یک طرح مبتنی بر ژنتیک برای تأیید صحت تصویر و تصحیح دستکاری برای نهان‌نگاری شکننده[۵]استفاده شده است. در این روش، همبستگی بین ضرایب مهم DCT و آستانه‌های که توسط کاربر تعریف شده، پیام تأیید صحت تصویر را تشکیل می‌دهند. در این روش، الگوریتم ژنتیک برای یافتن موقعیت مطلوب جاسازی داده‌های تأیید اعتبار به کار رفته است.

---

۱. Signature

۲. Quantization Table

۳. Huffman Coding

۴. Compact Representation

۵. Fragile Watermarking

۲-۳-۳ تکنیک‌های مبتنی بر دوربین

هر زمان که ما یک تصویر را از یک دوربین دیجیتال ضبط کنیم، تصویر از حسگر دوربین به حافظه منتقل می‌شود و تحت یک سری از مراحل پردازش قرار می‌گیرد، از جمله کوانتیزاسیون، همبستگی رنگ، اصلاح گاما، متعادل‌سازی سفید، و فشرده‌سازی JPEG. این مراحل پردازش، از گرفتن عکس تا ذخیره تصویر در حافظه ممکن است بر اساس مدل دوربین و مصنوعات دوربین متفاوت باشد. این تکنیک‌ها بر این اصل کار می‌کنند. این تکنیک‌ها را می‌توان به دو دسته اصلی تقسیم کرد:

- آرایه فیلتر رنگ[۱]
- حسگر نویز[۲]

۲-۳-۳-۱ آرایه فیلتر رنگ

در مرجع [۳] با توجه به اینکه شناسایی دوربین‌های مورد استفاده در ضبط[۳]تصاویر در کاربردهایی از جمله تشخیص جعل تصویر ضروری است. روشی برای شناسایی دوربین منبع بر اساس مجموعه‌ای از بهترین ویژگی‌های تصویر با استفاده از روش یادگیری با ناظر[۴]و طبقه‌بندی با استفاده از ماشین بردار پشتیبان ارائه شده است. ۵۰ ویژگی تصاویر دیجیتال را بر اساس ویژگی‌های رنگی، خصوصیات بافت[۵]، خصوصیات آماری تصویر شناسایی و با استفاده از شش روش مختلف استخراج شده و به دو سطح جهانی و محلی طبقه‌بندی کرده‌اند. نتایج تایید شده نشان می‌دهد که این ویژگی‌ها برای انجام تحلیل تصویر بهترین هستند.

۲-۳-۳-۲ حسگر نویز

در مرجع [۲] روش‌هایی برای تمایز بین تصویری که با استفاده از دوربین دیجیتال، رایانه و اسکنر تولید شده است، ارائه شده است. تفاوت مبتنی بر فرآیندهای تولید تصویر که در این دستگاه‌ها مورد استفاده قرار گرفته، مستقل از محتوای تصویر است. با استفاده از ویژگی‌های الگوی نویز باقیمانده[۶]موجود در تصاویر دیجیتال برای طبقه‌بندی بر اساس منابع تصاویر با ماشین بردار پشتیبان دقت بالایی در آزمایش‌ها به دست آمده است. اثربخشی این روش همچنین بر روی تصاویر فشرده شده JPEG، آزمایش شده است.

در مرجع [۴۶] از مفهوم تحلیل مؤلفه‌های اصلی[۷](PCA) حذف نویز در کارهای شناسایی دوربین منبع

---

۱. Color Filter Array (CFA)

۲. Sensor Noise

۳. Capturing

۴. Supervised Learning

۵. Texture Properties

۶. Residual Pattern Noise

۷. Principal Component Analysis (PCA)

استفاده کرده‌اند. بر اساس این مفهوم، چارچوبی مؤثر برای حذف نویز و فشرده‌سازی الگوی نویز حسگر(SPN) با اندازه کامل ارائه شده است که نماینده الگوی نویز حسگر متراکم را تشکیل می‌دهد. برای افزایش اثر حذف نویز[۲] روشی برای ساخت مجموعه آموزشی معرفی شده است. این روش تأثیر تداخل مصنوعات مختلف را به حداقل می‌رساند و نقش مهمی در یادگیری دستگاه استخراج ویژگی الگوی نویز حسگر دارد که نسبت به نویز ناخواسته مختلف حساس نیست. برای تقویت بیشتر عملکرد شناسایی دوربین منبع، روشی نوین مبتنی بر آنالیز تبعیض‌آمیز خطی[۳]برای استخراج ویژگی‌های متمایزتر از الگوی نویز حسگر اتخاذ شده است. برای ارزیابی، آزمایش‌های گسترده‌ای در پایگاه داده تصویر درسدن انجام شده است. نتایج نشان می‌دهد که چارچوب پیشنهادی می‌تواند به‌عنوان یک روش کارآمد پس پردازش، باعث تقویت عملکرد و کاهش بیشتر هزینه محاسباتی برای شناسایی دوربین منبع شود. هنگامی که فقط منابع متنی در دسترس است، عملکرد بسیار رقابتی در کارهای چالش برانگیز به دست می‌آورد.

در مرجع [۲۸] روشی برای شناسایی و تخصیص یک تصویر به یک دوربین دیجیتال خاص بر اساس ویژگی‌های باقیمانده وابسته به نویز که به تصاویر تحت بررسی متکی است، ارائه شده است. تصاویر با وضوح مختلف قابل تحلیل است. همچنین توانسته‌اند منبع دوربین‌ها را با توجه به روش‌های توصیف مکمل با بهره‌گیری از تمام پتانسیل تکنیک‌های طبقه‌بندی یادگیری ماشین شناسایی کنند. برای اعتبارسنجی مجموعه داده‌ای که همه تصاویر آن با وضوح محلی و فشرده‌سازی JPEG است را با ۲۵ دوربین دیجیتال ایجاد کرده‌اند.

در مرجع [۲۵] الگوریتمی مبتنی بر داده‌ها بر اساس شبکه‌های عصبی درهم‌پیچیده برای حل مسئله شناسایی مدل دوربین ارائه شده است که ویژگی‌های هر مدل دوربین را مشخص می‌کند. CNN پیشنهادی که تنها در مجموعه داده درسدن آموزش دیده است قادر به تعمیم دادن به مدل دوربین‌های ناشناخته است.

۲-۳-۴ تکنیک‌های مبتنی بر فیزیک محیطی

تفاوت‌های نور در یک تصویر را می‌توان، به‌عنوان مدرک دستکاری مورد بررسی قرار داد. این تکنیک‌ها بر اساس محیط روشنایی که تحت آن یک شی یا تصویر گرفته می‌شود، کار می‌کنند. نورپردازی برای گرفتن یک تصویر بسیار مهم است. این تکنیک‌ها در ادامه شرح داده شده‌اند.

در مرجع [۲۱] روشی نوین غیرفعال برای تبعیض بین تصاویر معتبر و جعلی و الگوریتمی کارآمد

---

۱. Sensor Pattern Noise (SPN)

۲. De-Noising

۳. Linear Discriminant Analysis (LDA)

برای تشخیص جعل بر اساس مولفه‌های درخشندگی[۱]تصاویر، آمار هیستوگرام[۲]تصاویر و تبدیل همگن[۳] ارائه شده است. به‌عنوان مراحل پیش‌پردازش برای تقویت جزئیات تصاویر از فیلتر بالا گذر[۴]و همسان-سازی هیستوگرام قبل از شناسایی جعل استفاده شده است. فرآیند تقویت جزئیات می‌تواند به‌دقت طبقه‌بندی بالایی دست یابد. پس از پیش‌پردازش هیستوگرام نورپردازی تخمین زده می‌شود. مقدار نقطه اوج[۵]مشتق هیستوگرام تخمین زده می‌شود و به‌عنوان یک معیار اندازه‌گیری[۶]برای تشخیص جعل استفاده می‌شود. فلسفه این استراتژی این است که در صورت جعل، نواحی جعلی تحت شرایط مختلف نورپردازی قرار می‌گیرند، از این‌رو قادر به انعکاس نور در نقطه‌های اوج هیستوگرام است. روش تخمین آستانه[۷]در این مقاله اتخاذ شده است. برای طبقه‌بندی، توابع چگالی احتمال[۸]از نقطه‌های اوج مشتق هیستوگرام اتخاذ شده است. این الگوریتم نرخ تشخیص جعل خوب را در تصاویر رنگی در مقایسه با پیشرفته‌ترین الگوریتم‌ها به دست می‌آورد. علاوه بر این، پیاده‌سازی بر روی داده‌های واقعی ساده است. این برنامه می‌تواند برای برنامه‌های تشخیص جعل فیلم و برنامه‌های پردازش تصویر در زمان واقعی گسترش یابد.

۲-۳-۵ تکنیک‌های مبتنی بر هندسه

تکنیک‌های مبتنی بر هندسه، اندازه‌گیری اشیاء در جهان و موقعیت آن‌ها نسبت به دوربین را اندازه‌گیری می‌کنند. تکنیک‌های تقلبی تصویر مبتنی بر هندسه در ادامه شرح داده شده‌اند.

۲-۳-۵-۱ نقطه اصلی

در تصاویر معتبر نقطه اصلی[۹](نمایش مرکز دوربین بر روی صفحه تصویر) در نزدیکی مرکز تصویر قرار دارد. هنگامی که یک فرد یا یک شیء در تصویر قرار می‌گیرد، نقطه اصلی به‌طور نسبی حرکت می‌کند. بنابراین، ناسازگاری در نقطه اصلی تصویر، می‌تواند به‌عنوان شواهد دستکاری استفاده شود [۶].

در مرجع [۴۷] روشی برای شناسایی مدل دوربین بر اساس یادگیری عمیق و شبکه‌های عصبی درهم‌پیچیده، ارزیابی و ارائه شده است. با تنظیم مدل AlexNet یک شبکه کوچک را امتحان کرده‌اند. با این وجود این شبکه کوچک نسبت به بزرگ‌ترین مدل GoogleNet کمی کمتر از یک درصد تا سه

---

۱. Illumination Components
۲. Histograms
۳. Homomorphic Transform
۴. High-Pass Filtering
۵. Peak
۶. Metric
۷. Thresholding estimation
۸. Probability Density Functions (PDFs)
۹. Principal Point

درصد کارآمد است. برای ارزیابی آزمایش‌ها از بانک اطلاعاتی درسدن و شش مدل دوربین شخصی استفاده کرده‌اند. نتایج متفاوتی را با دو فیلتر پردازش متفاوت، نقش مهمی را که پیش‌پردازش در دقت طبقه‌بندی کلی بازی می‌کند را نشان داده شده است.

۲-۴ مقایسه روش‌های تشخیص جعلی تصویر منفعل

تا اینجا به بررسی برخی از روش‌های تشخیص جعل تصاویر پرداخته شد و تعدادی از روش‌های تشخیص جعلی تصویر منفعل و برخی پژوهش‌های انجام شده و روش‌های موجود در هر زمینه به‌صورت اجمالی مورد بررسی قرار گرفتند. در جداول ۲-۱و ۲-۲و ۲-۳و ۲-۴ و ۲-۵ برخی روش‌های شرح داده شده در پژوهش‌های بیان شده به‌طور خلاصه مقایسه می‌شود.

جدول ۲-۱: مقایسه روش‌های مبتنی بر پیکسل در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر پیکسل			
عنوان تحقیق	**هدف اصلی تحقیق**	**مزایا و معایب**	**ردیف**
جرم‌شناسی فیلتر میانه بر اساس شبکه‌های عصبی درهم‌پیچیده [۲۲]	از شبکه CNN برای یادگیری خودکار ویژگی-های تصویر استفاده شده است. برای مقابله با چالش تشخیص فیلترهای میانه از بلوک‌های تصویر کوچک و فشرده استفاده شده است. یک روش تشخیص فیلتر میانه بر اساس شبکه‌های عصبی درهم‌پیچیده (CNN) با در نظر گرفتن ویژگی‌های فیلتر میانه، پیشنهاد شده است.	**نکات قوت**: جعل‌های برش خورده را به‌خوبی شناسایی می‌کند.	۱
نقشه‌های ویژگی‌های برجسته درهم‌پیچیده برای شناسایی مدل دوربین مبتنی بر CNN قدرتمند [۱۱]	روشی برای تشخیص تصاویر جعلی و مدل دوربین ارائه شده است.	**نکات قوت:** در برابر نمونه‌برداری مجدد و فشرده‌سازی JPEG مقاوم است.	۲
کشف و محلی‌سازی جعل تصویر با استفاده از ویژگی-های تغییر شکل مجدد و یادگیری عمیق [۴]	دو روش برای شناسایی نواحی آسیب‌دیده و محلی‌سازی دستکاری‌های تصویر ارائه شده است.		۳
معماری ترکیبی LSTM و کدگذار، کدگشایی برای کشف جعل تصویر [۱۳]	یک معماری برای طبقه‌بندی نواحی دستکاری-شده از موارد غیر دستکاری در تصویر ارائه شده است.	**نکات قوت**: قادر به محلی‌سازی دستکاری‌های تصویر در سطح پیکسل با دقت بالا است. در این روش تشخیص انواع مختلفی از دستکاری‌ها از جمله کپی و انتقال، حذف شی و چسباندن به‌صورت مؤثر انجام شده است.	۴

ادامه جدول

تکنیک‌های مبتنی بر پیکسل			
عنوان تحقیق	هدف اصلی تحقیق	مزایا و معایب	ردیف
چارچوب بازسازی RX_myKarve برای تجمع مجدد قطعات پیچیده تصاویر JPEG [۴۲]	بازسازی داده‌ها از قطعات تکه‌تکه شده (آسیب-دیده یا حذف شده) به یک تصویر کامل است.	**نکات قوت:** چارچوب RX_myKarve قادر به بازیابی موارد مختلفی از تصاویر تکه‌تکه شده JPEG با دقت بالا و قادر بازیابی عکس‌های کوچک که از تغییر شکل‌های پیچیده رنج می-برند و بازیابی کامل تمام موارد در مجموعه داده DFRWS-2006 و DFRWS-2007 است.	۵
ناحیه تشخیص جعل تصویر: یک رویکرد یادگیری عمیق [۱۲]	روش یادگیری عمیق برای یادگیری ویژگی‌ها به‌منظور شناسایی تصاویر دستکاری شده در قالب‌های مختلف تصویر ارائه شده است.	**مزیت:** مزیت این روش این است که قابل استفاده در هر دو قالب تصویر JPEG و TIFF نیز هست. نواحی دستکاری شده با دقت کلی ۰۹. ٪۹۱ شناسایی شده است.	۶
روشی برای جرم‌شناسی تصویر در مقیاس خودکار و بزرگ [۲۶]	طبقه‌بندی و تحلیل خودکار و تشخیص تصاویر جعلی برای شناسایی فروش غیرقانونی سلاح-های خودکار و سایر اشیاء خطرناک در وب است.		۷
بررسی انواع جعل تصویر و تشخیص آن‌ها [۱]	برای تشخیص جعل از ناسازگاری‌های غیرقابل تشخیص در رنگ روشنایی تصاویر استفاده شده است.	**مزیت:** با استفاده از طبقه‌بندی متافیوژنSVM عملکرد امیدوار کننده‌ای برای طبقه‌بندی حاصل شده است.	۸

جدول ۲-۲: مقایسه روش‌های مبتنی بر فیزیک محیطی در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر فیزیک محیطی			
عنوان تحقیق	هدف اصلی تحقیق	مزایا و معایب	ردیف
اجرای کارآمد روش‌های پیش‌پردازش برای تشخیص جعل تصویر [۲۱]	روشی نوین غیرفعال برای تبعیض بین تصاویر معتبر و جعلی و الگوریتمی کارآمد برای تشخیص جعل بر اساس مولفه‌های درخشندگی تصاویر، آمار هیستوگرام تصاویر و تبدیل همگن ارائه شده است.		۱

جدول ۲-۳: مقایسه روش‌های مبتنی بر هندسه در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر هندسه			
عنوان تحقیق	**هدف اصلی تحقیق**	**مزایا و معایب**	**ردیف**
شناسایی مدل دوربین با استفاده از شبکه‌های عصبی درهم‌پیچیده عمیق [۴۷]	شناسایی مدل دوربین بر اساس یادگیری عمیق و شبکه‌های عصبی درهم‌پیچیده که به‌طور خودکار و هم‌زمان ویژگی‌ها را استخراج می‌کند و طی فرآیند یادگیری طبقه‌بندی می‌کند.		۱

جدول ۲-۴: مقایسه روش‌های مبتنی بر فرمت در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر فرمت			
عنوان تحقیق	**هدف اصلی تحقیق**	**مزایا و معایب**	**ردیف**
احراز هویت دیجیتالی شده برای جرم‌شناسی تصویر [۲۷]	روشی برای شناسایی تصاویر دستکاری شده و هرگونه پیام پنهان در تصاویر ارائه شده است.		۱
تأیید اعتبار تصویر با استفاده از سرآیندهای JPEG [۴۳]	روشی برای شناسایی منبع تصویر و تعیین تغییر تصویر توسط نرم‌افزار ویرایشگر تصویر ارائه شده است.		۲
تأیید اعتبار تصویر دیجیتال از سرآیندهای JPEG [۱۰]	استفاده از فرمت JPEG به صورت‌های مختلف برای تایید اعتبار تصاویر که از نسخه اصلی خود تغییر کرده‌اند. تشخیص تصویری که در نرم‌افزار ویرایشگر عکس مورد تغییر قرار گرفته است.	**معایب:** در برابر حمله دوباره پخش استاندارد که در آن یک تصویر دیجیتال دستکاری، چاپ و عکس‌برداری مجدد می‌شود، آسیب-پذیر است. **نکات قوت**: هرگونه ویرایش عکس با فتوشاپ به‌راحتی و بدون ابهام قابل شناسایی است.	۳
شناسایی منبع جرم-شناسی با استفاده از سرآیند تصاویر JPEG: در مورد تلفن‌های هوشمند [۴۴]	یک مطالعه در مقیاس بزرگ از اطلاعات سرآیند تصاویر JPEG از تلفن‌های هوشمند اپل انجام شده است. تا تأثیر این پیشرفت در امکان انجام شناسایی منبع تصویر را بررسی کنند. هدف پیوند یک تصویر به ساخت یک مدل دوربین خاص یا یک نرم‌افزار خاص از اطلاعات سرآیند تصاویر JPEG است.	**نکات قوت:** چندین برنامه خاص یا نسخه سیستم‌عامل باقابلیت اطمینان بالا قابل تشخیص است.	۴
بررسی ته نقش‌نگاری شکننده برای تأیید صحت تصویر [۴۵]	روشی برای تأیید صحت تصویر و تصحیح دستکاری ارائه شده است.		۵

جدول ۲-۵: مقایسه روش‌های مبتنی بر دوربین در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر دوربین			
عنوان تحقیق	**هدف اصلی تحقیق**	**مزایا و معایب**	**ردیف**
شناسایی دوربین منبع با استفاده از ویژگی‌های تصویر [۳]	روشی برای شناسایی دوربین منبع بر اساس مجموعه‌ای از بهترین ویژگی‌های تصویر با استفاده از روش یادگیری با ناظر و طبقه‌بندی با استفاده از ماشین بردار پشتیبان ارائه شده است.	**نقاط قوت:** با توجه به اینکه ویژگی‌ها برای همه تصاویر مشترک است. از این‌رو استخراج ویژگی نسبت به سایر رویکردها عملکرد منطقی خوبی دارد.	۱
روش‌های قانونی برای طبقه‌بندی تصاویر تولید شده با اسکنر، کامپیوتر و دوربین دیجیتال [۲]	روش‌هایی برای تمایز بین تصویری که با استفاده از دوربین دیجیتال، رایانه و اسکنر تولید شده ، ارائه شده است.	**نقاط ضعف:** کلید دستیابی به نتایج دقیق انتخاب ویژگی‌های مناسب است.	۲
استنتاج ارائه به هم پیوسته اثر انگشت حسگر برای شناسایی دوربین منبع [۴۶]	از مفهوم تحلیل مؤلفه‌های اصلی (PCA) حذف نویز در کارهای شناسایی دوربین منبع استفاده کرده‌اند. بر اساس این مفهوم، چارچوبی مؤثر برای حذف نویز و فشرده‌سازی الگوی نویز حسگر (SPN) با اندازه کامل ارائه شده است.	**نقاط ضعف:** برای حفظ دقت شناسایی نیاز به انجام فرآیند آموزش مجدد با دوربین‌های جدید دارد. **نقاط قوت:** روشی کارآمد پس پردازش برای شناسایی منبع دوربین، تقویت عملکرد حذف نویز ناخواسته و کاهش هزینه محاسباتی در مرحله تطابق است.	۳
تخصیص منبع باز مجموعه عکاسی [۲۸]	روشی برای شناسایی و تخصیص یک تصویر به یک دوربین دیجیتال خاص بر اساس ویژگی-های باقیمانده وابسته به نویز که به تصاویر تحت بررسی متکی است، ارائه شده است.		۴
اولین گام به‌سوی شناسایی مدل دوربین با شبکه عصبی درهم‌پیچیده [۲۵]	شناسایی مدل دوربین با یادگیری ویژگی‌هایی از مشخصه تصاویری که با دوربین‌های مختلف به‌طور مستقیم از تصاویر گرفته شده‌اند، به‌جای اعمال هر مدل یا ویژگی دستورالعمل‌های دست ساز، به کار برده می‌شود.	**نقاط قوت:** یادگیری استخراج ویژگی را در مجموعه‌ای از مدل‌های دوربین دیده نشده را به‌خوبی تعمیم می‌دهد.	۵

۲-۵ جمع‌بندی

اشاره شد که روش‌های مبتنی بر فرمت در برابر حمله پخش دوباره استاندارد که در آن یک تصویر دیجیتالی دستکاری، چاپ و عکس‌برداری مجدد می‌شود، آسیب‌پذیر هستند. مشکل اکثر مقالات این است که ویژگی‌های خاصی را در تصاویر دستکاری شده با یک روش دستکاری خاص (مانند کپی-انتقال، چسباندن و غیره) شناسایی می‌کنند. یعنی هر یک از روش‌ها در مقابل روش‌های مختلف دستکاری قابل اعتماد نیستند.

در مرجع [۱۰] فقط از تصویر و جدول‌های کوانتیزاسیون تصویر بندانگشتی و کدینگ هافمن استفاده شده است. ما در روش پیشنهادی، سعی کردیم با افزودن پارامترهای جدید، تکنیک را بهبود ببخشیم. اما در مرجع [۴۴] تأثیر در پیشرفت به‌روزرسانی نرم‌افزار تلفن‌های هوشمند اپل در امکان انجام شناسایی

منبع با ارتباط یک تصویر به یک مدل خاص، ساخت یا یک نرم‌افزار خاص اطلاعات سرآیند JPEG، انجام شد که بررسی را در دو ویژگی، تعداد ورودی‌های موجود در راهنمای فایل تصویر و جداول چندی‌سازی JPEG، انجام شده که با استفاده اطلاعات سرآیند تصویر JPEG ارتباط یک تصویر با نسخه خاص از پشته نرم‌افزار مورد استفاده، چندین برنامه خاص یا نسخه سیستم‌عامل باقابلیت اطمینان بالا قابل تشخیص است. ما سعی کردیم مدل دوربین موجود در هر نوع سخت‌افزار را شناسایی کنیم.

در این فصل، به شرح و بررسی کارهای گذشته در حیطه جعل تصویر با روش‌های تشخیص جعلی تصویر منفعل انجام شده پرداختیم. برخی روش‌های شرح داده شده در پژوهش‌های بیان شده به‌طور خلاصه مقایسه و نتیجه‌گیری شد. در فصل بعدی به تعاریف و مفاهیم مورد نیاز در این رساله می‌پردازیم.

فصل ۳ : تعاریف و مفاهیم بنیادی

۳-۱ مقدمه

فشرده‌سازی تصویر و ویدئو موضوع بسیاری از تحقیقات انجام شده است. این شاخه از علم در حال حاضر به مرحله بلوغ خود رسیده است و گواه این امر نیز استفاده‌های وسیعی است که از فشرده‌سازی تصویر و ویدئو در زمینه‌های مختلف ارتباطات می‌شود. استانداردهای فشرده‌سازی نقش بسیار مهمی در رشد و توسعه روش‌های فشرده‌سازی ایفا نموده‌اند. استانداردهای جدیدی که برای فشرده‌سازی تصویر و ویدئو ارائه شده است شامل پیشرفته‌ترین روش‌های فشرده‌سازی می‌باشند. سوالی که در حال حاضر در تحقیقات مربوط به فشرده‌سازی تصویر و ویدئو مطرح می‌باشد این است که آیا می‌توان روشی جدید ارائه نمود که کارآیی آن روش نسبت به کارآیی روش‌های فشرده‌سازی قبلی تفاوت قابل ملاحظه‌ای نماید. به نظر می‌رسد بهبود قابل ملاحظه‌ای در تکنیک‌های فشرده‌سازی در آینده نزدیک رخ نخواهد داد. بنابراین روش‌های جدیدی در فشرده‌سازی را می‌توان ارائه نمود که برای کاربردهای جدید فشرده-سازی مناسب باشند. مهم‌ترین کاربردهای فشرده‌سازی در آینده نزدیک، کاربردهای ناشی از به‌کارگیری انتقال اطلاعات در سیستم‌های چند رسانه‌ای[۱] موبایل و یا شبکه‌های بیسیم می‌باشند.

در این فصل ساختار و استاندارد یک JPEG استاندارد معرفی می‌شود و اجزاء مختلف آن مورد مطالعه قرار می‌گیرد.

۳-۲ فشرده‌سازی JPEG

وقتی در مورد واژه JPEG[۲]صحبت می‌شود، عموما به استاندارد و روش پیاده‌سازی آن توجه داریم، در حالی که این عبارت به یک گروه بزرگ تحقیقاتی اطلاق می‌شود. این گروه از سال ۱۹۸۶ تاکنون، استانداردهای متعددی را به وجود آورده است و با همکاری سایر گروه‌ها نظیر شرکت ISO (که فعالیت خود را از سال ۱۹۸۳ آغاز کرده بود)، یک سری فعالیت‌های مشترک انجام می‌دهد. عبارت Joint در آغاز کلمه JPEG نیز حاکی از همین همکاری متقابل است [۴۸].

نام رسمی استانداردی که اغلب تحت عنوان JPG (یا JPEG) از آن یاد می‌شود، عبارت است از ISO/IEC IS 10918-1 ITU-T Recommendation T.81 این استاندارد در واقع شامل چهار بخش است:

- **بخش اول:** استاندارد اولیه و پایه JPEG که بسیاری از گزینه‌ها[۳]و موارد جایگزین[۴]برای کدینگ تصاویر (به‌خصوص باهدف حفظ تصاویر عکاسی طبیعی) را تعریف می‌کند.
- **بخش دوم:** نتایج و آزمایش‌های لازم را برای نرم‌افزار مطمئنی بر اساس بخش اول، تنظیم و ارائه می‌کند.

---

۱. Multimedia

۲. Joint Photographic Experts Group (JPEG)

۳. Options

۴. Alternatives

- **بخش سوم:** تنظیمات لازم را برای افزودن یک سری پسوندها[1]به‌منظور بهبود و ارتقاء استاندارد فراهم می‌کند (مانند فرمت SPIFF).
- **بخش چهارم:** روش‌های ثبت[2]برخی پارامترها برای گسترش[3]JPEG را تعریف می‌کند.

پس از تولید و تعریف استاندارد، لازم است از آن در دنیای واقعی استفاده شود و بنابراین ارائه یک فرمت برای چنین فایل‌هایی مورد نیاز است. فرمت اولیه فایل نخستین بار توسط شخصی به نام اریک همیلتون[4] ساخته و به‌صورت یک مبدل JPEG در میکرو سیستم‌های C-Cube قرار گرفته و با نام JFIF در دسترس عموم گذاشته شد [۹]. شاید مهم‌ترین گام در راه استفاده گسترده از JPEG توسط شخصی به نام تام‌لین[5](در گروه IJG) انجام شد که نرم‌افزار کد باز او به شکل موفقیت آمیزی در نرم‌افزارهای ویرایش تصویر و در مرورگرهای اینترنتی مورد استفاده قرار گرفت. پس از تولید استاندارد طی مراحل فوق، گروه JPEG بسیاری از نواقص و نارسائی‌های آن را رفع کرده و استاندارد اصلاح شده JPEG-LS Standard- ISO/IEC IS 14495-1 | ITU-T Recommendation T.87 را ارائه نمود؛ از جمله آنکه گروه بر آن شد تا امکان کدینگ بدون خطا را نیز در JPEG فراهم آورد. در این حالت برخلاف روش معمول در JPEG از ضرایب DCT بلوک‌های تصویر و روش فشرده‌سازی توأم با خطا استفاده نمی‌شود. در حقیقت این کار با توجه به نیاز کاربران، به‌خصوص کاربران تصاویر پزشکی که از بروز خطای ناشی از فشرده‌سازی توأم با خطا ناراضی بودند، انجام شد. روش جدید سعی دارد به شکلی بدون خطا (یا تقریباً بدون خطا) تصویر رنگی یا سیاه و سفید را فشرده و ذخیره کند. انتخاب روش مناسب، بر اساس تحقیقات گسترده‌ای انجام و نهایتاً از الگوریتم LOCO (حاصل کار پژوهشکدهٔ HP) استفاده شد [۵۰، ۴۹]. مطرح شدن این بحث‌ها منجر به تعریف استاندارد جدیدی تحت عنوان JPEG2000 گردید که البته خارج از حوزهٔ مستقیم مباحث مربوط به فشرده‌سازی بدون خطای JPEG (JPEG-LS) معرفی شده است.

از آنجا که ضرایب DCT بلوک‌های تصویر، تا حد زیادی می‌توانند ویژگی‌های بصری آن را حفظ کنند، ذخیره‌سازی به روش JPEG معمولی (و نه JPEG2000) به استخراج ضرایب DCT از تصویر روی آورده شده است (لازم به توضیح است که در فرمت JPEG2000 به‌جای ضرایب DCT، ضرایب ویولت از تصویر استخراج می‌شوند.).

۳-۳ مراحل فشرده‌سازی JPEG

مراحل فشرده‌سازی به روش JPEG در شکل ۳-۱ نشان داده شده است. به‌طور کلی مراحل فشرده‌سازی به روش JPEG معمولی عبارت است از:

تبدیل تصویر به بلوک‌های ۸×۸

---

۱. Extension
۲. Registering
۳. Extend
۴. Eric Hamilton
۵. Tom Lane

تبدیل مدل رنگی تصویر از RGB به YCbCr در رابطه (۳-۱) آمده است.

$$\begin{aligned} Y &= 0.299\,R + 0.587\,G + 0.114\,B \\ Cb &= -0.1687\,R - 0.3313\,G + 0.5\,B + 128 \\ Cr &= 0.5\,R - 0.4187\,G - 0.0813\,B + 128 \end{aligned} \qquad (۳-۱)$$

نمونه‌برداری از مولفه‌های رنگ: چشم انسان به مولفه‌های رنگی در قیاس با مولفه خاکستری حساسیت کمتری دارد. از این‌رو، در فرآیند انکدینگ JPEG تمام پیکسل‌های خاکستری لحاظ می‌شوند. اما از پیکسل‌های رنگ خاکستری و قرمز نمونه‌برداری می‌شود.

مراحل ذخیره‌سازی یک تصویر نمونه به روش JPEG در شکل ۳-۲ نشان داده شده است. در ادامه این مراحل به‌تفصیل شرح داده شده است.

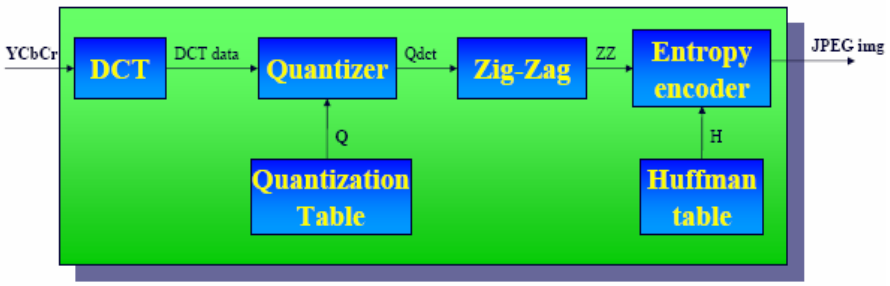
استخراج ضرایب DCT از هر یک از مولفه‌های رنگ در هر بلوک ۸×۸ (۶۴ ضریب هر مولفه، شامل یک ضریب DC و ۶۳ ضریب AC).

کوانتیزه کردن ضرایب بر اساس جدول کوانتیزاسیون (با تقسیم هر ضریب بر ضریب کوانتیزاسیون مربوطه). جدول کوانتیزاسیون معیاری از کیفیت تصویر محسوب می‌شود. باید توجه داشت که همین مرحله کوانتیزاسیون است که باعث می‌شود روش JPEG یک روش توأم با خطا باشد، زیرا بخشی از اطلاعات در حین فرآیند کوانتیزاسیون دور ریخته می‌شود.

ضریب DC قبلی برای تخمین ضریب کوانتیزهٔ فعلی مورد استفاده قرار می‌گیرد و تفاوت آن‌ها کد می‌شود.

در مورد ضرایب AC این کدینگ تفاضلی اتفاق نمی‌افتد و ضرایب به شکل زیگزاگی اسکن شده و در یک دنباله قرار می‌گیرند (از گوشه بالا سمت چپ تا گوشه پایین سمت راست تصویر). چینش زیگزاگی ضرایب باعث می‌شود که ضرایب با فرکانس‌های نزدیک، در کنار یکدیگر قرار بگیرند.

سپس دنباله ضرایب به روش طول گام[۱](RLE) و مبتنی بر آنتروپی[۲]فشرده و کد می‌شود. روش کدینگ می‌تواند به یکی از دو صورت کدینگ هافمن[۳]یا کدینگ حسابی[۴] انجام شود.



شکل ۳-۱: مراحل فشرده‌سازی به روش JPEG

۱. Run Length Encoding (RLE)
۲. Entropy Encoding
۳. Huffman Encoding
۴. Arithmetic Encoding

-415	-30	-61	27	56	-20	-2	0
4	-21	-60	10	13	-7	-8	4
-46	7	77	-24	-28	9	5	-5
-48	12	34	-14	-10	6	1	1
12	-6	-13	-3	-1	1	-2	3
-7	2	2	-5	-2	0	4	1
-1	0	0	-2	0	-3	4	0
0	0	-1	-4	-1	0	0	1

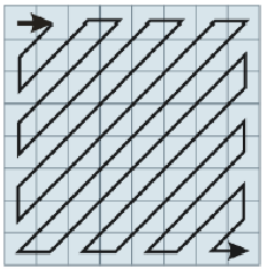
الف) نمونه‌ای از ضرایب DCT یک بلوک ۸×۸ تصویر

16	11	10	16	24	40	51	61
12	12	14	16	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

ب) جدول کوانتیزاسیون

-26	-3	-6	2	2	-1	0	0
0	-2	-4	1	1	0	0	0
-3	1	5	-1	-1	0	0	0
-3	1	2	0	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

ج) ضرایب DCT کوانتیزه شده



د) اسکن زیگزاگی

```
-26,
-3, 0,
-3, -2, -6,
2, -4, 1, -3,
1, 1, 5, 1, 2,
-1, 1, -1, 2, 0, 0,
0, 0, 0, 0, -1, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

ه) ضرایب چیده شده به ترتیب زیگزاگی

شکل ۳-۲: نمایش مراحل ذخیره‌سازی یک تصویر نمونه به روش JPEG

۳-۴ توضیحات کلی راجع به استاندارد JPEG

یک فایل JPEG حاوی اطلاعات فشرده شده تصویر به همراه جدول کوانتیزاسیون مربوط به آن است. در این قسمت یک سری توضیحات کلی راجع به استاندارد JPEG و برخی موارد لازم برای فهم درست و استفاده بهینه از استاندارد معرفی و تشریح می‌شود.

۳-۴-۱ حالت‌های مختلف کدینگ

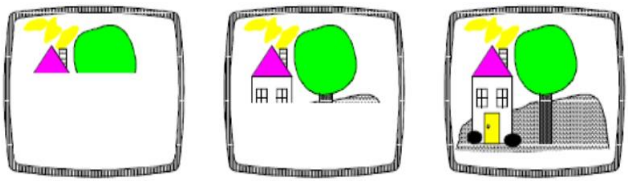
در حالت کلی دو نوع روش برای فرآیندهای انکد و دیکد وجود دارد: توأم با خطا[۱] و بدون خطا[۲]. روش‌هایی که بر تبدیل فوریه گسسته تکیه دارند، توأم با خطا هستند و بنابراین امکان فشرده‌سازی تا حد بالای را فراهم می‌کنند، اما در عین حال از کیفیت تصویر می‌کاهند. ساده‌ترین روش مبتنی بر DCT، فرآیند رشته‌ای (دنباله‌ای) پایه مبتنی بر DCT[۳] است. این روش برای بسیاری از نرم‌افزارها قابل استفاده است و اغلب به‌عنوان حالت پیش‌فرض در نظر گرفته می‌شود. گروه دوم روش‌ها که بدون خطا

۱. Lossy
۲. Lossless
۳. Baseline Sequential Process

هستند، کلاً بر اساس ضرایب DCT نبوده و برای نرم‌افزارهایی که نیاز به فشرده‌سازی بدون خطا دارند، طراحی شده است. به‌طور کلی می‌توان گفت چهار حالت مختلف کدینگ[۱] برای فایل JPEG وجود دارد: حالت رشته‌ای مبتنی بر DCT؛[۲] حالت تصاعدی (جلوسوی) مبتنی بر DCT؛[۳] بدون خطا[۱] و سلسله مراتبی[۲].

۳-۴-۱-۱ کدینگ رشته‌ای مبتنی بر DCT

همان‌طور که در شکل ۳-۳ نشان داده شده، برای این حالت نمونه‌های مربوط به بلوک‌های ۸×۸ به شکل بلوک به بلوک از چپ به راست و به‌صورت ردیف به‌ردیف (از بالا به پائین) در داخل فایل قرار داده می‌شوند. کد کردن ضرایب به این صورت باعث می‌شود هر ضریب بلافاصله بعد از تولید، وارد فرآیند فشرده‌سازی و ذخیره در فایل شود و بنابراین نیازی به ذخیره ضرایب نیست.



شکل ۳-۳: نمایش حالت کدینگ رشته‌ای (دنباله‌ای) مبتنی بر DCT

در جدول ۱-۳ ویژگی‌های مربوط به حالت کدینگ رشته‌ای به شکل خلاصه ارائه می‌شود.

جدول ۳-۱: فرآیند انکدینگ معمولی مبتنی بر DCT

Baseline process (required for all DCT-based decoders)
• DCT-based process • Source image: 8-bit samples within each component • Sequential • Huffman coding: 2 AC and 2 DC tables • Decoders shall process scans with 1, 2, 3, and 4 components • Interleaved and non-interleaved scans

۳-۴-۱-۲ روش‌های مختلف کدینگ مبتنی بر آنتروپی

در استاندارد JPEG امکان استفاده از دو روش فشرده‌سازی مبتنی بر آنتروپی فراهم شده است: روش هافمن و روش کدینگ حسابی. روش کدینگ هافمن از جدول‌های هافمن[۴] استفاده می‌کند. روش حسابی از جدول‌های شرطی مربوط به کدینگ حسابی[۵] استفاده می‌کند. هیچ مقدار پیش‌فرضی برای جدول‌های هافمن در نظر گرفته نشده است، بنابراین هر کاربردی بنا به محیط مناسب برای خود،

---

۱. Modes Of Operation

۲. Sequential DCT Based Process

۳. Progressive DCT Based Process

۴. Huffman tables

۵. Arithmetic Coding Conditioning Tables

جدول‌های مورد نیازش را انتخاب می‌کند. اما برای کدینگ حسابی، جدول‌های پیش‌فرض تعریف شده است.

اگر حالت انکدینگ، حالت دنباله‌ای (رشته‌ای) معمولی باشد، از کدینگ هافمن استفاده می‌شود. در غیر این صورت برای حالت‌های بدون خطا یا حالت تعمیم یافته مبتنی بر DCT می‌توان از روش هافمن و یا از روش کدینگ حسابی استفاده کرد.

۳-۱-۴-۳ دقت هر نمونه[۱]

برای حالت‌های مبتنی بر DCT دو دقت مختلف در نظر گرفته شده است: هشت بیتی یا ۱۲ بیتی نرم‌افزارهایی که نمونه‌هایی با دقت‌های متفاوت را استفاده می‌کنند، می‌توانند با شیفت دادن نمونه‌های هشت و ۱۲ بیتی نمونه‌های تصویر اصلی به میزان لازم، از آن‌ها استفاده کنند. فرآیند کدینگ پایه مبتنی بر DCT (یعنی حالت Baseline) تنها از دقت هشت بیتی استفاده می‌کند. اگر روش پیاده‌سازی شده مبتنی بر DCT باشد و بخواهد حالت ۱۲ بیتی را نیز پشتیبانی کند، نیاز به محاسبات بیشتری دارد. در استاندارد JPEG محاسبات مربوط به حالت‌های هشت و۱۲ بیتی جداگانه بررسی شده‌اند. برای حالت بدون خطا، دقت نمونه‌ها می‌تواند از دو الی ۱۶ بیت باشد.

۳-۴-۲ کوچک‌ترین واحد کد شده (MCU)

یکی از مفاهیم مربوط به حالت کدینگ چند مؤلفه‌ای یکی در میان، مفهوم کوچک‌ترین واحد کد شده (MCU)[۲]است. اگر دادگان فشرده تصویری به‌صورت عادی کد شده باشند (یعنی یکی در میان انتخاب نشده باشند)، MCU به‌صورت یک واحد داده تعریف می‌شود. مفاهیم تصویر فریم و اسکن دادگان تصویری فشرده شده، شامل تنها یک تصویر است. در حالت‌های کدینگ رشته‌ای هر تصویر تنها شامل یک فریم است. هر فریم شامل یک یا چند اسکن است. برای فرآیندهای رشته‌ای، هر اسکن شامل انکدینگ کامل یک یا چند مؤلفه تصویر است.

۳-۴-۳ فرمت‌های فشرده‌سازی JPEG

در یک فایل JPEG ، روش فشرده‌سازی هر چه که باشد (توأم با خطا یا بدون خطا)، و فرآیند کدینگ هر روشی که باشد (رشته‌ای، مرحله به مرحله، بدون خطا یا سلسله مراتبی)، ساختار ذخیره فایل به یک شکل واحد و استاندارد است. در فایل JPEG، بخش‌های مختلف تصویر فشرده شده به کمک مقادیر دو بایتی مخصوصی به نام شاخص[۳]شناسایی می‌شوند. به دنبال برخی از شاخص‌ها رشته‌ای از پارامترها

---

۱. Sample precision

۲. Minimum Coded Unit (MCU)

۳. Marker

می‌آیند؛ به‌عنوان‌مثال در مورد جدول‌ها بخش‌هایی تحت عنوان سرآیند فریم[۱] و یا سرآیند اسکن.[۲] برخی دیگر از شاخص‌ها بدون پارامتر استفاده می‌شوند و برای حالت‌هایی مانند شروع و یا انتهای تصویر به کار می‌روند.

وقتی یک شاخص به همراه دنباله‌ای از پارامترها می‌آید، خود شاخص به همراه پارامترهای آن، یک قطعه شاخص[۳] را تشکیل می‌دهند. دادگان تولید شده توسط انکدر آنتروپی هم قطعه‌بندی می‌شوند و یک شاخص معین تحت عنوان شاخص شروع مجدد[۴] برای جدا کردن قطعات دادگان کد شده مبتنی بر آنتروپی[۵] مورد استفاده قرار می‌گیرد.

به‌طور کلی سه فرمت برای دادگان فشرده وجود دارد:

۱) **فرمت Interchange:** در این فرمت علاوه بر قطعات شاخص و قطعات کد شده مبتنی بر آنتروپی خاصی که معمولا لازم است، این فرمت باید برای تمام جدول‌های مربوط به کوانتیزاسیون و کدینگ آنتروپی نیز شامل تمام قطعات شاخصی باشد که در هنگام دیکدینگ مورد نیاز است. این مسئله تضمین می‌کند که مستقل از آنکه در هر محیط نرم‌افزاری دادگان جدول چگونه به دادگان فشرده تصویر ملحق می‌شوند، تصویر در محیط‌های مختلف قابل دسترسی و استفاده باشد.

۲) **فرمت مخفف شده[۶] برای دادگان فشرده تصویری:** این فرمت شبیه به فرمت Interchange است، با این تفاوت که تمامی جدول‌های لازم برای دیکدینگ را در بر ندارد (ممکن است برخی از آن‌ها را داشته باشد). این فرمت برای استفاده در نرم‌افزارهایی است که مکانیسم‌های جایگزین برای تهیه همه یا بخشی از جدول‌های لازم برای دیکدینگ را در اختیار قرار می‌دهند.

۳) **فرمت مخفف شده برای دادگان مربوط به مشخصات جدول:**[۷] این فرمت تنها شامل دادگان جدول است. این فرمت وسیله‌ای است که به کمک آن نرم‌افزار، جدول‌های مورد نیاز را برای بازسازی یک یا چند تصویر، دیکدر نصب می‌کند.

از نظر ساختاری، فرمت‌های مربوط به دادگان فشرده شامل مجموعه‌ای منظم از پارامترها، شاخص‌ها و قطعات کد شده مبتنی بر آنتروپی می‌شود. پارامترها و شاخص‌ها اغلب در داخل قطعات شاخص سازمان‌دهی می‌شوند. هر یک از این فرمت‌ها اطلاعات را در مجموعه‌ای از بایت‌ها و به ترتیب‌های گوناگون در فایل تصویر ذخیره می‌کنند.

---

۱. Frame Header
۲. Scan Header
۳. Marker Segment
۴. Restart Marker
۵. Entropy Coded Data Segments
۶. Abbreviated Format
۷. Table–Specification data

۳-۴-۴ پارامترها، شاخص‌ها، قطعات شاخص و قطعات کد شده مبتنی بر آنتروپی

همان‌گونه که پیش‌تر نیز اشاره شد، فایل حاوی دادگان فشرده اطلاعات را به ترتیب مشخصی ذخیره می‌کند و برای ساده نمودن فرآیند دیکدینگ، یک سری شاخص برای قسمت‌های مختلف آن در نظر گرفته است. شاخص‌ها معمولا به همراه تعدادی پارامتر ارائه می‌شوند. در این قسمت توضیحات بیشتر راجع به این موضوع ارائه می‌شود.

پارامترها: پارامترها اعداد صحیحی هستند که مقادیر آن‌ها مربوط می‌شود به فرآیند انکدینگ، خواص تصویر اصلی و سایر ویژگی‌هایی که توسط نرم‌افزار قابل انتخاب هستند. پارامترها می‌توانند به‌صورت کدهای چهار بیتی، یک بایتی، یا دو بایتی تخصیص یابند. به غیر از تعدادی از پارامترهای اختیاری، این مقادیر عمدتاً اطلاعات مهمی را در بر دارند که بدون آن‌ها دیکدر قادر به بازسازی تصویر نیست. اختصاص کد به پارامترها معمولاً باید از نوع Unisigned Int و به طول مشخصی (بر حسب بیت) باشد. برای پارامترهایی که دو بایتی هستند (۱۶بیت طول دارند)، باید در دنباله بایت‌هایی که قرار است دادگان فشرده را تشکیل دهند، ابتدا بایت پر ارزش‌تر و سپس بایت کم ارزش‌تر قرار بگیرد. پارامترهایی که چهار بیتی هستند، معمولا به‌صورت جفت می‌آیند و در یک جفت از این‌گونه پارامترها که در داخل یک بایت کد می‌شوند، اولین پارامتر در چهار بیت پر ارزش‌تر بایت قرار می‌گیرد و پارامتر دوم در چهار بیت کم ارزش‌تر آن. به‌طور کلی در هر پارامتر چهار، هشت یا ۱۶ بیتی، ابتدا مقدار MSB و سپس مقدار LSB می‌آید.

شاخص‌ها:[۲] شاخص‌ها برای شناسایی بخش‌های ساختاری گوناگون در فرمت‌های مختلف فشرده‌سازی دادگان مورد استفاده قرار می‌گیرند. بیشتر شاخص‌ها در آغاز قطعات شاخص قرار می‌گیرند که شامل گروهی از پارامترهای مرتبط با آن می‌شوند. در عین حال، برخی از شاخص‌ها به‌تنهایی قرار می‌گیرند. تمامی شاخص‌ها با یک کد دو بایتی مشخص می‌شوند که بایت اول (پرارزش‌تر) آن‌ها (که در دنباله دادگان نیز در ابتدا می‌آید) برابر است با 'X'FF (هگزا دسیمال). بایت دوم بیان می‌کند که شاخص مربوطه، از چه نوعی است. مقدار موجود در بایت دوم هرگز برابر با صفر یا FF نیست. بر همین اساس دیکدر می‌تواند بخش‌های مختلف فایل را بدون نیاز به قطعات دیگر تصویر، تجزیه کند.

در جدول ۳-۲ انواع مختلف شاخص‌ها معرفی شده و علاوه بر نام اختصاری آن‌ها، کد اختصاص یافته به هریک به همراه توضیح مختصری راجع به آن‌ها ارائه شده است. در این جدول، شاخص‌هایی که با علامت * مشخص شده‌اند، به‌تنهایی به کار می‌روند و پارامتری به همراه ندارند.

قطعات شاخص:[۳] هر قطعه شاخص در فایل شامل یک شاخص به همراه تعدادی بایت مرتبط به آن است. اولین پارامتر بعد از هر شاخص (یادآوری می‌شود که هر شاخص یک کد دو بایتی است)، پارامتری

---

۱. Parameters

۲. Markers

۳. Markers Segments

است به طول دو بایت که طول قطعه مورد نظر را مشخص می‌کند. این پارامتر، تعداد بایت‌های موجود در قطعه فعلی را با احتساب خود دو بایت مربوط به پارامتر طول و بدون احتساب دو بایت مربوط به شاخص، معین می‌کند. قطعات شاخص توسط SOFها[۱]و SOSها[۲]شناسایی شده (ر.ک. به جدول ۳-۲) و اصطلاحاً سرآیند[۳]نامیده می‌شوند: به ترتیب سرآیند فریم[۴] و سرآیند اسکن.[۵]

قطعات داده کد شده مبتنی بر آنتروپی:[۶] یک قطعه کد شده مبتنی بر آنتروپی در بردارنده خروجی یک فرآیند کدینگ آنتروپی است. مستقل از اینکه روش کدینگ مبتنی بر آنتروپی، روش هافمن بوده یا روش حسابی، این قطعات حاوی تعداد صحیحی از بایت‌ها هستند. برای اینکه تعداد بایت‌ها، عدد صحیحی شود، در گدینگ هافمن، به تعداد کافی یک بیتی به انتهای دنباله بیت‌ها افزوده می‌شود تا بایت پایانی تکمیل شود. در کدینگ حسابی نیز فرآیندی برای جبران در نظر گرفته می‌شود.

همچنین به‌منظور تضمین عدم وقوع شاخص در میان دادگان کد شده، هنگام فشرده‌سازی ترتیبی داده می‌شود که در صورت تشکیل 'X'FF در دنباله دادگان، به بایت بعدی مقدار خالص صفر اختصاص داده شود تا دیکدر دچار خطا نشود و از آن صرف نظر کند.

۱. Start Of Frame
۲. Start Of Scan
۳. Header
۴. Frame Header
۵. Scan Header
۶. Entropy Coded Data Segment

جدول ۳-۲: انواع شاخص‌های فایل JPEG [۵۱].

کد اختصاص یافته	نماد	توضیحات
شاخص‌های مربوط به آغاز فریم، غیر تفاضلی، کدینگ هافمن		
X’FFC0’	SOF_0	Baseline DCT
X’FFC1’	SOF_1	Extended sequential DCT
X’FFC2’	SOF_2	Progressive DCT
X’FFC3’	SOF_3	Lossless (sequential)
شاخص‌های مربوط به آغاز فریم، تفاضلی، کدینگ هافمن		
X’FFC5’	SOF_5	Differential sequential DCT
X’FFC6’	SOF_6	Differential progressive DCT
X’FFC7’	SOF_7	Differential lossless (sequential)
شاخص‌های مربوط به آغاز فریم، غیر تفاضلی، کدینگ حسابی		
X’FFC8’	JPG	Reserved for JPEG extensions
X’FFC9’	SOF_9	Extended sequential DCT
X’FFCA’	SOF_{10}	Progressive DCT
X’FFCB’	SOF_{11}	Lossless (sequential)
شاخص‌های مربوط به آغاز فریم، تفاضلی، کدینگ حسابی		
X’FFCD’	SOF_{13}	Differential sequential DCT
X’FFCE’	SOF_{14}	Differential progressive DCT
X’FFCF’	SOF_{15}	Differential lossless (sequential)
مشخص کننده جدول هافمن		
X’FFC4’	DHT	Define Huffman table(s)
مشخص کننده جدول شرطی مربوط به کدینگ حسابی		
X’FFCC’	DAC	Define arithmetic coding conditioning(s)
خروج از بازه‌های شروع مجدد		
X’FFD0’ through X’FFD7’	RST_m*	Restart with modulo 8 count “m”
سایر شاخص‌ها		
X’FFD8’	SOI*	Start of image
X’FFD9’	EOI*	End of image
X’FFDA’	SOS	Start of scan
X’FFDB’	DQT	Define quantization table(s)
X’FFDC’	DNL	Define number of lines
X’FFDD’	DRI	Define restart interval
X’FFDE’	DHP	Define hierarchical progression
X’FFDF’	EXP	Expand reference component(s)
X’FFE0’ through X’FFEF’	APP_n	Reserved for application segments
X’FFF0’ through X’FFFD’	JPG_n	Reserved for JPEG extensions
X’FFFE’	COM	Comment
شاخص‌های رزرو شده		
X’FF01’	TEM*	For temporary private use in arithmetic coding
X’FF02’ through X’FFBF’	RES	Reserved

۳-۵ بررسی ترتیب اجزاء اصلی فایل JPEG در حالت‌های کدینگ رشته‌ای

شکل ۳-۴ ترتیب قرار گیری اجزاء سطح بالا و پر اهمیت فایل JPEG را در فرمت Interchange برای تمامی حالت‌های انکدینگ به غیر از کدینگ سلسله مراتبی نشان می‌دهد. در این شکل سه شاخص مشخص شده‌اند که به ترتیب زیر معرفی می‌شوند:

- **SOI:** شاخص آغاز تصویر.[۱] بیانگر آغاز اطلاعات تصویر فشرده در فرمت‌های Interchange و فرمت مخفف (abbreviated).
- **EOI:** شاخص انتهای تصویر.[۲] بیانگر تمام اطلاعات تصویر در فرمت‌های Interchange و مخفف.
- **RST_m:** شاخص شروع مجدد.[۳] این شاخص، یک شاخص اختیاری است که در صورت فعال بودن شروع مجدد، در بین قطعات کد شده آنتروپی قرار می‌گیرد. به‌طور کلی، هشت نوع شاخص شروع مجدد وجود دارد (m=0-7) که برای هر اسکن از صفر شروع می‌شوند و به ترتیب در یک دنباله تکرار می‌شوند تا شمارنده به مضربی از هشت برسد.

سطح اول شکل ۳-۴ نشان می‌دهد که تصویر JPEG ای که فرمتی غیر از ساختار سلسله مراتبی دارد، با یک SOI شروع و با EOI خاتمه می‌یابد و شامل یک فریم است.

سطح دوم شکل ۳-۴ نشان می‌دهد که یک فریم باید با یک سرآیند فریم شروع شود و شامل یک یا چند اسکن باشد. بخش‌های اختیاری مانند جدول‌های انکدینگ یا کوانتیزاسیون و یا برخی قطعات شاخص متفرقه[۴] می‌توانند بعد از سرآیند فریم، قرار بگیرند. اگر قطعه DNL ای موجود باشد، باید بلافاصله بعد از اولین اسکن قرار بگیرد.

برای فرآیندهای کدینگ رشته‌ای مبتنی بر DCT و نیز حالت بدون خطا، هر اسکن باید شامل یک الی چهار مؤلفه تصویری باشد.

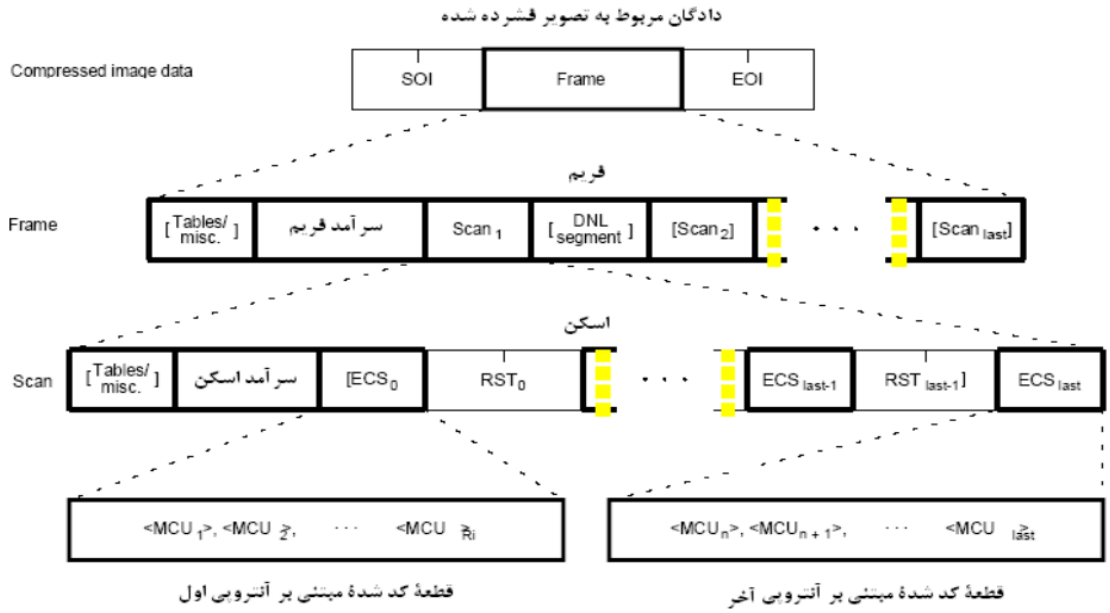
---

۱. Star Of Image Marker

۲. End Of Image Marker

۳. ReStart Marker

۴. Miscellaneous Marker Segments



شکل ۳-۴: توصیف کلی و سرتاسری قسمت‌های مهم فایل JPEG در فرمت Interchange

سطح سوم شکل ۳-۴ بیان می‌دارد که یک اسکن باید با سرآیند اسکن[۱]شروع شود و شامل یک یا چند قطعه کد شده مبتنی بر آنتروپی باشد. در اینجا نیز مشابه با آغاز فریم، ممکن است بعد از سرآیند اسکن، جدول‌های اختیاری و یا برخی قطعات شاخص متفرقه قرار بگیرند. اگر شروع مجدد فعال نشده باشد، تنها یک قطعه کد شده آنتروپی وجود خواهد داشت. اگر شروع مجدد فعال شده باشد، تعداد قطعات کد شده توسط اندازه تصویر و بازه شروع مجدد که از پیش تعریف شده است[۲]معین خواهد شد. در این حالت باید یک شاخص شروع مجدد (RST) پس از هر قطعه کد شده (به غیر از آخرین قطعه) قرار بگیرد.

سطح چهارم شکل ۳-۴ بیان می‌دارد که هر قطعه کد شده مبتنی بر آنتروپی از دنباله‌ای از MCU ها تشکیل شده است. اگر شروع مجدد فعال شده باشد و بازه شروع مجدد تعریف شده نیز برابر با Ri باشد، هر قطعه کد شده (به‌جز قطعه آخر) باید شامل Ri عدد MCU باشد. آخرین قطعه شامل هر تعداد MCU ای می‌شود که اسکن را تکمیل می‌نماید.

در شکل ۳-۴ محل‌هایی را که جدول‌ها می‌توانند قرار بگیرند، مشخص کرده است. از طرف دیگر عنوان کردیم که فرمت Interchange باید شامل تمامی جدول‌های مورد نیاز برای دیکدینگ تصویر فشرده شده باشد بنابراین، این جدول‌ها باید در یک یا چند موقعیت از محل‌های مجاز قرار بگیرند.

۱. Scan Header

۲. Defind Restart Interval (DRI)

۳-۵-۱ سرآیند فریم

در شکل ۳-۵ اجزاء مختلف یک سرآیند فریم که باید در ابتدای یک فریم قرار بگیرد، نمایش داده شده است. این سرآیند ویژگی‌های تصویر اصلی، مؤلفه‌های داخل فریم، فاکتورهای نمونه‌برداری[۱] برای هر مؤلفه و همچنین آدرسی را که از آن جدول‌های کوانتیزه شده باید همراه با هر مؤلفه، مورد استفاده قرار بگیرد را مشخص می‌کند.

در این قسمت، شاخص‌ها و پارامترهای نمایش داده شده در شکل ۳-۵ تعریف می‌شوند. اندازه (بر حسب بیت) و مقادیر مجاز هر پارامتر در جدول ۳-۳ نشان داده شده است.

SOF_n: شاخص آغاز فریم[۲] محل شروع پارامترهای یک فریم را نشان می‌دهد. اندیس n بیان می‌دارد که اولاً فرآیند انکدینگ حالت رشته‌ای معمولی (Baseline) است یا حالت رشته‌ای تعمیم یافته، حالت تصاعدی و یا بدون خطا، و ثانیاً کدام فرآیند انکدینگ مبتنی بر آنتروپی مورد استفاده قرار گرفته است (هافمن یا کدینگ حسابی).

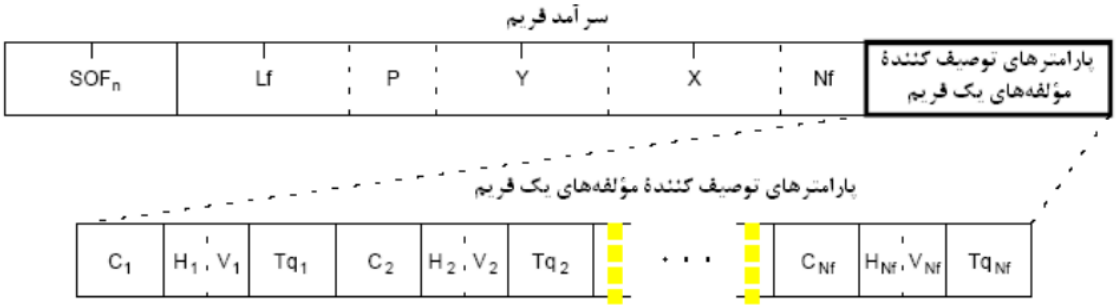
SOF_0: حالت کدینگ رشته‌ای معمولی (Baseline) مبتنی بر DCT (و کدینگ هافمن).

SOF_1: حالت انکدینگ رشته‌ای تعمیم یافته (Extended) مبتنی بر DCT با کدینگ هافمن.

SOF_2: حالت انکدینگ تصاعدی (مرحله به مرحله) مبتنی بر DCT به همراه کدینگ هافمن.

SOF_3: حالت انکدینگ بدون خطا (رشته‌ای) به همراه کدینگ هافمن.

SOF_9: حالت انکدینگ رشته‌ای تعمیم یافته مبتنی بر DCT با روش کدینگ حسابی.



شکل ۳-۵: اجزاء و ترتیب قرارگیری بایت‌ها در داخل سرآیند فریم

SOF_{10}: حالت انکدینگ تصاعدی (مرحله به مرحله) مبتنی بر DCT به همراه کدینگ حسابی.

SOF_{11}: حالت انکدینگ بدون خطا (رشته‌ای) به همراه کدینگ حسابی.

Lf: طول سرآیند فریم[۳] طول قسمت سرآیند فریم را مشخص می‌کند (شکل ۳-۵). لازم به یادآوری است که این طول بدون احتساب خود دو بایت مربوط به سرآیند فریم و با احتساب بایت‌های مربوط به Lf محاسبه می‌شود.

---

۱. Sampling Factors

۲. Start Of Frame Marker

۳. Frame Header Length

P: دقت نمونه[۱] مشخص می‌کند نمونه‌های موجود در مؤلفه‌های داخل یک فریم چه دقتی بر حسب بیت دارند.

Y: تعداد سطرها[۲] مشخص می‌کند ماکزیمم تعداد سطرهای موجود در تصویر اصلی چند است. این مقدار باید با تعداد سطرهای موجود در مؤلفه دارای بیشترین تعداد نمونه‌های عمودی، برابر باشد.

X: تعداد نمونه‌ها در هر سطر (تعداد ستون‌ها). ماکزیمم تعداد نمونه‌های موجود در هر سطر از تصویر اصلی را مشخص می‌کند. این مقدار باید با ماکزیمم تعداد نمونه‌های موجود در هر سطر از مؤلفه‌های تصویر برابر باشد.

Nf: تعداد مؤلفه‌های تصویری موجود در فریم. مشخص می‌کند چه تعداد از مؤلفه‌های تصویر اصلی در فریم هستند. مقدار Nf باید برابر با تعداد مجموعه‌های مؤلفه‌های فریم که در سرآیند فریم قرار دارند، باشد (C_i، H_i، V_i و Tq_i).

C_i: معرف مؤلفه[۳] یک برچسب منحصر به فرد به مؤلفه i ام اختصاص می‌دهد. این مقادیر در بخش سرآیندهای اسکن برای شناسایی مولفه‌ها در داخل اسکن مورد استفاده قرار می‌گیرند. مقدار C_i باید با مقادیر C_1 الی C_{i-1} متفاوت باشد.

H_i: فاکتور نمونه‌برداری افقی[۴] رابطه بین بعد افقی مؤلفه و ماکزیمم ابعاد تصویر X را مشخص می‌کند. همچنین در صورتی که بیش از یک مؤلفه در هر اسکن کد شود، تعداد واحدهای داده افقی موجود در مؤلفه C_i را در هر MCU مشخص می‌کند.

V_i: فاکتور نمونه‌برداری عمودی[۵] رابطه بین بعد عمودی مؤلفه و ماکزیمم ابعاد تصویر Y را مشخص می‌کند. همچنین در صورتی که بیش از یک مؤلفه در هر اسکن کد شود، تعداد واحدهای داده عمودی موجود در مؤلفه C_i را در هر MCU مشخص می‌کند.

Tq_i: انتخاب‌گر آدرس جدول کوانتیزاسیون [۶]. این پارامتر یکی از چهار آدرس ممکن را برای جدول کوانتیزاسیون مشخص می‌کند که در بازسازی ضرایب DCT مربوط به مؤلفه C_i مورد نیاز است. اگر قرار است در فرآیند دیکدینگ، روند عکس کوانتیزاسیون [۷]انجام شود، باید هنگام دیکد کردن اسکن‌های شامل مؤلفه C_i، این جدول در این آدرس نصب شده باشد. تا زمانی که تمام اسکن‌های شامل C_i به پایان نرسیده‌اند، این آدرس نباید دوباره (به متغیر دیگری) تخصیص یابد و یا محتویات آن تغییر کند.

---

۱. Sample Precision

۲. Number Of Line

۳. Component Identifier

۴. Horizontal Sampling Factor

۵. Vertical Sampling Factor

۶. Quantization Table Destination Selector

۷. DeQuantization

جدول ۳-۳: پارامترهای موجود در سرآیند فریم، اندازه هر یک (برحسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (برحسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Lf	۱۶	۸ + ۳ × Nf			
P	۸	۸	۸, ۱۲	۸, ۱۲	۲-۱۶
Y	۱۶	۰ - ۶۵ ۵۳۵			
X	۱۶	۱ - ۶۵ ۵۳۵			
Nf	۸	۱-۲۵۵	۱-۲۵۵	۱-۴	۱-۲۵۵
C_i	۸	۰-۲۵۵			
H_i	۴	۱-۴			
V_i	۴	۱-۴			
Tq_i	۸	۰-۳	۰-۳	۰-۳	۰

۳-۵-۲ سرآیند اسکن

در شکل ۳-۶ اجزاء مختلف یک سرآیند اسکن که باید در ابتدای یک اسکن قرار بگیرد، نمایش داده شده است. این سرآیند مشخص می‌کند کدام مؤلفه‌ها در داخل یک اسکن موجود هستند، آدرس جدول‌هایی که برای کدینگ آنتروپی (در فرآیند دیکد هر مؤلفه) مورد نیاز است کجا هستند، و همچنین در مورد روش تصاعدی مبتنی بر DCT مشخص می‌کند کدام قسمت از ضرایب DCT کوانتیزه شده در داخل اسکن قرار گرفته‌اند. در مورد فرآیندهای انکدینگ بدون خطا، پارامترهای اسکن پیش‌بینی کننده (تخمین گر)[۱] و تبدیل نقطه‌ای[۲] را معین می‌کنند.

توجه: اگر تنها یک مؤلفه در داخل یک اسکن وجود داشته باشد، طبق تعریف آن مؤلفه به شکل معمولی (و نه یکی در میان) کد شده است (یعنی به‌صورت Non-Interleaved). اگر بیش از یک مؤلفه تصویری در هر اسکن موجود باشد، باز طبق تعریف این مؤلفه‌ها یکی در میان در اسکن قرار گرفته‌اند (یعنی به شکل Interleaved) شاخص‌ها و پارامترهای نمایش داده شده در شکل ۳-۶ در ادامه تعریف می‌شوند. همچنین اندازه (بر حسب بیت) و مقادیر مجاز برای هر پارامتر در جدول ۳-۴ نشان داده شده است.

SOS: شاخص آغاز اسکن.[۳] محل شروع پارامترهای اسکن را مشخص می‌کند.

Ls: طول سرآیند اسکن.[۴] طول سرآیند اسکن را مشخص می‌کند (با احتساب خود دو بایت مربوط به Ls و بدون احتساب SOS).

---

۱. Predictor

۲. Point Transform

۳. Start Of Scan Marker

۴. Scan Header Length

Ns: تعداد مؤلفه‌های تصویری داخل یک اسکن. مشخص می‌کند در یک اسکن، چه تعداد از مؤلفه‌های تصویر اصلی قرار دارند. مقدار Ns باید برابر با تعداد مجموعه‌های پارامتر یک اسکن (یعنی Cs_j، Td_j، Ta_j) باشد که در سرآیند اسکن قرار دارند.

Cs_j: انتخاب‌گر مؤلفه اسکن.[1] انتخاب می‌کند که کدام یک از Nf مؤلفه تصویری که در پارامترهای فریم مشخص شده‌اند باید به‌عنوان j مین مؤلفه در اسکن قرار بگیرند. هر Cs_j باید با یکی از مقادیر C_i که در سرآیند فریم مشخص شده‌اند، هم‌خوانی داشته باشد. همچنین ترتیب موجود در سرآیند اسکن باید با ترتیب موجود در سرآیند فریم منطبق باشد. اگر Ns>1 آنگاه ترتیب مؤلفه‌های یکی در میان (Interleaved) در MCU بدین صورت است: ابتدا Cs_1 سپس Cs_2 و غیره. اگر Ns>1 محدودیت زیر باید در رابطه (۳-۲) با مؤلفه‌های تصویری موجود در یک اسکن لحاظ شود.

$$\sum_{j=1}^{N_s} H_j \times V_j \leq 10 \qquad (۳-۲)$$

که در آن H_j و V_j فاکتورهای نمونه‌برداری افقی و عمودی مربوط به مؤلفه اسکن j م هستند. این فاکتورهای نمونه‌برداری در سرآیند فریم برای مؤلفه C_i معین شده‌اند.

Td_j: انتخاب‌گر آدرس جدول مربوط به کدینگ آنتروپی DC. یکی از چهار مقدار ممکن برای آدرس جدول کدینگ آنتروپی DC را مشخص می‌کند که به کمک آن ضرایب DC مؤلفه Cs_j بازیابی می‌شود. هنگامی که دیکدر آماده دیکد کردن اسکن فعلی است، باید جدول آنتروپی DC در این آدرس نصب شده باشد. این پارامتر برای فرآیندهای بدون خطا آدرس جدول کدینگ آنتروپی را مشخص می‌کند.

Ta_j: انتخاب‌گر آدرس جدول مربوط به کدینگ آنتروپی AC. یکی از چهار مقدار ممکن برای آدرس جدول کدینگ آنتروپی AC را مشخص می‌کند که به کمک آن ضرایب AC مؤلفه Cs_j بازیابی می‌شود. هنگامی‌که دیکدر آماده دیکد کردن اسکن فعلی است، باید جدول آنتروپی AC انتخاب شده در این آدرس نصب شده باشد. مقدار این پارامتر برای فرآیندهای بدون خطا صفر است.

Ss: محل شروع انتخاب طیفی یا تخمین‌گر.[2] در حالت‌های انکدینگ مبتنی بر DCT این پارامتر نخستین ضریب DCT را در هر بلوک که قرار است طبق یک ترتیب زیگزاگ در یک اسکن کد شوند، مشخص می‌کند. این پارامتر در فرآیندهای رشته‌ای مبتنی بر DCT باید برابر با صفر قرار داده شود. در فرآیندهای بدون خطا، از این پارامتر برای انتخاب تخمین‌گر استفاده می‌شود.

Se: پایان انتخاب طیفی.[3] این پارامتر آخرین ضریب DCT را در هر بلوک که قرار است طبق یک ترتیب زیگزاگ در یک اسکن کد شوند، مشخص می‌کند. این پارامتر در فرآیندهای رشته‌ای مبتنی بر DCT باید برابر با ۶۳ قرار داده شود. در فرآیندهای بدون خطا، این پارامتر معنای خاصی ندارد و باید برابر با صفر در نظر گرفته شود.

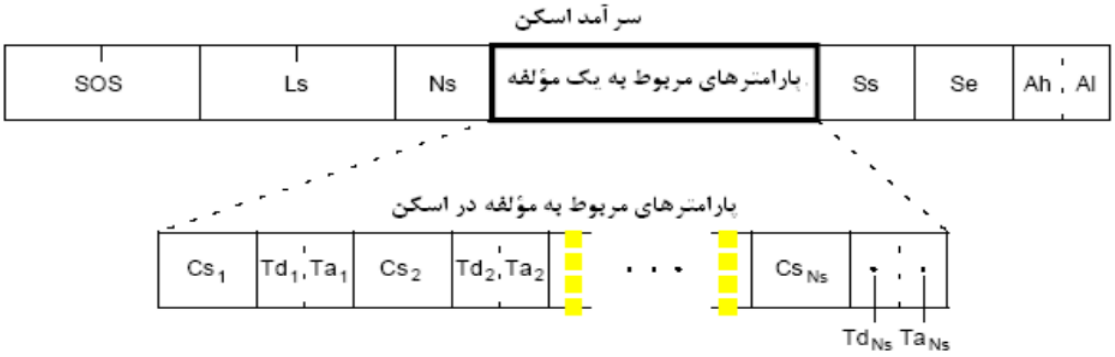
---

۱. Scan Component Selector

۲. Start of Spectral or Predictor Selection

۳. End of Spectral Selection

Ah: موقعیت بالای بیت تخمینی در دنباله.[1] این پارامتر تبدیل نقطه‌ای را مشخص می‌کند که در اسکن قبلی برای باندی از ضرایب که توسط Ss و Se تعیین شده‌اند، مورد استفاده قرار گرفته است (یعنی پایین‌ترین بیت تقریبی در دنباله در اسکن قبلی). این پارامتر باید برای اولین اسکن هر یک از باندهای ضرایب برابر با صفر قرار داده شود. در حالت بدون خطا، این پارامتر معنای خاصی ندارد و باید برابر با صفر در نظر گرفته شود.



شکل ۳-۶: اجزاء و ترتیب قرارگیری بایت‌ها در داخل سرآیند فریم

Al: موقعیت پائین بیت تخمینی در دنباله یا تخمین نقطه‌ای.[2] در حالت‌های مبتنی بر DCT این پارامتر تبدیل نقطه‌ای را مشخص می‌کند؛ یعنی موقعیت پائین بیت، که قبل از کد کردن باند ضرایب تعیین شده توسط Ss وSe مورد استفاده قرار گرفته است. این پارامتر در فرآیندهای مبتنی بر DCT باید برابر با صفر قرار داده شود. در حالت‌های بدون خطا، این پارامتر تبدیل نقطه‌ای (Pt) را مشخص می‌کند.
انتخاب‌گرهای آدرس جدول‌های آنتروپی، یعنی Td_j و Ta_j هم می‌توانند معرف جدول‌های هافمن باشند (در فریم‌هایی که کدینگ هافمن را استفاده می‌کنند) و هم می‌توانند معرف جدول‌های مربوط به کدینگ حسابی باشند (در فریم‌هایی که کدینگ حسابی را استفاده می‌کنند). در حالت اخیر، انتخاب‌گر آدرس جدول آنتروپی هم آدرس جدول شرطی کدینگ حسابی[3] و هم محدوده آماری مربوطه[4] را مشخص می‌کند.

---

۱. Successive approximation bit Position High
۲. Successive Approximation bit Position Low or Point Transform
۳. Arithmetic Coding Conditioning Table
۴. Associated Statistics Area

جدول ۳-۴: پارامترهای موجود در سرآیند اسکن، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (بر حسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Ls	۱۶	۶+۲×Ns			
Ns	۸	۱-۴			
Csj	۸	۰-۲۵۵[a]			
Tdj	۴	۰-۱	۰-۳	۰-۳	۰-۳
Taj	۴	۰-۱	۰-۳	۰-۳	۰
Ss	۸	۰	۰	۰-۶۳	۱-۷[b]
Se	۸	۶۳	۶۳	Ss-۶۳[c]	۰
Ah	۴	۰	۰	۰-۱۳	۰
AI	۴	۰	۰	۰-۱۳	۰-۱۵

a) Csj باید عضوی از مجموعه C_i باشد که در سرآیند فریم مشخص شد

b) ۰ برای فریم‌های تفاضلی بدون خطا در حالت سلسله مراتبی

c) ۰ اگر Ss برابر با صفر باشد

۳-۵-۳ جدول‌ها و قطعات شاخص متفرقه

در شکل ۳-۷ نشان داده می‌شود که قسمت‌هایی از شکل ۳-۴ که برای قرارگیری جدول‌ها (جدول‌های کوانتیزاسیون یا جدول‌های مربوط به کدینگ آنتروپی) و یا قطعات شاخص متفرقه در نظر گرفته شده است، حاوی چه اطلاعاتی هستند.

اگر برای یک آدرس معین در دادگان تصویر فشرده جدولی اختصاص یافته باشد، این جدول باید جایگزین هر گونه جدولی گردد که قبلاً در این آدرس قرار گرفته بوده است و هرگاه که در اسکن‌های باقیمانده از یک فریم و یا تصاویر پی‌درپی در فرمت مخفف شده (Abbreviated Format) به این آدرس رجوع می‌شود، باید بتواند مورد استفاده قرار گیرد. اگر برای یک آدرس مشخص، جدولی بیش از یک بار تخصیص یابد، باید جایگزین جدول قبلی گردد. در هنگام اسکن‌های متوالی ضرایب DCT یک مؤلفه خاص، نباید تخصیص جدول تغییر کند.

شکل ۳-۷: قطعات شاخص متفرقه

۱-۳-۵-۳ جدول کوانتیزاسیون

در شکل ۳-۸ قطعه شاخصی که یک یا چند جدول کوانتیزاسیون در آن تعریف می‌شود، نشان داده شده است. در این قسمت، شاخص‌ها و پارامترهای موجود در شکل ۳-۸ تعریف شده و مقادیر مجاز پارامترها در جدول ۳-۵ ارائه می‌شود.

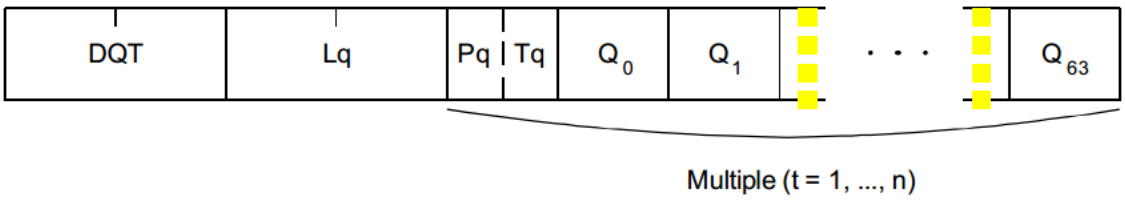
DQT: شاخص معرف جدول کوانتیزاسیون.[۱] این شاخص محل شروع جدول کوانتیزاسیون و پارامترهای متناظر با آن را مشخص می‌کند.

Lq: طول جدول کوانتیزاسیون. تعداد بایت‌های اختصاص یافته به‌کل جدول کوانتیزاسیون را که در جدول ۳-۵ ارائه شده، مشخص، می‌کند.

Pq: دقت المان‌های موجود در جدول کوانتیزاسیون.[۲] دقت (مقدار بیت بر نمونه) هر یک از مقادیر Q_K را مشخص می‌کند. مقدار صفر بیانگر Q_K های هشت بیتی و مقدار یک بیانگر Q_K های ۱۶ بیتی است. اگر دقت نمونه (P) هشت بیت بر نمونه باشد، باید مقدار Pq برابر با صفر باشد.

Tq: معرف آدرس جدول کوانتیزاسیون.[۳] یکی از چهار آدرس ممکن در دیکدر را مشخص می‌کند که باید جدول کوانتیزاسیون در آن نصب شود.

Q_K: المانی از جدول کوانتیزاسیون.[۴] جزء K ام از ۶۴ جزء جدول کوانتیزاسیون را مشخص می‌کند که در آن K اندیسی است متناظر با یکی از ضرایب DCT که با ترتیب زیگزاگ چیده شده‌اند. المان‌های جدول کوانتیزاسیون باید طبق یک اسکن زیگزاگی مشخص شوند. مقدار نشان داده شده در جدول ۳-۵ برابر است با تعداد جدول‌های کوانتیزاسیون موجود در یک قطعه شاخص DQT. اگر برای آدرس خاصی یک جدول کوانتیزاسیون تعریف شده باشد، این جدول جایگزین جدول قبلی موجود در آن آدرس خواهد شد و از این پس (در صورت ارجاع به آن در اسکن‌های بعدی تصویر فعلی و یا در تصاویر بعدی که در فرمت مخفف شده در ادامه خواهند آمد) مورد استفاده قرار خواهد گرفت. اگر برای آدرس خاصی هیچ جدولی تعریف نشده باشد، در این صورت اگر این آدرس در قسمت سرآیند فریم مشخص شده باشد، حاصل غیرقابل پیش‌بینی خواهد بود. همچنین باید توجه داشت که یک فرآیند هشت بیتی مبتنی بر DCT نباید در جدول کوانتیزاسیون خود از دقت ۱۶ بیتی استفاده کند.



شکل ۳-۸: تخصیص جدول کوانتیزاسیون

---

۱. Define Quantization Table Marker (DQT)

۲. Quantization Table Element Precision

۳. Quantization Table Destination Identifier

۴. Quantization Table Element

جدول ۳-۵: پارامترهای موجود در بخش تخصیص جدول کوانتیزاسیون، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (بر حسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Lq	۱۶	$۲ + \sum_{t=۱}^{n} (٦٥ + ٦٤ \times Pq(t))$			تعریف نشده
Pq	۴	۰	۰،۱	۰،۱	تعریف نشده
Tq	۴	۰-۳			تعریف نشده
Q_k	۸،۱۶	۱-۲۵۵ , ۱ - ۶۵ ۵۳۵			تعریف نشده

۳-۵-۳-۲ جدول هافمن

در شکل ۳-۹ قطعه شاخصی که یک یا چند جدول هافمن در آن تعریف می‌شود، نشان داده شده است. در این قسمت، شاخص‌ها و پارامترهای موجود در شکل ۳-۹ تعریف شده و مقادیر مجاز پارامترها در جدول ۳-۶ ارائه می‌شود.

DHT: شاخص معرف جدول هافمن.[۱] محل شروع تعریف جدول هافمن و پارامترهای متناظر با آن را مشخص می‌کند.

Lh: طول جدول هافمن. طول متناظر با تمامی پارامترهای جدول هافمن (که در جدول ۳-۶ ارائه شده‌اند) را برحسب بایت مشخص می‌کند.

Tc: کلاس (گروه) جدول.[۲] اگر مقدار آن برابر با صفر باشد، جدول DC است و اگر برابر با یک باشد، جدول AC است.

Th: معرف آدرس جدول هافمن.[۳] یکی از چهار آدرس ممکن در دیکدر را که جدول هافمن باید در آن نصب شود، مشخص می‌کند.

L_i: تعداد کدهای هافمن دارای طول i. برای هر یک از ۱۶ طول ممکن برای این قسمت، تعداد کدهای هافمن برابر با آن طول را مشخص می‌کند. L_i ها، المان‌های لیستی تحت عنوان BITS را تشکیل می‌دهند.

$V_{i,j}$: مقدار اختصاص یافته به هر کد هافمن. برای هر i مقدار متناظر با هر کد هافمن به طول L_i را مشخص می‌کند. معنای هر مقدار با توجه به مدل کدینگ هافمن معلوم می‌شود. مقادیر $V_{i,j}$ المان‌های لیست HUFFVAL را تشکیل می‌دهند.

---

۱. Define Huffman Table Marker (DHT)

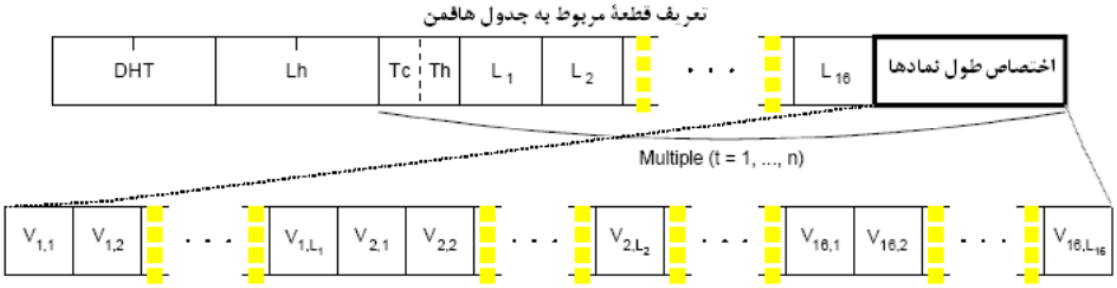
۲. Table Class

۳. Huffman Table Destination Identifier

مقدار n در جدول ۳-۶ برابر است با تعداد جدول‌های هافمنی که در قطعه شاخص DHT تعریف شده‌اند. مقدار m تعداد پارامترهایی است که پس از $L_i(t)$ ۱۶ پارامتر هر جدول هافمن t می‌آید، و از رابطه (۳-۳) تعیین می‌شود:

$$m_t = \sum_{i=1}^{16} L_i \qquad (۳-۳)$$

در کل برای هر جدول مقدار m_t متفاوت است. اگر برای آدرس خاصی یک جدول هافمن تعریف شده باشد، این جدول جایگزین جدول قبلی موجود در آن آدرس خواهد شد و از این پس (در صورت ارجاع به آن در اسکن‌های بعدی تصویر فعلی و یا در تصاویر بعدی که در فرمت مخفف شده در ادامه خواهند آمد) مورد استفاده قرار خواهد گرفت. اگر برای آدرس خاصی هیچ جدولی تعریف نشده است، در این صورت اگر این آدرس در قسمت سرآیند اسکن مشخص شده باشد، حاصل غیرقابل پیش‌بینی خواهد بود.



شکل ۳-۹: تخصیص جدول هافمن

جدول ۳-۶: پارامترهای موجود در بخش تخصیص جدول هافمن، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (بر حسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Lh	۱۶	$۲ + \sum_{t=1}^{n}(۱۷ + m_t)$			
Tc	۴	۰،۱		۰،۱	۰
Th	۴	۰،۱		۰-۳	
L_i	۸	۰-۲۵۵			
$V_{i,j}$	۸	۰-۲۵۵			

۳-۵-۴ دادگان کاربردی (نرم‌افزاری)

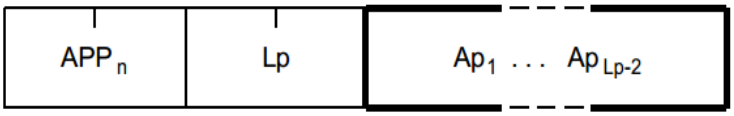
در شکل ۳-۱۰ ساختار مربوط به یک قطعه شامل دادگان کاربردی نشان داده شده است. قطعات App_n برای کاربرد نرم‌افزارها رزرو شده‌اند. از آنجا که ممکن است برای نرم‌افزارها و کاربردهای مختلف، نحو

تعریف این قطعات متفاوت باشد، باید هنگام تبادل اطلاعات بین نرم‌افزارها و کاربردهای مختلف، این دادگان حذف شوند. شاخص و پارامترهای متناظر با آن در جدول ۳-۷ نشان داده شده و در این قسمت تعریف می‌شوند.

App_n: شاخص دادگان کاربردی[۱] محل شروع یک بخش حاوی دادگان کاربردی را مشخص می‌کند.

Lp: طول بخش دادگان کاربردی. تعداد بایت‌های متناظر با قطعه شاخص دادگان کاربردی را معین می‌کند (با احتساب دو بایت متناظر با خود Lp).

Ap_i: بایت‌های دادگان کاربردی. تفسیر این بایت‌ها به نرم‌افزار و کاربرد بستگی دارد.



شکل ۳-۱۰: دادگان کاربردی

جدول ۳-۷: پارامترهای موجود در بخش دادگان کاربردی، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (بر حسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Lp	۱۶	۲- ۶۵ ۵۳۵			
Ap_i	۸	۰-۲۵۵			

همان گونه که اشاره شد ۱۶ نوع از دادگان کاربردی وجود دارند که با شاخص کاربردی آغاز می‌شوند و این شاخص‌ها می‌توانند یکی از موارد FFE0 تا FFEF باشند. در بخش زیر دادگان کاربردی پر اهمیت‌تر معرفی شده‌اند.

۳-۵-۴-۱ قالب تبادل فایل JPEG[۲] (JFIF)

JFIF اولین نوع از دادگان کاربردی (APP_0) به‌حساب می‌آید. اطلاعات مربوط به JFIF با شاخص کاربردی FFE0 آغاز می‌شوند و در ادامه اطلاعات بعدی می‌آیند. در جدول ۳-۸ اطلاعات مربوط به JFIF نشان داده شده است.

۱. Application Data Marker

۲. JPEG File Interchange Format (JFIF)

جدول ۳-۸: اطلاعات JFIF

فضای ذخیره‌سازی	اندازه (بایت)	شرح
نشانه APP_0	۲	همیشه معادل ۰xFFE۰
طول	۲	طول بخش به‌استثنای نشانه APP_0
شناسه	۵	همیشه معادل (۰x۴A۴۶۴۹۴۶۰۰) "JFIF"
نسخه	۲	بایت اول نسخه اصلی (معمولاً ۰x۰۱)، بایت دوم نسخه فرعی (معمولاً ۰x۰۲).
واحدهای چگالی	۱	واحدهای چگالی پیکسل • ۰ – واحد ندارد و فقط نسبت طول به عرض مشخص شده است. • ۱ – پیکسل بر اینچ • ۲ – پیکسل بر سانتیمتر
چگالی X	۲	چگالی پیکسل افقی صحیح
چگالی Y	۲	چگالی پیکسل عمودی صحیح
عرض (tw) تصویر بندانگشتی	۱	اندازه افقی تصویر بندانگشتی JFIF جاسازی شده در هر پیکسل
ارتفاع (th) تصویر بندانگشتی	۱	اندازه عمودی تصویر بندانگشتی JFIF جاسازی شده در هر پیکسل
داده تصویر بندانگشتی	۳×tw×th	Uncompressed 24 bit RGB raster thumbnail

۲-۴-۵-۳ قالب فایل تصویری تعویض‌پذیر[۱] (EXIF)

اولین بار یک شرکت خدمات مهندسی الکترونیک در ژاپن (JEIDA[۲])، استانداردی جهت افزودن ابر اطلاعات[۳] به تصاویر تهیه شده از دوربین‌های عکاسی را پیشنهاد داد.

هر تصویر JPEG با سرآیند FFD8 که به‌عنوان[۴] SOI شناخته شده شروع و با ته آمد FFD9 به معنای EOI[۵] به پایان می‌رسد. در این میان اطلاعات تصویر و ابر اطلاعات بر اساس یک چیدمان خاص قرار می‌گیرند. هر اطلاعات اضافه در یک قالب خاص بر اساس یک سرآیند شاخص، طول اطلاعات خود و اطلاعات تعریف می‌شود.

ساختار JPEG، شاخص‌های گوناگون را با کاربردهای مختلفی مورد استفاده قرار می‌دهد. در این میان شاخص‌هایی که در رنج و بازه FFE0 تا FFEF به‌منظور افزودن ابر داده‌ها در تصویر مورد استفاده قرار می‌گیرد. این اطلاعات برای بازخوانی نیاز به کدگشایی بر اساس انکدر JPEG ندارند.

اما به هر حال خواندن آن‌ها کمی متفاوت از بازیابی اطلاعات بر اساس JPEG است. این شاخص‌ها، شاخص‌هایی کاربردی[۶] نامیده می‌شوند.

---

۱. Exchangeable Image File Format (EXIF)

۲. Japanese Electronics Industry Development Association (JEIDA)

۳. Metadata

۴. Start of Image (SOI)

۵. End of Image (EOI)

۶. Application Marker

ساختار راهنمای فایل تصویر[1](IFD): EXIF از ساختاری ساده برای نمایش IFD و اطلاعات تصویر استفاده می‌کند. ابتدا دو بایت که فرمت اطلاعات را مشخص می‌کند وجود دارد و دو بایت بعدی ویژگی اطلاعات (نظیر طول، عرض، رزولوشن و غیره) مشخص می‌کند در بعضی از موارد طول اطلاعات بیشتر از چهار بایت بعدی طول اطلاعات را مشخص می‌کند. بنابراین اگر طول اطلاعات کمتر از چهار بایت باشد. چهار بایت بعدی حاوی اطلاعات خواهد بود
و در غیر این صورت چهار بایت بعدی به offset حافظه‌ای اشاره می‌کند که اطلاعات در آنجا قرار دارد.

۳-۴-۵-۳ دادگان کاربردی فتوشاپ

یکی دیگر از دادگان کاربردی، دادگان کاربردی مربوط به نرم‌افزار فتوشاپ است. این دادگان با شاخص کاربردی FFED شروع می‌شوند و پس از آن اندازه قطعه مشخص می‌شود. در ادامه اطلاعاتی به‌عنوان ابر داده آورده می‌شود که مربوط به تصاویر طراحی شده در فتوشاپ است.
در ابر داده مربوط به این بخش امکان قرار دادن یک تصویر بندانگشتی از تصویر نیز وجود دارد. قرار دادن تصویر بندانگشتی در بخش‌های قبل وابسته نیست و نرم‌افزار فتوشاپ این تصویر بندانگشتی را می‌سازد.

۳-۴-۵-۴ دادگان کاربردی APP14

FFEE یکی دیگر از دادگان کاربردی که در تصاویر JPEG وجود دارد مربوط به‌قرار دادن کلمه Adobe و نسخه‌ی بکار گرفته شده از آن برای ساخت تصویر است. در این قسمت پس از دو بایت مربوط به اندازه قطعه، پنج بایت مربوط به کلمه‌ی Adobe می‌آید. سپس در ادامه با شش بایت نسخه مربوطه مشخص می‌شود.

۳-۵-۵ تعریف تعداد سطرها (DNL)

در شکل ۳-۱۱ ساختار مربوط به یک قطعه شاخص برای تعریف تعداد سطرها[2](DNL) نشان داده شده است. قطعه DNL، مکانیسمی را برای تعریف (یا تعریف مجدد) تعداد سطرهای موجود در فریم (پارامتر Y در قسمت سرآیند فریم) را در انتهای اسکن اول، فراهم می‌کند. مقدار تعیین شده باید با تعداد سطرهای MCU ای که در اسکن اول انکد می‌شوند، متناسب باشد. اگر این قطعه مورد استفاده قرار گیرد، فقط باید در انتهای اسکن اول و بعد از کد کردن تعداد صحیحی از سطرهای MCU جای داده شود. اگر مقدار Y (تعداد سطرها) در سرآیند فریم برابر با صفر بوده باشد، استفاده از این قطعه شاخص

---

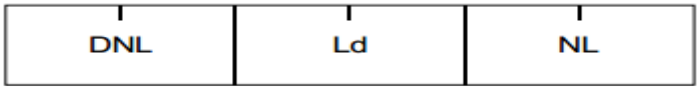
۱. Image File Directory (IFD)
۲. Define Number of Lines (DNL)

اجباری است. شاخص و پارامترهای متناظر با آن در جدول ۳-۹ نشان داده شده و در این قسمت تعریف می‌شوند.

DNL: شاخص محل تعریف تعداد سطرها[۱]مشخص کننده محل شروع قطعه تعریف کننده تعداد سطرها.

Ld: طول قطعه شاخص تعریف تعداد سطرها (بر حسب بایت).

NL: تعداد سطرها. تعداد سطرهای موجود در یک فریم را مشخص می‌کند.



شکل ۳-۱۱: تعریف تعداد سطرها

جدول ۳-۹: پارامترهای موجود در بخش تعریف تعداد سطرها، اندازه هر یک (بر حسب بیت) و مقادیر مجاز آن‌ها

پارامتر	اندازه (بر حسب بیت)	مقادیر پارامترها در حالت‌های مختلف انکدینگ			
		حالت انکدینگ رشته‌ای مبتنی بر DCT		حالت تصاعدی مبتنی بر DCT	حالت بدون خطا
		حالت معمولی (اصلی)	تعمیم یافته		
Ld	۱۶	۴			
NL	۱۶	۱- ۶۵ ۵۳۵ [a]			
a) مقدار اختصاص یافته باید با تعداد سطرهای کد شده در نقطه‌ای که قطعه DNL از دادگان فشرده قطعه خارج می‌شود، همسان باشد.					

۳-۶ جمع‌بندی

در این فصل مفاهیم مورد نیاز در این رساله تعریف شد. در ادامه این رساله، روش جدیدی برای احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه می‌شود. در این روش ابتدا با توجه به دادگان کاربردی در سرآیند تصویر JPEG، نوع نرم‌افزار ویرایشگر یا مدل دوربین شناسایی می‌شود و سپس با توجه به دیگر اطلاعات موجود در سرآیند نیز نرم‌افزار ویرایشگر و مدل دوربین را باری دیگر شناسایی می‌شود و سپس در صورت عدم تطابق اطلاعات، سرآیند تغییر یافته شناسایی می‌شود. در فصل بعدی به معرفی بیشتر روش پیشنهادی می‌پردازیم.

۱. Define Number of Lines Marker

فصل ٤ : روش پیشنهادی

۴-۱ مقدمه

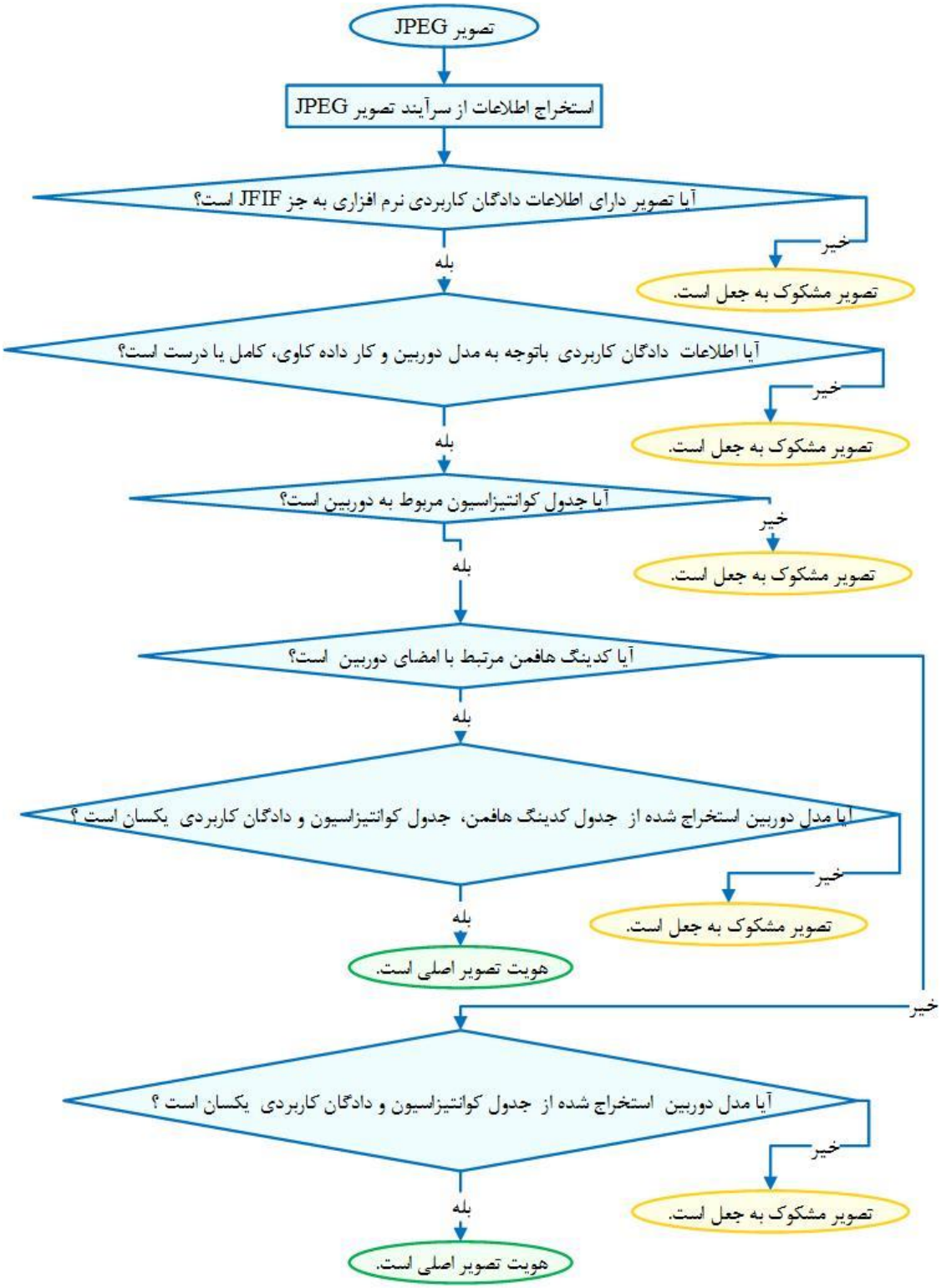
تایید صحت تصاویر دیجیتال که به‌عنوان شواهد به دادگاه فرستاده می‌شوند، بسیار مهم است. ما توضیح می‌دهیم که چگونه می‌توان به صورت‌های مختلفی از سرآیند تصویر JPEG برای تأیید اعتبار استفاده کرد. دوربین‌ها معمولاً از وضوح‌ها و کیفیت‌های متعدد پشتیبانی می‌کنند که هر یک تصاویر JPEG، را با پارامترهای مختلف فشرده‌سازی، ارائه می‌دهند. در نرم‌افزار ویرایش عکس از پارامترهای JPEG متمایز از دوربین استفاده می‌شود، هرگونه ویرایش باعث تغییر در امضای اصلی می‌شود و بنابراین به‌راحتی و بدون ابهام می‌توان آن را تشخیص داد. امضای دوربین از یک تصویر JPEG متشکل از اطلاعات مربوط به جداول کوانتیزاسیون، کدینگ هافمن، تصویر بندانگشتی و ابر اطلاعات EXIF استخراج می‌شود. استخراج این آثار ساده است و روشی کارآمد برای اثبات اعتبار تصویر دیجیتال ارائه شده است.

در این فصل، روش پیشنهادی احراز هویت تصاویر JPEG بر مبنای منبع، شرح داده شده و مراحل مختلف روش پیشنهادی پیاده‌سازی می‌شود. همچنین ابزارهای استفاده شده برای پیاده‌سازی به‌صورت اجمالی توضیح داده می‌شوند.

۴-۲ روش پیشنهادی احراز هویت تصاویر JPEG

روش پیشنهادی در این رساله از اطلاعات سرآیند تصاویر JPEG به‌منظور احراز هویت تصاویر استفاده می‌کند. در واقع، به کمک روش پیشنهادی منبع عکس مشخص می‌شود. با توجه به منبع عکس می‌توان تا حد زیادی هویت تصویر را مشخص نمود. اگر منبع تصویر دوربین باشد و به‌درستی تعیین شده باشد، می‌توان بیان نمود که تصویر دارای هویت اصلی است و جعلی نمی‌باشد. اگر منبع تصویر، نرم‌افزار ویرایشگر تصویر شناسایی شود، تصویر به‌عنوان مشکوک به جعل معرفی خواهد شد. هر چند ممکن است که محتوای اصلی تصویر تغییر نکرده باشد، اما با توجه به توضیحات فصل دوم فشرده‌سازی مضاعف از مصادیق جعل است و تصویر با منبع نرم‌افزار حداقل دارای فشرده‌سازی مضاعف می‌باشد. از این‌رو، تصاویر با منبع نرم‌افزار ویرایشگر در دسته مشکوک به جعل قرار خواهند گرفت.

مراحل روش پیشنهادی در شکل ۴-۱ نشان داده شده است. این مراحل در ادامه فصل به‌تفصیل شرح داده شده است.



شکل ۴-۱: چارت مراحل روش پیشنهادی

برای انجام رساله مراحل زیر انجام گرفته است به شرح آن‌ها می‌پردازیم.

۴-۲-۱ بررسی و استخراج اطلاعات مهم سرآیند تصاویر JPEG:

بررسی ساختار فایل‌های JPEG و آشنایی با سرآیند و داده اصلی آن‌ها در گام اول قرار گرفته است. در این مرحله، به کمک نرم‌افزارهای JPEGSNOOP، EXIFTOOL، EXIV2 و JHEAD اطلاعات سرآیند تصویر استخراج می‌شود و بررسی‌ها و تحلیل‌ها، بر اساس اطلاعات استخراج شده انجام می‌شوند.

۴-۲-۱-۱ آشنایی با نرم‌افزارهای استخراج، تولید و ویرایش سرآیند JPEG و استفاده از آن‌ها

از نرم‌افزارهای زیادی برای استخراج استفاده می‌شود. از میان این نرم‌افزارها، چهار نرم-افزارJPEGSNOOP، EXIFTOOL، EXIV2 و JHEAD نرم‌افزارهای قوی‌تری برای استخراج و تولید سرآیند هستند. در ادامه، هر یک از این نرم‌افزارها به‌اختصار معرفی می‌شوند.

JPEGSNOOP: این ابزار برای دیکد تصویر JPEG استفاده می‌شود. همچنین از این ابزار برای آنالیز مناسب سرآیند، حجم عظیمی از اطلاعات سرآیند تصاویر مختلف به‌عنوان دادگان در این نرم‌افزار جمع‌آوری شده است و از این اطلاعات برای آنالیز مناسب سرآیند تصاویر استفاده می‌شود. در صورت ویرایش اطلاعات JPEG این نرم‌افزار قادر به تشخیص آن خواهد بود.

EXIFTOOL: قدرتمندترین ابزار خواندن، نوشتن و ویرایش سرآیند تصویر، صوت، ویدئو و PDF و استخراج و افزودن تصویر بندانگشتی است. از این ابزار برای خواندن، نوشتن تصاویر بخصوص JPEG، TIFF ، CR2، PNG و GIF استفاده می‌شود. از این‌رو، از این نرم‌افزار می‌توان برای تبدیل سرآیند تصاویر به یکدیگر استفاده کرد. مثلا به کمک این نرم‌افزار و برخی از استاندارد سازی‌ها می‌توان سرآیند TIFF را به JPEG تبدیل نمود. این ابزار کد آزاد در فضای مجازی وجود دارد. این ابزار برخی سرآیندهای زائد در تصویر JPEG را تولید می‌کند. از طرف دیگر فضای خالی را از بین می‌برد. برخی پارامترها را نیز معادل می‌کند مانند ۱۰/۲۰۰۰ که تبدیل به ۱/۲۰۰ می‌شود. برای استفاده از این نرم‌افزار باید به نکات گفته شده توجه داشت و در استاندارد سازی آن‌ها را تصحیح نمود. این ابزار قابلیت خواندن تمام بخش‌های سرآیند را دارد. اما تنها قابلیت ویرایش و تولید بخش‌های موجود در جدول ۴-۱ در سرآیند را دارد. البته باید توجه داشت که این نرم‌افزار قابلیت ویرایش و تولید سرآیند غالب تصاویر متعارف JPEG را دارد. و تنها شاید کمتر از یک درصد تصاویر JPEG موجود در فضای مجازی توسط این نرم‌افزار حمایت نمی‌شوند. البته برخی از بخش‌های سرآیند مانند DQT و SOF قابل ویرایش نیستند و با تغییر آن‌ها تصویر قابل نمایش نیست. از این‌رو، این بخش‌ها توسط نرم‌افزار ویرایش نمی‌شوند.

EXIV2: این ابزار نیز برای خواندن و نوشتن در سرآیند تصاویر استفاده می‌شود. این برنامه از خواندن و نوشتن سرآیند در فرمت‌های JPEG، TIFF و PNG حمایت می‌کند. اما تنها قابلیت خواندن سرآیند CR2 را دارد. همچنین از فرمت تصویری GIF و BMP پشتیبانی حداقلی دارد. برخی از کمبودهای نرم‌افزار EXIFTOOL را می‌توان با این نرم‌افزار حل کرد.

JHEAD: این ابزار برای خواندن و نوشتن اطلاعات دوربین‌های دیجیتال در بخش EXIF سرآیند استفاده می‌شود. در واقع توانایی این نرم‌افزار تنها در بخش EXIF است. از این نرم‌افزار برای حذف بخش تصویر بندانگشتی نیز استفاده می‌شود.

هر یک از ابزارهای فوق، توانایی متفاوتی دارند که با بررسی‌های انجام شده، بهترین ترکیب آن‌ها برای استخراج و تولید سرآیند تصویر JPEG استفاده می‌شود.

جدول ۴-۱: قابلیت نرم‌افزار EXIFTOOL برای ویرایش و تولید بخش‌های سرآیند تصاویر

JPEG Meta Information	Can Read?	Can Edit?	Can Create?	Description
APP_0-JFIF	Yes	Yes	Yes	JPEG File Interchange Format
APP_0-CIFF	Yes	Yes	No	Camera Image File Format (used by some Canon models)
APP_1-EXIF	Yes	Yes	Yes	Exchangeable Image File Format (including maker notes)
APP_1-XMP	Yes	Yes	Yes	Extensible Metadata Platform (multi-segment)
APP_2-ICC	Yes	Yes	Yes	International Color Consortium (multi-segment)
APP_3-Kodak Meta	Yes	Yes	No	Kodak Meta information (EXIF-like)
APP_{12}-Ducky	Yes	Yes	Yes	Photoshop "Save for Web"
APP_{13}-Photoshop IRB	Yes	Yes	Yes	Image Resource Block (multi-segment, includes IPTC)
APP_{14} - Adobe	Yes	Yes	Yes	Adobe DCT Filter
COM	Yes	Yes	Yes	JPEG Comment (multi-segment)
DQT	Yes	No	No	(used to calculate the Extra:JPEGDigest tag value)
SOF	Yes	No	No	JPEG Start Of Frame

۴-۲-۲ عدم وجود دادگان کاربردی در اطلاعات سرآیند تصویر JPEG

در صورت عدم وجود دادگان کاربردی، تصویر مشکوک به جعل است. عدم وجود دادگان کاربردی نشان از عدم اصالت تصویر دارد. تمام عکس‌ها با منبع دوربین دارای اطلاعات دادگان کاربردی هستند. حذف این اطلاعات نشان استفاده از نرم‌افزار ویرایشگر تصویر است. البته همان‌طور که بیان شد، وجود برخی از دادگان کاربردی خود نشان دهنده وجود نرم‌افزار ویرایشگر تصویر است. برخی از نرم‌افزارهای ویرایشگر تصویر نظیر corelpainter نیز تمام دادگان کاربردی را حذف کرده و فقط JFIF را نگه می‌دارند. از این رو حذف دادگان کاربردی به‌جز JFIF نیز نشان دهنده استفاده از نرم‌افزارهای ویرایشگر تصویر است.

۴-۲-۳ بررسی و استخراج اطلاعات مهم دادگان کاربردی (نرم‌افزاری)

دادگان کاربردی مهم‌ترین بخش اختیاری در سرآیند هستند. قطعات App_n برای کاربرد نرم‌افزارها رزرو شده‌اند. از آنجا که ممکن است برای نرم‌افزارها و کاربردهای مختلف، نحو تعریف این قطعات متفاوت

باشد، باید هنگام تبادل اطلاعات بین نرم‌افزارها و کاربردهای مختلف، این دادگان حذف شوند. یک یا چند قطعه APP_0 تا APP_F مربوط به دادگان کاربردی (با شاخص آغازین FFE0 تا FFEF) پس از شاخص آغاز تصویر می‌آیند. لازم به ذکر است که این دادگان اختیاری هستند و در صورت عدم وجود آن‌ها مشکلی برای تصویر ایجاد نمی‌شود. در بخش زیر دادگان کاربردی پر اهمیت‌تر معرفی شده‌اند.

۴-۲-۳-۱ قالب تبادل فایل JPEG (JFIF)

بخش JFIF از دادگان کاربردی پر اهمیت بشمار می‌رود که در غالب تصاویر JPEG وجود دارد. JFIF یکی از شاخص‌های کاربردی است که به‌عنوان شاخص کاربردی صفر شناخته شده و با شاخص FFE0 در ساختار JPEG مورد استفاده قرار می‌گیرد.

البته در رابطه با بخش JFIF این نکته را باید بیان نمود که در اکثر فایل‌های JPEG بخش JFIF شامل داده تصویر بندانگشتی نیست و اطلاعات عرض و ارتفاع تصویر بندانگشتی برابر با صفر است.

در سال ۱۹۹۲، استانداردی تحت عنوان JFIF[۱]، جهت افزودن اطلاعاتی نظیر طول، عرض، فضای رنگ و غیره به تصاویر JPEG اضافه شد. اما نیاز عکاسان در تهیه یک عکس فراتر از این اطلاعات مختصر و ساده بود. هر عکاس نیاز به جزئی‌ترین اطلاعات تصویر ثبت شده خود نظیر زمان، مدل، دوربین، لنز، Gps، مشخصات تصویر بندانگشتی، فضای رنگ، نوع ویرایشگر، کپی رایت و غیره داشت. این نیاز شرکت JEIAD را بر آن داشت استانداردی منطبق بر نیاز عکاسان را به فرمت تصویری JPEG اضافه کند. از این‌رو در سال ۱۹۹۸، استانداردی تحت عنوان EXIF که برگرفته از Exchangeable Image File Format بود را ارائه کرد.

۴-۲-۳-۲ قالب فایل تصویری تعویض‌پذیر (EXIF)

ابر اطلاعات EXIF که در سرآیند JPEG یافت می‌شود، اطلاعات متنوعی درباره دوربین و تصویر ذخیره می‌کند. ابر اطلاعات EXIF که با عنوان APP_1 شناخته می‌شود، با سرآیند شاخص FFE1 در ساختار مورد استفاده قرار می‌گیرد. این شاخص کاربردی، بلافاصله بعد از سرآیند اصلی JPEG (FFD8) قرار می‌گیرد. یکی از بخش‌های مهم در EXIF تصویر بندانگشتی[۲]است.

یک EXIF، متشکل از تعدادی راهنمای فایل تصویر[۳](IFD) است، اولین IFD، با عنوان IFD0 شناخته می‌شود. معمولاً IFDها شامل اطلاعات اصلی تصویر نظیر X-Resolution، Y-Resolution، مدل، سازنده و غیره هستند. انتهای IFD آخر در یک SubIFD معرف مکان شروع subIFD بعدی است. نشانه‌ای که برای معرفی IFD بعدی استفاده می‌شود، به‌صورت "۰×۸۷۶۹" است.

---

۱. JPEG File Format Standard

۲. Thumbnail

۳. Image File Directory

مطابق استاندارد EXIF، پنج راهنمای اصلی فایل تصویر که به‌اختصار IFD نامیده می‌شود وجود دارد که ابر اطلاعات در آن‌ها سازمان‌دهی می‌شوند که شامل (۱) اولیه[۱] (۲) EXIF؛ (۳) قابلیت سازگاری[۲] (۴) تصویر بندانگشتی و (۵) GPS هستند. تولید کنندگان دوربین آزاد هستند تا هر اطلاعاتی را در هر IFD وارد کنند. با شمارش تعداد ورودی‌های موجود در هر یک از این پنج IFD، نمایشی متراکم از انتخاب آن‌ها استخراج می‌شود. استاندارد EXIF امکان IFDهای اضافی را ایجاد می‌کند. برخی از تولید کنندگان دوربین ابر اطلاعات خود را به روش‌هایی سفارشی می‌کنند که مطابق با استاندارد EXIF نیست.

ابر اطلاعات EXIF یک تصویر به‌راحتی ویرایش می‌شود، اما لازم به ذکر است که اصلاح محتوای هر قسمت EXIF موجود، روی تعداد EXIF استخراج شده تأثیر نخواهد داشت و از این‌رو بر امضای استخراج شده تأثیری نخواهد داشت. هر نوع دوربین و مدل سازگار با آن می‌تواند با ساخت و مدل مشخص شده در ابر اطلاعات EXIF تصویر مقایسه شود. هرگونه عدم تطابق، شواهد محکمی بر نوعی دستکاری است. نمایش شاخص EXIF بر اساس حالت Intel است. این شاخص حاوی تصویر بندانگشتی نیز است. همان‌طور که قبلاً اشاره شد، شاخص EXIF دارای سرآیندی با کد اسکی و دو بایت به‌صورت OXOO است. بعد از سرآیند اطلاعات، شاخص EXIF وجود دارد. یکی از نکات مهم و قابل توجه شاخص EXIF، استفاده از فرمت TIFF جهت ذخیره‌سازی اطلاعات تصویر است. بنابراین بعد از سرآیند EXIF، بلافاصله سرآیند TIFF قرار می‌گیرد.

تصویر بندانگشتی: تصویر بندانگشتی در بیشتر مواقع تصویر یک نسخه کوچک شده با وضوح کامل از تصویر اصلی است که غالباً در سرآیند تصویر JPEG تعبیه شده است. یک تصویر کوچک معمولاً از اندازه چند صد پیکسل مربع بزرگ‌تر نیست و با برش، فیلتر و نمونه‌برداری پایین از تصویر با وضوح کامل ایجاد می‌شود. سپس تصویر بندانگشتی به‌طور معمول در سرآیند فشرده شده و ذخیره می‌شود. به همین ترتیب، می‌توان همان عناصر را از تصویر بندانگشتی مانند تصویر با وضوح کامل استخراج کرد. در صورت تخریب تصویر اصلی، می‌توان این تصویر را به‌عنوان تصویر اصلی ارائه نمود. در برخی فایل‌های JPEG امکان دارد دو تصویر بندانگشتی وجود داشته باشد که در اکثر مواقع با یکدیگر برابرند. این حالت در تصاویر خروجی دوربین رخ نمی‌دهد. باید توجه داشت خواص تصویر بندانگشتی کاملا با تصویر اصلی متفاوت است این تفاوت در مواردی از قبیل ماتریس کوانتیزاسیون، کدینگ هافمن، شاخص آغاز فریم و غیره وجود دارد.) با توجه به بررسی‌های انجام شده، هیچ تصویر بندانگشتی دارای دادگان کاربردی نرم‌افزاری نیست. در تولید تصویر بندانگشتی، توجه به‌اندازه‌ی آن حائز اهمیت است. تنها اندازه‌های خاصی برای تصاویر بندانگشتی وجود دارد. تصویر بندانگشتی که دارای ابعادی به غیر از ابعاد متداول است، می‌تواند جزء پارامترهای تشخیص مشکوک بودن تصویر به جعل لحاظ شود. در فشرده‌سازی تصویر بندانگشتی تنها از حالت کدینگ رشته‌ای مبتنی بر DCT استفاده می‌شود اگر در فشرده‌سازی

---

۱. Primary

۲. Interoperability

تصویر بندانگشتی از حالت‌های دیگر فشرده‌سازی استفاده شده باشد، بیانگر مشکوک بودن تصویر به جعل است. برخی از تولید کنندگان دوربین تصویر بندانگشتی ایجاد نمی‌کنند یا آن‌ها را به‌عنوان تصویر JPEG کدگذاری نمی‌کنند. در چنین مواردی، به‌سادگی مقدار صفر را به تمام پارامترهای تصویر بندانگشتی اختصاص داده شده است. وجود یا عدم وجود تصویر بندانگشتی در اطلاعات سرآیند تصویر، پارامتری برای تشخیص مشکوک بودن تصویر به جعل نیست.

۴-۲-۳-۳ دادگان کاربردی فتوشاپ

یکی دیگر از دادگان کاربردی، دادگان کاربردی مربوط به نرم‌افزار فتوشاپ است. این دادگان با شاخص کاربردی FFED شروع می‌شوند و پس از آن اندازه قطعه مشخص می‌شود.

۴-۲-۳-۴ دادگان کاربردی APP14

FFEE یکی دیگر از دادگان کاربردی که در تصاویر JPEG وجود دارد و مربوط به‌قرار دادن کلمه Adobe و نسخه‌ی بکار گرفته شده از آن برای ساخت تصویر است.

۴-۲-۴ استخراج امضای تصویر از روی جدول کوانتیزاسیون و کدینگ هافمن

جداول چندی‌سازی[۱] مراحل فشرده‌سازی JPEG با برخی تغییرات توسط همه کدگذارهای JPEG استفاده می‌شود منبع اصلی تغییر در این کدگذارها انتخاب مقادیر جدول کوانتیزاسیون است. مرحله کوانتیزاسیون منبع اصلی کاهش داده‌ها و از دست رفتن اطلاعات است. جدول کوانتیزاسیون از بخش-های اجباری در سرآیند بشمار می‌آید. در این بخش دو جدول کوانتیزاسیون یکی برای شدت روشنایی و دیگری برای رنگ وجود دارد. البته باید توجه داشت که ابتدا ماتریس کوانتیزاسیون درخشندگی می‌آید. نکته‌ای که در رابطه با ماتریس‌های کوانتیزاسیون وجود دارد، تعداد قطعات مربوط به آن است. همان‌گونه که اشاره شد یک یا دو قطعه مربوط به ماتریس کوانتیزاسیون در تصاویر JPEG وجود دارد که این قطعات از بخش‌های اصلی فایل JPEG بشمار می‌رود. اگر در فایل JPEG یک قطعه مربوط به ماتریس کوانتیزاسیون وجود داشت هر دو ماتریس کوانتیزاسیون درخشندگی و رنگ در این قسمت وجود دارند و با توجه به شناسه‌ی آن (صفر یا یک) امکان شناسایی آن وجود دارد. اگر دو قطعه مربوط به ماتریس کوانتیزاسیون وجود داشت، ابتدا ماتریس کوانتیزاسیون درخشندگی با شناسه صفر و پس از آن، ماتریس کوانتیزاسیون رنگ با شناسه یک می‌آید. نحوه‌ی ذخیره‌سازی ماتریس کوانتیزاسیون در یک تصویر، با توجه به اسکن زیگزاگی است. یعنی داریه‌های ماتریس کوانتیزاسیون به ترتیب زیگزاگی در کنار هم قرار گرفته‌اند. یک یا دو قطعه DQT مربوط به ماتریس کوانتیزاسیون پس از دادگان کاربردی می‌آیند. ماتریس‌های کوانتیزاسیون شامل دو ماتریس درخشندگی و رنگ هستند که پس از شاخص

---

۱. Quantization

آغازین FF DB اندازه قطعه می‌آید و پس از آن یک بایت برای مشخص کردن نوع ماتریس کوانتیزاسیون (رنگ یا درخشندگی) می‌آید. جداول کوانتیزاسیون به دو صورت استاندارد، متناسب با دوربین و متناسب با نرم‌افزار در سرآیند تصویر JPEG وجود دارند. در ادامه به شرح این جداول می‌پردازیم.

جداول کوانتیزاسیون استاندارد: جداول کوانتیزاسیون استاندارد با بررسی چندین هزار تصویر حاصل شده است و حالت بهینه برای غالب تصاویر است. این جداول در شکل ۴-۲ نشان داده شده است.

جدول کوانتیزاسیون درخشندگی

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

جدول کوانتیزاسیون رنگ

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

شکل ۴-۲: جدول کوانتیزاسیون استاندارد

جداول کوانتیزاسیون متناسب با دوربین و نرم‌افزار: برخی دوربین‌ها و نرم‌افزارها مانند فتوشاپ جداول کوانتیزاسیون خاص خود دارند. در واقع، این جداول یک امضا از آن نرم‌افزار و دوربین‌های خاص بشمار می‌رود. نمونه‌ای از جداول کوانتیزاسیون متناسب با دوربین در شکل۴-۳ و جداول کوانتیزاسیون متناسب با نرم‌افزار در شکل۴-۴ نشان داده شده است. همچنین جدول کوانتیزاسیون دوربین‌ها و نرم-افزارهای مختلف استخراج و در پیوست ذکر شده است.

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	1	2	2
1	1	1	1	1	1	2	3
1	1	1	1	2	2	3	3
1	1	1	1	2	3	3	3
1	1	2	2	2	4	3	3
1	1	2	3	4	3	4	3
2	2	3	3	3	4	4	3
2	3	3	3	3	3	3	3

جدول کوانتیزاسیون رنگ

1	1	1	2	3	3	6	6
1	1	1	2	4	3	6	6
1	1	2	2	6	6	6	6
2	2	2	3	6	6	6	6
3	4	6	6	6	6	6	6
3	3	6	6	6	6	6	6
6	6	6	6	6	6	6	6
6	6	6	6	6	6	6	6

شکل ۴-۳: جدول کوانتیزاسیون متناسب با دوربین Canon – Canon PowerShot G1 (Superfine) با نمونه‌برداری رنگ۱×۲

جدول کوانتیزاسیون رنگ

4	5	8	15	20	20	20	20
5	7	10	14	20	20	20	20
8	10	14	20	20	20	20	20
15	14	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

جدول کوانتیزاسیون درخشندگی

4	3	3	4	6	7	8	10
3	3	3	4	5	6	8	10
3	3	3	4	6	9	12	12
4	4	4	7	9	12	12	17
6	5	6	9	12	13	17	20
7	6	9	12	13	17	20	20
8	8	12	12	17	20	20	20
10	10	12	17	20	20	20	20

شکل ۴-۴: جدول کوانتیزاسیون متناسب با نرم‌افزار Photoshop – (Save For Web 070) با نمونه‌برداری رنگ ۱×۱

کدینگ هافمن: پس از کوانتیزاسیون، ضرایب DCT در معرض کدگذاری آنتروپی، معمولاً کدگذاری هافمن قرار می‌گیرند. کدگذاری هافمن یک برنامه کدگذاری با طول متغیر است که مقادیر متناوب را با کدهای کوتاه‌تر کدگذاری می‌کند و مقادیر متناوب کمتری را با کدهای طولانی‌تر رخ می‌دهد.
این شاخص جز بخش‌های اصلی فایل JPEG بشمار می‌رود. قطعه DHT مربوط به کدینگ هافمن است جدول هافمن با شاخص آغازین FF C4 مشخص شده است و معمولاً پس از قطعه DRI قرار می‌گیرد. در حالت فشرده‌سازی Baseline DCT، چهار جدول مربوط به کدینگ هافمن وجود دارد. دو جدول برای حالت DC و AC شدت روشنایی و دو جدول برای حالت DC و AC رنگ. این چهار جدول می‌تواند در چهار قطعه شاخص مجزا باشند یا امکان دارد در یک قطعه شاخص باشند و با شناسه مربوط به هر یک از یکدیگر مجزا شوند. جداول هافمن به سه صورت استاندارد، بهینه و متناسب با نرم‌افزار در سرآیند تصویر JPEG وجود دارند. در ادامه به شرح این جداول می‌پردازیم.
جدول هافمن استاندارد: کدینگ هافمن استاندارد با بررسی چندین هزار تصویر حاصل شده است و حالت بهینه برای غالب تصاویر است. این کدینگ به‌صورت زیر است. لازم به ذکر است که در تصاویر متداول JPEG، چهار جدول مربوط به کدینگ استاندارد هافمن وجود دارد که این چهار جدول می‌توانند در یک یا چهار قطعه مجزا قرار گیرند. در شکل۴-۵ جداول کدینگ هافمن استاندارد در چهار قطعه مجزا نشان داده شده است.

```
ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00
00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a
0b
ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04
04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41
06 13 51 61 07 22 71 14 32 81 91 a1 08 23 42 b1
c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 18 19
1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44
45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64
65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 83 84
85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2
a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9
ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7
d8 d9 da e1 e2 e3 e4 e5 e6 e7 e8 e9 ea f1 f2 f3
f4 f5 f6 f7 f8 f9 fa
ff c4 00 1f 01 00 03 01 01 01 01 01 01 01 01 01
00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a
0b
ff c4 00 b5 11 00 02 01 02 04 04 03 04 07 05 04
04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 12
41 51 07 61 71 13 22 32 81 08 14 42 91 a1 b1 c1
09 23 33 52 f0 15 62 72 d1 0a 16 24 34 e1 25 f1
17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43
44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63
64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82
83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99
9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7
b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5
d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3
f4 f5 f6 f7 f8 f9 fa
```

شکل ۴-۵: جداول کدینگ هافمن استاندارد

تصاویر بندانگشتی در بیش از ۵۰٪ موارد از جدول استاندارد کدینگ هافمن استفاده می‌کنند. البته جدول استاندارد دیگری نیز برای کدینگ هافمن در تصاویر بندانگشتی وجود دارد. این جدول به صورت شکل ۴-۶ است. تصاویر بندانگشتی در اکثر موارد یا از جدول استاندارد یا جدول شکل ۴-۶ استفاده می‌کنند. این قطعه به‌صورت شکل ۴-۶ شامل چهار جدول کدینگ هافمن است که می‌توان این چهار جدول را در چهار قطعه مجزا قرار داد.

```
ff c4 01 3f 00 00 01 05 01 01 01 01 01 01 00 00
00 00 00 00 00 03 00 01 02 04 05 06 07 08 09 0a
0b
01 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00
00 01 00 02 03 04 05 06 07 08 09 0a 0b
10 00 01 04 01 03 02 04 02 05 07 06 08 05 03 0c
33 01 00 02 11 03 04 21 12 31 05 41 51 61 13 22
71 81 32 06 14 91 a1 b1 42 23 24 15 52 c1 62 33
34 72 82 d1 43 07 25 92 53 f0 e1 f1 63 73 35 16
a2 b2 83 26 44 93 54 64 45 c2 a3 74 36 17 d2 55
e2 65 f2 b3 84 c3 d3 75 e3 f3 46 27 94 a4 85 b4
95 c4 d4 e4 f4 a5 b5 c5 d5 e5 f5 56 66 76 86 96
a6 b6 c6 d6 e6 f6 37 47 57 67 77 87 97 a7 b7 c7
d7 e7 f7
11 00 02 02 01 02 04 04 03 04 05 06 07 07 06 05
35 01 00 02 11 03 21 31 12 04 41 51 61 71 22 13
05 32 81 91 14 a1 b1 42 23 c1 52 d1 f0 33 24 62
e1 72 82 92 43 53 15 63 73 34 f1 25 06 16 a2 b2
83 07 26 35 c2 d2 44 93 54 a3 17 64 45 55 36 74
65 e2 f2 b3 84 c3 d3 75 e3 f3 46 94 a4 85 b4 95
c4 d4 e4 f4 a5 b5 c5 d5 e5 f5 56 66 76 86 96 a6
b6 c6 d6 e6 f6 27 37 47 57 67 77 87 97 a7 b7 c7
```

شکل ۴-۶: جداول کدینگ هافمن استاندارد تصویر بندانگشتی

جدول هافمن بهینه: در برخی از تصاویر، فراوانی شدت روشنایی پیکسل‌ها بررسی می‌شوند و بر اساس این فراوانی جدول هافمن تشکیل می‌شود. این جدول بهینه‌ترین حالت برای آن تصویر است. در واقع با این جدول، بیشترین فشرده‌سازی انجام می‌شود. در ۵۵٪ از تصاویر JPEG از جدول هافمن بهینه استفاده می‌شود. در شکل ۴-۷ جداول کدینگ هافمن بهینه در چهار قطعه مجزا نشان داده شده است.

```
ff c4 00 1d 00 00 00 07 01 01 01 00 00 00 00 00
00 00 00 00 00 00 01 03 04 05 06 07 02 08 09
ff c4 00 58 10 00 01 03 02 05 02 04 04 03 06 03
06 02 06 01 15 01 02 03 11 00 04 05 06 12 21 31
41 51 07 13 22 61 08 14 71 81 32 91 a1 15 23 42
b1 c1 d1 52 62 f0 16 24 33 72 e1 f1 82 92 09 17
25 34 43 53 a2 b2 35 63 73 c2 18 27 44 b3 36 54
83 93 a3 d2 26 37 45 55 65 e2
ff c4 00 1c 01 00 02 03 01 01 01 01 00 00 00 00
00 00 00 00 00 01 02 00 03 04 05 06 07 08
ff c4 00 3e 11 00 02 02 01 04 01 03 04 00 04 04
06 02 01 02 07 00 01 02 11 03 04 12 21 31 41 13
22 51 05 32 61 71 14 23 33 81 42 91 a1 b1 06 24
c1 d1 e1 f0 34 52 43 15 62 72 f1 25 82 44 a2 b2
```

شکل ۴-۷: جداول کدینگ هافمن بهینه Canon – Canon PowerShot SX260 HS

جدول هافمن متناسب با نرم‌افزار: برخی نرم‌افزارها مانند فتوشاپ جدول هافمن خاص خود دارند. در واقع، این جدول یک امضا از آن نرم‌افزار و دوربین‌های خاص از جدول هافمن استاندارد استفاده می‌شود اما ترتیب جداول عوض شده است. این کار نیز یک امضا از آن نرم‌افزار بشمار می‌رود. نمونه‌ای از جداول

کدینگ هافمن متناسب با دوربین در شکل ۴-۸ و جداول کدینگ هافمن متناسب با نرم‌افزار فتوشاپ در شکل ۴-۹ نشان داده شده است.

```
ff c4 00 1e 00 00 01 04 03 01 01 01 00 00 00 00
00 00 00 00 00 04 01 02 03 05 00 06 07 08 09 0a
ff c4 00 55 10 00 02 01 03 03 02 04 04 03 06 04
04 04 01 02 17 01 02 03 00 04 11 05 12 21 31 41
06 13 51 61 07 22 71 81 14 32 91 08 23 42 a1 b1
c1 15 52 d1 f0 33 62 e1 f1 16 24 43 72 53 82 92
a2 09 17 34 25 44 63 b2 c2 d2 18 54 73 83 a3 36
64 93 26 27 74 b3 e2
ff c4 00 1c 01 00 02 03 01 01 01 01 00 00 00 00
00 00 00 00 00 01 02 00 03 04 05 06 07 08
ff c4 00 42 11 00 02 02 02 01 03 02 05 01 07 03
03 04 00 03 09 00 01 02 11 03 21 31 04 12 41 22
51 05 13 32 61 71 81 06 14 23 91 a1 b1 c1 42 d1
f0 33 52 e1 15 24 62 f1 07 16 43 a2 b2 25 34 82
92 26 63 72
```

شکل ۴-۸: جداول کدینگ هافمن متناسب با دوربین Canon PowerShot SX700 HS

```
ff c4 01 a2 00 00 00 06 02 03 01 00 00 00 00 00
00 00 00 00 00 07 08 06 05 04 09 03 0a 02 01 00
0b
01 00 00 06 03 01 01 01 00 00 00 00 00 00 00 00
00 06 05 04 03 07 02 08 01 09 00 0a 0b
10 00 02 01 02 05 02 03 04 06 06 05 05 01 03 06
6f 01 02 03 04 11 05 06 21 12 00 07 31 41 13 08
51 22 61 14 71 81 32 91 09 a1 23 f0 c1 42 b1 15
d1 16 e1 f1 52 33 17 24 62 18 43 34 25 82 0a 19
72 53 26 63 92 44 35 a2 54 b2 1a 73 36 c2 d2 27
45 37 46 e2 f2 83 93 a3 b3 64 55 28 c3 d3 29 38
e3 f3 47 48 56 65 2a 39 3a 49 4a 57 58 59 5a 66
74 75 84 85 67 76 77 68 86 87 94 95 a4 a5 b4 b5
c4 c5 d4 d5 e4 e5 f4 f5 96 97 a6 a7 b6 b7 c6 c7
d6 d7 e6 e7 f6 f7 69 6a 78 79 7a 88 89 8a 98 99
9a a8 a9 aa b8 b9 ba c8 c9 ca d8 d9 da e8 e9 ea
f8 f9 fa
11 00 01 03 02 03 04 07 06 03 04 03 06 07 07 01
69 01 02 03 11 00 04 21 05 12 31 06 41 f0 51 61
07 13 22 71 81 91 a1 b1 c1 08 32 d1 14 e1 23 f1
42 15 52 09 16 33 62 d2 72 24 82 c2 92 93 43 17
73 83 a2 b2 63 25 34 53 e2 b3 35 26 44 54 64 45
55 27 0a 84 b4 18 19 1a 28 29 2a 36 37 38 39 3a
46 47 48 49 4a 56 57 58 59 5a 65 66 67 68 69 6a
74 75 76 77 78 79 7a 85 86 87 88 89 8a 94 95 96
97 98 99 9a a3 a4 a5 a6 a7 a8 a9 aa b5 b6 b7 b8
b9 ba c3 c4 c5 c6 c7 c8 c9 ca d3 d4 d5 d6 d7 d8
d9 da e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7
f8 f9 fa
```

شکل ۴-۹: جداول کدینگ هافمن متناسب با نرم‌افزار فتوشاپ Adobe Photoshop CS5 Windows

۵-۲-۴ انطباق امضای تصویر با اطلاعات سرآیند تصویر JPEG

پس از استخراج امضای تصویر از جداول کوانتیزاسیون و کدینگ هافمن، مطابقت امضای تصویر با دادگان کاربردی بررسی خواهد شد.

تطابق جدول کوانتیزاسیون تصویر با جدول کوانتیزاسیون دادگان دوربین بررسی می‌شود و در صورت عدم تطابق، تصویر مشکوک به جعل است. اما اگر جدول کوانتیزاسیون، منطبق بر یک مدل دوربین باشد و با مدل دوربین موجود در اطلاعات دادگان کاربردی یکسان باشد، هویت تصویر اصلی است. همچنین، تطابق جداول کدینگ هافمن تصویر با جداول کدینگ هافمن دادگان دوربین، در صورتی که این جداول بهینه نبوده، بررسی می‌شود. در صورت تطابق، اگر جدول کوانتیزاسیون تصویر با مدل دوربین موجود در اطلاعات دادگان کاربردی یکسان باشد و همچنین با مدل دوربین حاصل از تطابق جداول هافمن یکی باشد، هویت تصویر اصلی است. در صورت عدم تطابق جداول کدینگ هافمن تصویر با جداول کدینگ هافمن دادگان دوربین، در صورتی که این جداول بهینه نبوده، تصویر مشکوک به جعل است.

در برخی از مدل‌های دوربین از جدول هافمن استاندارد استفاده می‌شود. از این‌رو، اگر در تصویر از جدول کدینگ هافمن استاندارد استفاده شده باشد، تصویر در بخش کدینگ هافمن مشکلی ندارد و بررسی بقیه موارد مانند آنچه در پارگراف قبل گفته شد، انجام می‌شود. البته با توجه به این نوع کدینگ هافمن که در برخی از مدل‌های خاص دوربین استفاده می‌شود، مدل دوربین تا حدی مشخص می‌شود و در بررسی‌های بعدی باید به این نکته توجه داشت.

اگر در تصویر از جدول کوانتیزاسیون متناسب با نرم‌افزار استفاده شده باشد، تصویر مشکوک به جعل است.

در برخی از مدل‌های دوربین از جدول کوانتیزاسیون استاندارد استفاده شده است. از این‌رو، اگر در تصویر از جدول کوانتیزاسیون استاندارد استفاده شده باشد، تصویر در این بخش مشکلی ندارد و جداول کدینگ هافمن و دادگان کاربردی مانند بخش قبل، بررسی خواهند شد. البته با توجه به جدول کوانتیزاسیون می‌توان مدل دوربین را مشخص کرد و در بررسی‌های بعدی این مدل را مبنا قرار داد.

ممکن است اطلاعات سرآیند تصویر ویرایش شود به این صورت که ماتریس کوانتیزاسیون، جداول کدینگ هافمن، اطلاعات دادگان کاربردی نرم‌افزاری و تصویر بندانگشتی با رعایت ترتیب بخش‌های مختلف سرآیند تصویر، از تصویر اصلی استخراج شوند و جایگزین اطلاعات سرآیند تصویر ویرایش شده شوند. در این صورت تشخیص هویت تصویر با این روش امکان‌پذیر نیست. اما اگر هر یک از بخش‌های موجود در سرآیند تصویر مانند تصویر اصلی تغییر داده نشود، تشخیص هویت تصویر با این روش امکان-پذیر است.

۴-۳ داده‌کاوی اطلاعات سرآیند

کار داده‌کاوی بر روی پایگاه داده تولیدی انجام شده است. در این کار سرآیندهای اختیاری پر کاربرد و پارامترهای پر کاربرد استخراج، مطالعه و بررسی شدند. این داده‌کاوی در این راستا انجام شده تا مشخص شود کدام پارامترهای دادگان کاربردی و دیگر پارامترهای سرآیند حیاتی هستند و در صورت عدم وجود آن‌ها تصویر مشکوک است.

۴-۴ ترتیب متداول بخش‌های مختلف در فایل JPEG

در فصل سوم، ترتیب اجزاء اصلی فایل JPEG بررسی شد. در این فصل، خلاصه‌ای از ترتیب کلی قطعات شاخص در فایل‌های متداول JPEG آورده شده است که در ادامه قابل مشاهده است.

SOI: این قطعه شاخص در ابتدای فایل JPEG می‌آید (با شاخص آغازین FF D8).

APP_0 تا APP_F: یک یا چند قطعه مربوط به دادگان کاربردی (با شاخص آغازین FFE0 تا FFEF) پس از SOI می‌آیند. لازم به ذکر است که این دادگان اختیاری هستند و در صورت عدم وجود آن‌ها مشکلی برای تصویر ایجاد نمی‌شود.

DQT: یک یا دو قطعه مربوط به ماتریس کوانتیزاسیون پس از دادگان کاربردی می‌آیند. ماتریس‌های کوانتیزاسیون شامل دو ماتریس درخشندگی و رنگ هستند که پس از شاخص آغازین FF DB اندازه قطعه می‌آید و پس از آن یک بایت برای مشخص کردن نوع ماتریس کوانتیزاسیون (رنگ یا درخشندگی) می‌آید.

البته باید توجه داشت که ابتدا ماتریس کوانتیزاسیون درخشندگی می‌آید. نکته‌ای که در رابطه با ماتریس‌های کوانتیزاسیون وجود دارد، تعداد قطعات مربوط به آن است. همان‌گونه که اشاره شد یک یا دو قطعه مربوط به ماتریس کوانتیزاسیون در تصاویر JPEG وجود دارد که این قطعات از بخش‌های اصلی فایل JPEG بشمار می‌رود. اگر در فایل JPEG یک قطعه مربوط به ماتریس کوانتیزاسیون وجود داشت هر دو ماتریس کوانتیزاسیون درخشندگی و رنگ در این قسمت وجود دارند و با توجه به شناسه‌ی آن (صفر یا یک) امکان شناسایی آن وجود دارد. اگر دو قطعه مربوط به ماتریس کوانتیزاسیون وجود داشت، ابتدا ماتریس کوانتیزاسیون درخشندگی با شناسه صفر و پس از آن ماتریس کوانتیزاسیون رنگ با شناسه یک می‌آید.

SOF: پس از قطعه مربوط به ماتریس‌های کوانتیزاسیون قطعه شاخص سرآیند ابتدایی فایل JPEG می‌آید. این قطعه جزء بخش‌های اصلی فایل JPEG بشمار می‌رود. البته این قطعه همان‌گونه که بیان شد می‌تواند با توجه به نوع کدینگ و فشرده‌سازی استفاده شده در فایل، از شاخص‌های ابتدایی مختلفی پیروی کند که در این رساله نوع متداول فایل JPEG با شاخص آغازین FF C0 مورد ارزیابی قرار گیرد.

DRI: این قطعه مربوط به تعریف شروع مجدد فاصله زمانی است (با شاخص آغازین FF DD) و بخش اختیاری در فایل‌های JPEG است. این بخش معمولاً پس از سرآیند ابتدایی فایل JPEG می‌آید و اندازه

این بخش ثابت و چهار بایت است که دو بایت اول آن اندازه این بخش را مشخص می‌کند. این بخش فاصله‌ی بین نشانه‌های RST_n در ماکرو بلاک‌ها را تعیین می‌کند.
قطعه‌ی DRI اگر چه جزء قطعه‌های اختیاری است اما وقتی از آن استفاده می‌شود جزو قطعات اصلی به شمار می‌آید و حذف آن تصویر را مخدوش می‌کند. از این‌رو این قطعه و قطعات مربوط به آن یعنی قطعات RST را نمی‌توان حذف کرد. اما قطعات اختیاری دیگر را می‌توان حذف کرد و با حذف آن‌ها تصویر مخدوش نمی‌شود.
DHT: این قطعه مربوط به کدینگ هافمن است (با شاخص آغازین FF C4) و معمولاً پس از قطعه DRI قرار می‌گیرد. در حالت فشرده‌سازی Baseline DCT، چهار جدول مربوط به کدینگ هافمن وجود دارد. این چهار جدول می‌تواند در چهار قطعه شاخص مجزا باشند یا امکان دارد در یک قطعه شاخص باشند و با شناسه‌ی مربوط به هر یک از یکدیگر مجزا شوند. این شاخص جز بخش‌های اصلی فایل JPEG بشمار می‌رود.
SOS: این قطعه، قطعه شاخص اسکن داده فایل است و پس از قطعه DHT می‌آید (با شاخص آغازین FF DA). پس از این قطعه اطلاعات مربوط به تصویر اصلی بدون هیچ‌گونه شاخص آغازینی می‌آیند. در واقع بین این قطعه و داده اصلی تصویر شاخصی وجود ندارد.
RST: از جمله شاخص‌های پر کاربردی که در بخش اسکن داده از آن استفاده می‌شود، شاخص خروج از بازه‌های شروع مجدد است (با شاخص FFD0 تا FFD7). این شاخص‌ها در صورت فعال بودن DRI فعال می‌باشند و در صورت عدم DRI، در تصاویر JPEG وجود ندارند. این شاخص‌ها در میان داده اصلی فایل قرار می‌گیرند و پس از این شاخص‌ها اسکن داده دوباره فعال می‌شود. ترتیب این شاخص‌ها در یک فایل از FFD0 تا FFD7 است و نقطه‌ی قرار گیری آن‌ها با توجه به اندازه‌ای است که در قطعه DRI وجود دارد.
EOI: انتهای فایل JPEG با این شاخص مشخص می‌شود که شامل FF D9 است.

۴-۵ تهیه دادگان و داده‌کاوی آن‌ها

دادگانی بالغ بر ۲۰۰ هزار تصویر JPEG از دوربین‌های مختلف و سایت‌های عکس‌برداری حرفه‌ای توسط پژوهشگران این پژوهش جمع‌آوری شده است و نتایج داده‌کاوی بر روی این تصاویر بررسی و گزارش شدند. این نتایج در فصل بعد به‌تفصیل بیان می‌شوند.

۴-۶ تولید دادگانی از سرآیندها

برای تولید دادگانی ارزشمند از سرآیندهای تصاویر JPEG، ابتدا از پایگاه داده نرم‌افزار JPEGSNOOP استفاده شده است. پارامترهای مربوط به ماتریس‌های کوانتیزاسیون و زیر نمونه‌برداری برای هر مدل دوربین از این پایگاه داده استخراج شد. در راستای ارتقا پایگاه داده، سرآیند تمام تصاویر تهیه شده،

استخراج شدند و به پایگاه داده قبلی اضافه شدند. در این بخش پارامترهای وجود تصویر بندانگشتی، ابزارهای تولید کننده تصویر و تصویر بندانگشتی، مدل دوربین، ماتریس‌های کوانتیزاسیون تصویر اصلی و تصویر بندانگشتی، کدینگ هافمن تصویر و تصویر بندانگشتی، زیر نمونه‌برداری تصویر و تصویر بندانگشتی، اندازه تصویر و تصویر بندانگشتی و استاندارد EXIF استخراج و به پایگاه داده اضافه شدند. همچنین سرآیند خام (خروجی نرم‌افزار JPEGSNOOP) نیز در پایگاه داده ذخیره شد تا در صورت لزوم از آن استفاده شود.

۴-۷ جمع‌بندی

در این فصل با توجه به اهمیت آشکارسازی جعل در جرم‌شناسی روش جدیدی برای بهبود عملکرد احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه شد. به توضیح و بررسی روش پیشنهادی و نوآوری‌های این رساله پرداخته شد.

روش پیشنهادی از پنج مرحله اصلی تشکیل شده بود که شامل:

۱) بررسی و استخراج اطلاعات مهم از سرآیند تصاویر JPEG
۲) در صورت عدم وجود دادگان کاربردی یا فقط وجود JFIF، تصویر مشکوک به جعل است.
۳) بررسی و استخراج اطلاعات مهم دادگان کاربردی (نرم‌افزاری)
۴) استخراج امضای تصویر از جدول کوانتیزاسیون و کدینگ هافمن
۵) انطباق امضای تصویر با اطلاعات سرآیند تصویر JPEG

در این فصل روش پیشنهادی برای پیاده‌سازی طرح بررسی شد و راهکارهای اجرایی برای آن پیشنهاد شد. در فصل بعدی پیاده‌سازی و ارزیابی نتایج حاصل از روش احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند، مورد بررسی قرار می‌گیرد

فصل ۵ : پیاده‌سازی و ارزیابی نتایج

۵-۱ مقدمه

با ظهور دوربین‌های جدید، تلفن‌های هوشمند[۱] و تبلت‌ها[۲] تعداد تصاویر دیجیتال به‌طور تصاعدی افزایش یافته و رسانه‌های اجتماعی مانند فیس‌بوک،[۳] اینستاگرام[۴] و توییتر[۵] بیشتر در توزیع آن‌ها نقش داشته‌اند [۴]. تصاویر دیجیتال برای نمایش زمان و مکان، به‌عنوان مدرک به دادگاه ارائه می‌شوند و یکی از مدارک مهم جرم هستند (به‌عنوان مثال، در پورنوگرافی[۶] کودکان، پرونده‌های فیلم دزدی دریایی یا ادعاهای بیمه) [۲۸]. به دلیل دوستی بسیار زیاد کاربران به ابزارهای پردازش چندرسانه‌ای (به‌عنوان مثال فتوشاپ،[۷] گیمپ،[۸] ویرایش تصاویر کورل،[۹] نمایش تصاویر[۱۰] و برنامه‌های گوشی‌های هوشمند مانند اسنپ سید،[۱۱] پیکسلر[۱۲] اطلاعات سرآیند تصویر به‌راحتی توسط افراد قابل تغییر و حذف هستند. بنابراین، اطلاعات سرآیند تصویر، قابل اعتماد نیستند [۴, ۴۶].

در این فصل، ارزیابی نتایج حاصل از پیاده‌سازی روش پیشنهادی مورد بررسی قرار می‌گیرد. در ابتدای این فصل به معرفی پایگاه داده مورد استفاده می‌پردازیم. مجموعه داده استفاده شده از تصاویر دوربین-های مختلف و سایت‌های عکس‌برداری حرفه‌ای توسط پژوهشگران این پژوهش جمع‌آوری شده است.
در این رساله به داده‌کاوی در پایگاه داده بر روی پارامترهای پر کاربرد سرآیند تصویر JPEG می‌پردازیم. برای نشان دادن اهمیت انتخاب هر یک از پارامترهای مورد استفاده فراوانی دادگان کاربردی مختلف در دادگان بررسی می‌شود.
در ادامه این فصل نگاهی اجمالی به انواع معیارهای ارزیابی کیفیت احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند خواهیم داشت و معیارهای مورد استفاده در این پژوهش معرفی می‌شوند. در نهایت با استفاده از معیارهای ارزیابی مورد نظر، میزان کیفیت نتایج حاصل از الگوریتم احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند بررسی می‌شود.

---

۱. smartphones
۲. tablets
۳. Facebook
۴. Instagram
۵. Twitter
۶. pornography
۷. Adobe Photoshop
۸. Gimp
۹. Corel Paint Shop
۱۰. Irfan View
۱۱. Snapseed
۱۲. Pixlr

۵-۲ مجموعه داده

دادگانی بالغ بر ۲۰۰ هزار تصویر JPEG از دوربین‌های مختلف و سایت‌های عکس‌برداری حرفه‌ای توسط پژوهشگران این پژوهش جمع‌آوری شده است:

- دوربین PENTAX با مدل
  - PENTAX Optio S5i
- دوربین Canon با مدل‌های
  - Canon EOS-1Ds Mark II (fine)
  - Canon PowerShot G1 (Superfine)
  - Canon EOS-1D Mark II N (fine)
  - Canon DIGITAL IXUS 40
  - Canon EOS-1D(fine)، (superfine)
  - Canon PowerShot SD700 IS (fine)
  - Canon PowerShot S30 (video)
- دوربین NIKON با مدل‌های
  - COOLPIX P2 (FINE)،
  - E8400 (FINE)، COOLPIX P3 (FINE)،
  - COOLPIX P4 ()، COOLPIX L12 (FINE)،
  - COOLPIX S10 (FINE)
- دوربین SONY با مدل
  - DSC-R1 (fine)، DSC-H9 (variable)
- دوربین FUJIFILM با مدل‌های
  - FinePix F700 (normal)،
  - FinePix S5000 (normal)،
  - FinePix F40fd()
- سایت‌های عکس‌برداری حرفه‌ای
  - Flickr
  - Pixabay
  - unsplash

۵-۳ ابزارهای مورد استفاده برای پیاده‌سازی

از چهار نرم‌افزار قوی JPEGSNOOP، EXIFTOOL، EXIV2 و JHEAD برای استخراج، تولید و ویرایش سرآیند JPEG استفاده شده است. در فصل قبل هر یک از این نرم‌افزارها به‌اختصار معرفی شده‌اند. از زبان برنامه‌نویسی PHP و بانک اطلاعاتی SQLite برای پیاده‌سازی استفاده شده است.

۵-۴ ارزیابی نتایج

برای ارزیابی نتایج از چندین نرم‌افزار معروف ویرایشگر تصویر و نرم‌افزار برنامه‌نویسی استفاده شده است و تصاویر در این نرم‌افزارها با پارامترهای مختلف فشرده‌سازی JPEG ذخیره شده است. که نتایج ارزیابی در ادامه آورده شده است.

۵-۴-۱ تفاوت تصویر اصلی با تصویر ذخیره شده در نرم‌افزار فتوشاپ[۱]

تصویر اصلی دارای اطلاعات دادگان کاربردی JFIF به‌صورت شکل ۵-۱ است

```
*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length     = 16
  Identifier = [JFIF]
  version    = [1.1]
  density    = 180 x 180 DPI (dots per inch)
  thumbnail  = 0 x 0
```

شکل ۵-۱: اطلاعات دادگان کاربردی JFIF تصویر اصلی

اطلاعات JFIF با ذخیره تصویر در نرم‌افزار ویرایشگر فتوشاپ حذف می‌شود. نام نرم‌افزار ویرایش تصویر به‌صورت شکل ۵-۲ به اطلاعات بخش EXIF اضافه شده است.

```
EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000A
  [Make                              ] = "Canon"
  [Model                             ] = "Canon PowerShot SX260 HS"
  [Orientation                       ] = 1 = Row 0: top, Col 0: left
  [XResolution                       ] = 1800000/10000
  [YResolution                       ] = 1800000/10000
  [ResolutionUnit                    ] = Inch
  [Software                          ] = "Adobe Photoshop CC 2017 (Windows)"
```

شکل ۵-۲: بخشی از اطلاعات EXIF تصویر مشکوک به جعل

قطعه APP13 با شاخص کاربردی FFED، قطعه APP2 با شاخص کاربردی FFE2 و قطعه APP14 با شاخص کاربردی FFEE به‌صورت شکل ۵-۳ دادگان کاربردی (نرم‌افزاری) است که به منظور افزودن ابر داده‌ها به اطلاعات سرآیند تصویر مشکوک به جعل اضافه شده است.

۱. Photoshop

```
*** Marker: APP13 (xFFED) ***
  OFFSET: 0x000021C5
  Length          = 9782
  Identifier      = [Photoshop 3.0]
      8BIM: [0x0404] Name="" Len=[0x001F] DefinedName="IPTC-NAA record"
*** Marker: APP2 (xFFE2) ***
  OFFSET: 0x00005683
  Length          = 3160
  Identifier      = [ICC_PROFILE]
    ICC Profile:
*** Marker: APP14 (xFFEE) ***
  OFFSET: 0x000062DD
  Length            = 14
  DCTEncodeVersion  = 100
  APP14Flags0       = 0
  APP14Flags1       = 0
  ColorTransform    = 1 [YCbCr]
```

شکل ۵-۳: اطلاعات دادگان کاربردی تصویر مشکوک به جعل

اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. شاخص ماتریس کوانتیزاسیون رنگ حذف شده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار فتوشاپ استفاده شده است. البته در نرم‌افزار فتوشاپ می‌توان تصویر JPEG را با کیفیت‌های مختلف ذخیره کرد که هر کیفیت یک ماتریس کوانتیزاسیون مربوط به خود دارد.

قطعه DRI به‌صورت شکل ۵-۴ به اطلاعات سرآیند تصویر مشکوک به جعل اضافه شده است.

```
*** Marker: DRI (Restart Interval) (xFFDD) ***
  OFFSET: 0x00006386
  Length      = 4
  interval    = 175
```

شکل ۵-۴: قطعه DRI در اطلاعات سرآیند تصویر مشکوک به جعل

اعداد جداول هافمن در خروجی نرم‌افزار فتوشاپ تغییر کرده است که به دلیل انتخاب جدول هافمن متناسب با نرم‌افزار در این نرم‌افزار است. در برخی از نرم‌افزارها یا دوربین‌های خاص، از جداول هافمن خاصی استفاده می‌شود که این جداول بهینه یا استاندارد نیستند. به این جداول، جداول متناسب با نرم‌افزار گفته می‌شود. در تصویر اصلی، چهار جدول هافمن در چهار قطعه شاخص مجزا قرار داشت. اما با ذخیره تصویر در نرم‌افزار ویرایشگر فتوشاپ، چهار جدول در یک قطعه شاخص قرار گرفت. همچنین در این نرم‌افزار، ترتیب قرارگیری جداول هافمن در مقایسه با تصویر اصلی تغییر کرده است. در تصویر حاصل از نرم‌افزار فتوشاپ قطعات APP13 و APP14 و DRI به‌صورت شکل ۵-۵ به اطلاعات بخش تصویر بندانگشتی اضافه شده است.

```
* Embedded Thumb Marker: APP13
  Length = 12

* Embedded Thumb Marker: APP14
  Length = 14

* Embedded Thumb Marker: DRI
  Length = 4
```

شکل ۵-۵: قطعه APP13 و APP14 و DRI در اطلاعات سرآیند تصویر بندانگشتی مشکوک به جعل

همچنین در تصویر حاصل از نرم‌افزار فتوشاپ، اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تصویر بندانگشتی تغییر کرده است.

۵-۴-۲ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Paint

با ذخیره تصویر در این نرم‌افزار، اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر ذخیره شده در این نرم‌افزار، از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است.

کدهای جدول هافمن برای حالت DC و AC شدت روشنایی و حالت DC و AC رنگ تغییر کرده است. در تصویر اصلی از جداول کدینگ هافمن بهینه استفاده شده است و در تصویر مشکوک به جعل از جداول کدینگ هافمن استاندارد استفاده شده است.

اطلاعات بخش تصویر بندانگشتی در تصویر اصلی به‌صورت شکل ۵-۶ بوده است که با ذخیره تصویر در نرم‌افزار Paint از اطلاعات سرآیند تصویر حذف شده است.

```
*** Embedded JPEG Thumbnail ***
  Offset: 0x00001612
  Length: 0x0000183B (6203)

  * Embedded Thumb Marker: SOI

  * Embedded Thumb Marker: DQT
    Length = 132
    ----
    Precision=8 bits
    Destination ID=0 (Luminance, typically)
```

شکل ۵-۶: اطلاعات بخش تصویر بندانگشتی در تصویر اصلی

۵-۴-۳ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار متلب[۱]

قطعه COM به‌صورت شکل ۵-۷ با ذخیره تصویر در نرم‌افزار متلب به اطلاعات سرآیند تصویر مشکوک به جعل اضافه شده است.

۱. Matlab

```
*** Marker: COM (Comment) (xFFFE) ***
  OFFSET: 0x00000014
  Comment length = 14
    Comment=My JPEG file
```

شکل ۵-۷: قطعه COM در اطلاعات سرآیند تصویر مشکوک به جعل

قطعه APP1 با شاخص کاربردی FFE1 به‌صورت شکل ۵-۸ اطلاعات مربوط به EXIF در اطلاعات سرآیند تصویر اصلی بوده است که با ذخیره تصویر با نرم‌افزار متلب از سرآیند تصویر JPEG مشکوک به جعل حذف شده است.

```
*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000014
  Length           = 13822
  Identifier       = [Exif]
  Identifier TIFF  = 0x[49492A00 08000000]
  Endian           = Intel (little)
  TAG Mark x002A   = 0x002A

  EXIF IFD0 @ Absolute 0x00000026

*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00003614
  Length           = 4094
  Identifier       = [http://ns.adobe.com/xap/1.0/]
    XMP =
          |<?xpacket begin='□ª□' id='W5M0MpCehiHzr
```

شکل ۵-۸: قطعه APP1 در اطلاعات سرآیند تصویر اصلی

اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ در خروجی نرم‌افزار متلب، تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است.

کدهای جدول هافمن برای حالت DC و AC شدت روشنایی و برای حالت DC و AC رنگ تغییر کرده است. در نرم‌افزار متلب از جداول کدینگ هافمن استاندارد استفاده شده است. در خروجی نرم‌افزار متلب، اطلاعات سرآیند تصویر بندانگشتی از سرآیند تصویر حذف شده است.

۵-۴-۴ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار ACDSee Pro

با ذخیره تصویر در این نرم‌افزار اطلاعات JFIF از سرآیند تصویر حذف شده است. قطعه APP2 با شاخص کاربردی FFE2 به اطلاعات سرآیند تصویر اضافه شده است. ترتیب قرارگیری قطعات تغییر کرده است. قطعه SOF بعد از قطعه DQT قرار گرفته است. همچنین اعداد ماتریس کوانتیزاسیون رنگ و درخشندگی تغییر کرده است و شاخص ماتریس کوانتیزاسیون رنگ حذف شده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است.

مقادیر جداول هافمن تغییر کرده است. چهار جدول در چهار قطعه شاخص مجزا بود که با ذخیره تصویر در نرم‌افزار ویرایشگر چهار جدول در یک قطعه شاخص قرار گرفته‌اند. در تصویر اصلی و تصویر حاصل از نرم‌افزار، از جداول کدینگ هافمن بهینه استفاده شده است که البته پارامتری مشکوک نیست. قطعه APP1 به اطلاعات تصویر بندانگشتی اضافه شده است. مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تصویر بندانگشتی تغییر کرده است.

۵-۴-۵ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Program4pc-Photo Editor

قطعه APP1 با شاخص کاربردی FFE1، اطلاعات مربوط به EXIF در اطلاعات سرآیند تصویر اصلی بوده است که با ذخیره تصویر در این نرم‌افزار از سرآیند تصویر حذف شده است. اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است.

جداول کدینگ هافمن تغییر کرده است. در تصویر اصلی و تصویر حاصل از نرم‌افزار، از جداول کدینگ هافمن بهینه استفاده شده است.

همچنین در خروجی این نرم‌افزار، اطلاعات سرآیند تصویر بندانگشتی از سرآیند تصویر حذف شده است.

۵-۴-۶ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار GIMP

در تصویر خروجی نرم‌افزار GIMP، اعداد ماتریس کوانتیزاسیون درخشندگی تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است. البته در نرم‌افزار GIMP می‌توان تصویر JPEG را با کیفیت‌های مختلف ذخیره کرد که هر کیفیت یک ماتریس کوانتیزاسیون مربوط به خود دارد.

تصویر اصلی از حالت کدینگ رشته‌ای معمولی (Baseline) مبتنی بر DCT استفاده کرده است که در این نرم‌افزار به حالت کدینگ تصاعدی (مرحله به مرحله) مبتنی بر DCT به‌صورت شکل ۵-۹ تغییر کرده است.

```
*** Marker: SOF2 (Progressive DCT, Huffman) (xFFC2) ***
  OFFSET: 0x00003C05
  Frame header length = 17
  Precision = 8
  Number of Lines = 1050
  Samples per Line = 1400
```

شکل ۵-۹: حالت کدینگ تصاعدی

در این نرم‌افزار، قطعه APP0 به سرآیند تصویر بندانگشتی اضافه شده است. اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تصویر بندانگشتی تغییر کرده است. شاخص جدول کوانتیزاسیون رنگ به تصویر بندانگشتی اضافه شده است. سه شاخص جدول هافمن به اطلاعات بخش تصویر بندانگشتی اضافه شده است.

۵-۴-۷ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Corel AfterShot Pro

اطلاعات JFIF از سرآیند تصویر حذف شده است. شاخص اول EXIF و پارامترهای آن حذف شده است. پارامترهای نام دوربین و مدل دوربین به‌صورت شکل ۵-۱۰ از اطلاعات EXIF حذف شده است.

```
EXIF IFD0 @ Absolute 0x00000026
  Dir Length = 0x000A
  [ImageDescription                    ] = "
  [Make                                ] = "Canon"
  [Model                               ] = "Canon PowerShot SX260 HS"
  [Orientation                         ] = 1 = Row 0: top, Col 0: left
```

شکل ۵-۱۰: بخشی از اطلاعات EXIF تصویر اصلی

قطعه APP2 به سرآیند تصویر اضافه شده است. مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است. البته در این نرم‌افزار می‌توان تصویر JPEG را با کیفیت‌های مختلف ذخیره کرد که هر کیفیت یک ماتریس کوانتیزاسیون مربوط به خود دارد.

مقادیر جدول هافمن در خروجی این نرم‌افزار تغییر کرده است. در تصویر اصلی از جداول کدینگ هافمن بهینه استفاده شده است و در تصویر مشکوک به جعل از جداول کدینگ هافمن استاندارد استفاده شده است. همچنین اطلاعات سرآیند تصویر بندانگشتی از سرآیند تصویر حذف شده است.

۵-۴-۸ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Capture NX

در تصویر حاصل از این نرم‌افزار، نام نرم‌افزار ویرایشگر "Capture NX 2.4.7 W" به‌صورت شکل ۵-۱۱ به سرآیند تصویر اضافه شده است.

```
EXIF IFD0 @ Absolute 0x00000026
  Dir Length = 0x000B
  [ImageDescription                ] = "
  [Make                            ] = "Canon"
  [Model                           ] = "Canon PowerShot SX260 HS"
  [Orientation                     ] = 1 = Row 0: top, Col 0: left
  [XResolution                     ] = 180/1
  [YResolution                     ] = 180/1
  [ResolutionUnit                  ] = Inch
  [Software                        ] = "Capture NX 2.4.7 W"
```

شکل ۵-۱۱: بخشی از اطلاعات EXIF تصویر مشکوک به جعل

در تصاویر خروجی این نرم‌افزار، قطعه APP2 به سرآیند تصویر اضافه شده است. مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. شاخص و پارامترهای ماتریس کوانتیزاسیون رنگ حذف شده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است. البته در این نرم‌افزار می‌توان تصویر JPEG را با کیفیت‌های مختلف ذخیره کرد که هر کیفیت یک ماتریس کوانتیزاسیون مربوط به خود دارد.

تصویر اصلی، دارای چهار جدول هافمن در چهار قطعه شاخص مجزا است. اما با ذخیره تصویر در این نرم‌افزار ویرایشگر چهار جدول در یک قطعه شاخص قرار گرفتند. در تصویر خروجی این نرم‌افزار، کدهای جدول هافمن برای حالت DC و AC شدت روشنایی و برای حالت DC و AC رنگ تغییر کرده است. در تصویر اصلی از جداول کدینگ هافمن بهینه استفاده شده است و در تصویر خروجی این نرم‌افزار از جداول کدینگ هافمن استاندارد استفاده شده است.

در تصویر حاصل از این نرم‌افزار، قطعه DRI با شاخص ابتدایی xFFDD و پارامترهای آن به اطلاعات سرآیند تصویر اضافه شده است. همچنین، مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تصویر بندانگشتی تغییر کرده است. قطعه DRI و پارامترهای آن به اطلاعات سرآیند تصویر بندانگشتی اضافه شده است.

۵-۴-۹ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Corel Painter

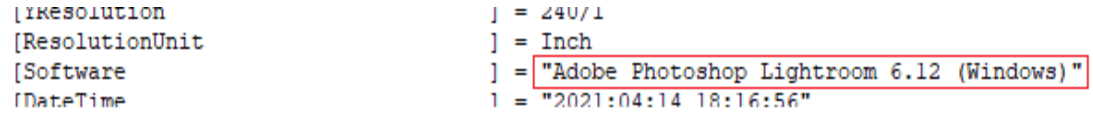
در تصویر حاصل از این نرم‌افزار، شاخص و پارامترهای EXIF حذف شده است. همچنین، اعداد ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر مشکوک به جعل از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است. البته در این نرم‌افزار می‌توان تصویر JPEG را با کیفیت‌های مختلف ذخیره کرد که هر کیفیت یک ماتریس کوانتیزاسیون مربوط به خود دارد. در تصویر حاصل از این نرم‌افزار، ماتریس کوانتیزاسیون رنگ دارای شاخص نیست.

در تصویر خروجی این نرم‌افزار، کدهای جدول هافمن برای حالت DC و AC شدت روشنایی و برای حالت DC و AC رنگ تغییر کرده است. در تصویر اصلی و تصویر حاصل از این نرم‌افزار، از جداول

کدینگ هافمن بهینه استفاده شده است که پارامتری مشکوک نیست. اطلاعات سرآیند تصویر بندانگشتی از سرآیند تصویر حذف شده است.
در تصاویر حاصل از این نرم‌افزار، ترتیب برخی از قطعات تغییر کرده است و قطعه SOF قبل از قطعه DHT قرار گرفته است.

۵-۴-۱۰ مقایسه تصویر اصلی با تصویر ذخیره شده در نرم‌افزار Adobe Photoshop Light room

در تصویر حاصل از این نرم‌افزار، اطلاعات JFIF از سرآیند تصویر حذف شده است. نام نرم‌افزار ویرایشگر "Adobe Photoshop Lightroom 6.12 (Windows)" به‌صورت شکل ۵-۱۲ به اطلاعات EXIF اضافه شده است.



شکل ۵-۱۲: بخشی از اطلاعات EXIF تصویر مشکوک به جعل

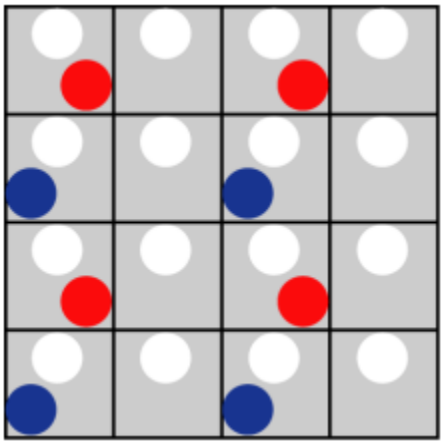
در تصاویر حاصل از این نرم‌افزار، قطعه APP13 و APP2 به اطلاعات بخش سرآیند اضافه شده است. مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تغییر کرده است. شاخص و پارامترهای ماتریس کوانتیزاسیون رنگ حذف شده است. در تصویر اصلی از ماتریس کوانتیزاسیون متناسب با دوربین استفاده شده است و در تصویر حاصل از این نرم‌افزار، از ماتریس کوانتیزاسیون متناسب با نرم‌افزار استفاده شده است.
در تصاویر حاصل از این نرم‌افزار، قطعه DRI و APP14 به اطلاعات سرآیند تصویر اضافه شده است. در تصویر اصلی، چهار جدول در چهار قطعه شاخص مجزا قرار داشته است که با ذخیره تصویر در نرم‌افزار ویرایشگر چهار جدول در یک قطعه شاخص قرار گرفته‌اند. مقادیر جداول هافمن و ترتیب قرارگیری جداول هافمن در تصویر حاصل از نرم‌افزار، تغییر کرده است.
در تصویر اصلی و تصویر حاصل از نرم‌افزار، از جداول کدینگ هافمن بهینه استفاده شده است که پارامتری مشکوک به شمار نمی‌رود.
در تصویر حاصل از نرم‌افزار، مقادیر ماتریس کوانتیزاسیون درخشندگی و رنگ تصویر بندانگشتی تغییر کرده است. قطعه DRI و APP14 به اطلاعات تصویر بندانگشتی اضافه شده است.

۵-۵ داده‌کاوی اطلاعات سرآیند:

برای داده‌کاوی بر روی پایگاه داده تولیدی ابتدا دادگان نسبتا مناسبی از تصاویر JPEG تهیه شد. سپس داده‌کاوی بر روی پارامترهای سرآیند انجام گرفت. نتایج داده‌کاوی در پایگاه داده روی پارامترهای پر کاربرد به شرح زیر است:

۵-۵-۱ داده‌کاوی بر روی زیر نمونه‌برداری در پایگاه داده

چشم انسان به مولفه‌های رنگی در قیاس با مولفه خاکستری حساسیت کمتری دارد. از این‌رو، در فرآیند انکدینگ JPEG تمام پیکسل‌های خاکستری لحاظ می‌شوند. اما از پیکسل‌های رنگ خاکستری و قرمز نمونه‌برداری می‌شود. در شکل ۵-۱۳ نمونه‌برداری ۴:۲:۰ (معادل ۴:۱:۱) نشان داده شده است. همان‌طور که مشاهده می‌شود، از تمام مولفه‌های خاکستری نمونه‌برداری شده اما از مولفه‌های رنگ قرمز و آبی از هر چهار پیکسل تنها یک نمونه لحاظ شده است.



شکل ۵-۱۳: نمونه‌برداری ۴:۲:۰

پارامتر نمونه‌برداری در سرآیند تصویر JPEG تعریف شده است. داده‌کاوی این پارامتر روی تصاویر پایگاه داده انجام شده است. تصاویر پایگاه داده شامل ۲۱۱ هزار تصویر هستند. ۶۰ هزار از این تصاویر از نرم‌افزار فتوشاپ استفاده کرده‌اند. همان‌گونه که بیان شد، در نهان‌نگاری از تصاویر پاک استفاده می‌شود که این تصاویر خروجی دوربین‌ها هستند. از این‌رو نتایج داده‌کاوی روی تصاویر خروجی دوربین‌ها حائز اهمیت است. از این‌رو نتایج داده‌کاوی در کل دادگان بدون فتوشاپ به‌طور مجزا، بیان شده است.

در جدول ۵-۱، فراوانی نمونه‌برداری برای مولفه‌های رنگ آبی و قرمز به ازای چهار پیکسل در کل دادگان و در دادگان بدون فتوشاپ به‌طور مجزا، نشان داده شده است.

جدول ۵-۱: شرایط نمونه‌برداری

شرایط نمونه‌برداری در تمام تصاویر پایگاه‌داده		شرایط نمونه‌برداری در تصاویری که از نرم‌افزار فتوشاپ است	
فراوانی	زیر نمونه‌برداری	فراوانی	زیر نمونه‌برداری
۱۳۸۱۴۸	۲×۲	۱۲۰۵۴۴	۲×۲
۶۳۵۳۷	۱×۱	۲۰۹۱۹	۱×۱
۷۴۷۰	۲×۱	۶۹۱۹	۲×۱
۱۰۵۳	۱×۲	۸۲۴	۱×۲
۷۵۵	Gray	۴۰۸	Gray
۸۱	؟×؟	۱۹	؟×؟
۳	۴×۱	۳	۴×۱
۱	۴×۲	۱	۴×۲
۱	۲×۴	۱	۲×۴

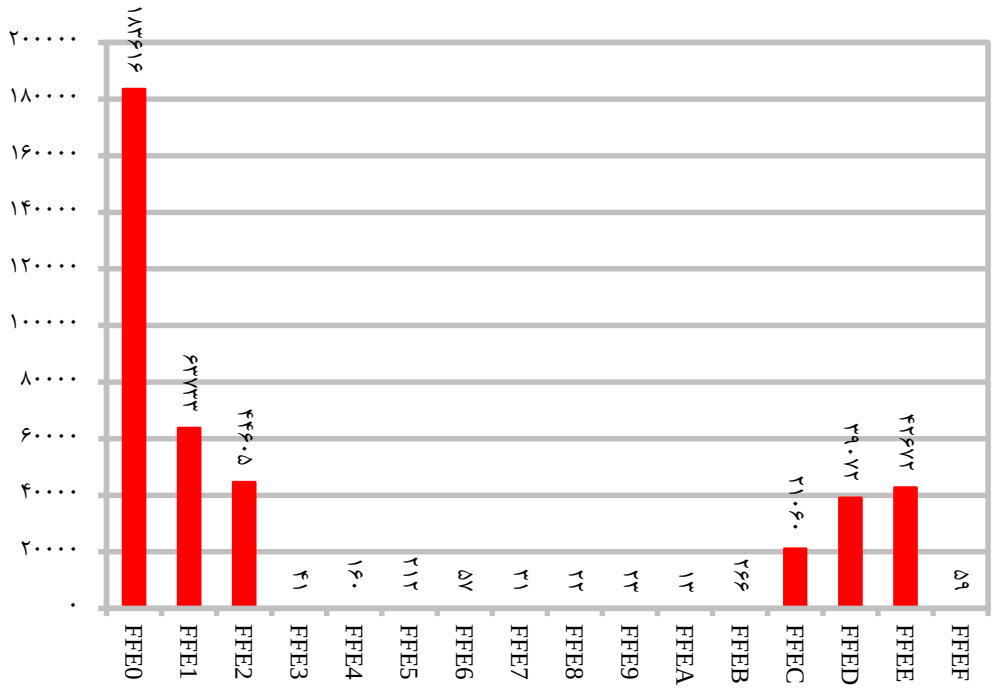
همان‌گونه که مشاهده می‌شود، فراوانی نمونه‌برداری ۴:۲:۲، ۴:۲:۰ (معادل ۴:۱:۱) و ۴:۲:۱ از بقیه حالات بیشتر است.

برخی از حالات نمونه‌برداری بسیار کم استفاده هستند که در صورت مشاهده‌ی این حالات باید به بررسی دقیق‌تر تصویر و سرآیندهای آن پرداخت. در واقع تصاویر با سرآیندهای بسیار کم استفاده، مشکوک هستند.

۵-۵-۲ داده‌کاوی بر روی دادگان کاربردی (نرم‌افزاری)

دادگان کاربردی در بخش ۳-۵-۴ به‌تفصیل بیان شده‌اند. فراوانی دادگان کاربردی مختلف در دیتابیس ارزیابی شده است. در شکل ۵-۱۴، فراوانی دادگان کاربردی در تمام تصاویر پایگاه داده، مشخص شده است.

همان‌گونه که در شکل ۵-۱۴ نیز مشخص است، فراوانی دادگان کاربردی با شاخص شروع، FFE0، FFE1، FFE2، FFEC، FFED و FFEE از بقیه شاخص‌ها بیشتر هستند و در واقع بقیه دادگان کاربردی بسیار کم استفاده هستند.

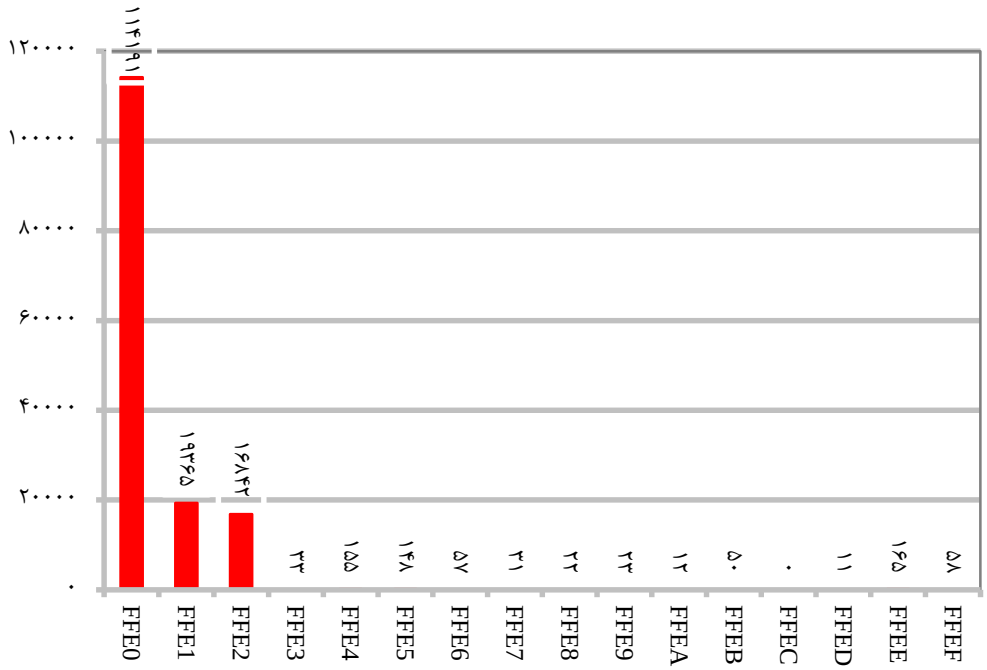


شکل ۵-۱۴: فراوانی دادگان کاربردی در تمام تصاویر پایگاه داده

برچسب‌های مرتبط با نرم‌افزارهای دیگری مانند فتوشاپ، باید از سرآیند حذف شوند. از این‌رو نتایج داده‌کاوی با لحاظ کردن برچسب‌های مرتبط با دوربین و بدون لحاظ کردن برچسب‌های مرتبط با نرم‌افزارهای شبیه فتوشاپ حائز اهمیت است. این نتایج در شکل ۵-۱۵ آورده شده است.

مهم‌ترین دادگان کاربردی مرتبط با دوربین، اطلاعات مربوط به JFIF با شاخص آغازین FFE0 و اطلاعات مربوط به EXIF با شاخص آغازین FFE1 است. در اطلاعات سرآیند تصاویر مرتبط با دوربین شاخص‌های FFE0، FFE1 و FFE2 وجود دارند. دادگان کاربردی مرتبط به نرم‌افزارهای ویرایشگر تصویر با شاخص FFE2 تا FFEF آغاز می‌شوند. در اطلاعات سرآیند تصاویری که در نرم‌افزارهای ویرایشگر مورد ویرایش قرار گرفتند، یک یا چند مورد از شاخص FFE2 تا FFEF در سرآیند تصویر مشاهده می‌شود.

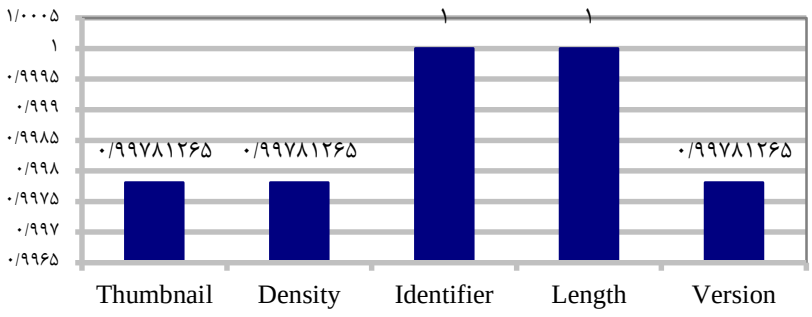
همان‌گونه که در شکل ۵-۱۵ نیز مشخص است، فراوانی دادگان کاربردی با شاخص شروع، FFE0، FFE1 و FFE2 از بقیه شاخص‌ها در تصاویر بدون فتوشاپ بیشتر هستند و در واقع بقیه دادگان کاربردی بسیار کم استفاده هستند. در واقع JFIF، EXIF و EXIF اختیاری از دادگان کاربردی مهم هستند و در سرآیند خروجی تصویر باید تولید شوند.



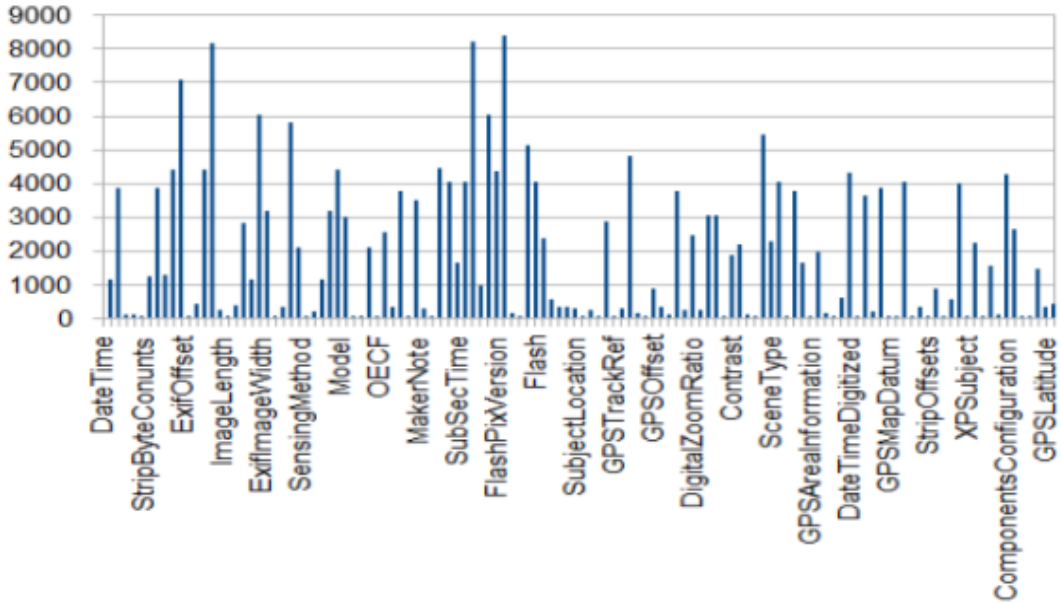
شکل ۵-۱۵: فروانی دادگان کاربردی در تصاویر بدون فتوشاپ در پایگاه داده

برای آشنایی با اهمیت هر یک از پارامترهای موجود در JFIF و EXIF، فراوانی این پارامترها نیز مورد بررسی قرار گرفته‌اند.

در شکل ۵-۱۶ فراوانی پنج پارامتر JFIF و شکل ۵-۱۷، ۱۲۳ پارامتر EXIF نشان داده شده است. همان‌گونه که مشخص است، پنج پارامتر JFIF در اکثر سرآیندهایی که این دادگان کاربردی را دارند، استفاده شده است. اما فراوانی در پارامترهای EXIF متنوع هستند. این تنوع متناسب با مدل دوربین و پارامترهای موجود در دوربین است.



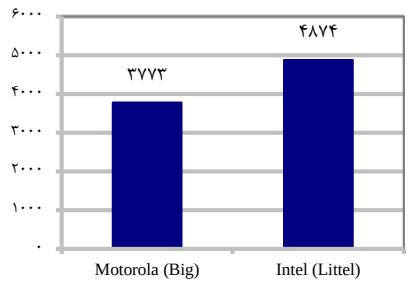
شکل ۵-۱۶: فروانی پارامترهای JFIF



شکل ۵-۱۷: فراوانی پارامترهای EXIF

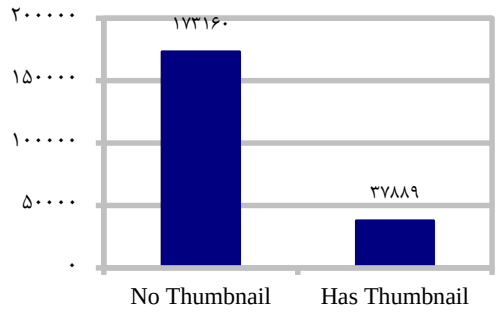
در دادگان کاربردی EXIF، دو فرمت Intel و Motorola برای ذخیره‌سازی داده وجود دارد. این فرمت‌ها متناسب با نوع دوربین و نرم‌افزار هستند. فروانی این دو نوع فرمت ذخیره‌سازی در شکل ۵-۱۸ نشان داده شده است.

همان‌گونه که مشاهده می‌شود فراوانی فرمت ذخیره‌سازی Intel، ۵۷٪ و Motorola، ۴۳٪ است.



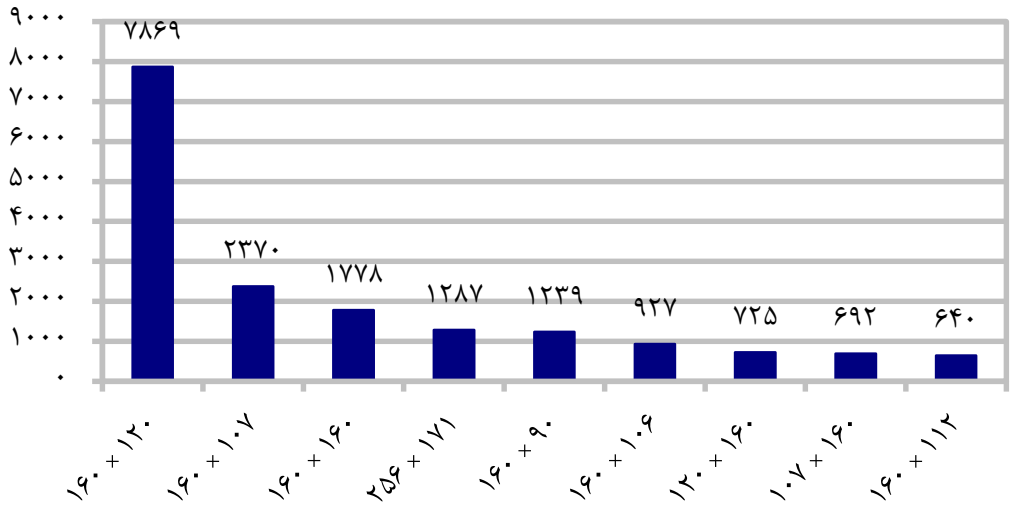
شکل ۵-۱۸: فراوانی فرمت ذخیره‌سازی اطلاعات در EXIF

یکی از بخش‌های مهم در EXIF تصویر بندانگشتی (Thumbnail) است. فراوانی وجود تصویر بندانگشتی، در شکل ۵-۱۹ نشان داده شده است. البته باید توجه داشت که از کل تصاویر تنها ۶۳۰۰۰ تصویر بخش EXIF را داشتند. از این‌رو در تصاویری که بخش EXIF را داشته‌اند، فراوانی وجود تصویر بندانگشتی، ۶۰٪ است.



شکل ۵-۱۹: فراوانی وجود تصویر بندانگشتی

تنها اندازه‌های خاصی برای تصاویر بندانگشتی وجود دارد. فراوانی اندازه‌ی تصویر بندانگشتی در شکل ۵-۲۰ نشان داده شده است.



شکل ۵-۲۰: فراوانی اندازه‌های تصویر بندانگشتی

در برخی از تصاویر JPEG دو تصویر بندانگشتی در سرآیند تصویر، وجود دارد که در اکثر مواقع با یکدیگر برابرند. این حالت در تصاویر خروجی دوربین رخ نمی‌دهد. این حالت تنها در نرم‌افزارهای ویرایشگر تصویر رخ می‌دهد.

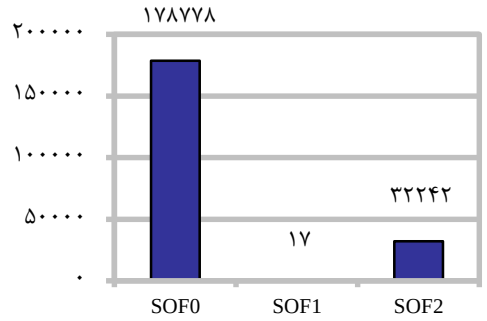
۵-۵-۳ داده‌کاوی بر روی شاخص آغاز فریم (SOF)

شاخص آغاز فریم از بخش‌های اجباری در سرآیند بشمار می‌آید. این بخش نشان دهنده‌ی نوع فشرده‌سازی تصویر JPEG است.

تصاویر JPEG می‌توانند از ساختارهای مختلفی برای فشرده‌سازی و کدینگ استفاده نمایند. در سرآیند فایل JPEG قطعه وجود دارد که ساختار فشرده‌سازی و کدینگ را مشخص می‌کند. ۱۵ ساختار

مختلف برای فشرده‌سازی تصویر به فرمت JPEG وجود دارد که کاربران تنها از دو ساختار اول آن برای فشرده‌سازی استفاده می‌کنند. متداول‌ترین فایل JPEG از فشرده‌سازی Baseline DCT و کدینگ هافمن استفاده می‌کند و بعد از آن فشرده‌سازی Extended DCT و کدینگ هافمن رواج دارد. در تحقیقی که در سال ۲۰۱۱ انجام گرفت، بیش از ۹۰ ٪ فایل‌های JPEG موجود در فضای مجازی از فشرده‌ساز نوع اول بهره می‌گرفتند. اما هم‌اکنون ۸۰ ٪ از فشرده‌ساز نوع اول و ۲۰٪ از فشرده‌ساز نوع دوم و سوم بهره می‌گیرند. در شکل ۵-۲۱ فراوانی انواع فشرده‌سازی نشان داده شده است. همان‌گونه که مشاهده می‌شود فراوانی فشرده‌سازی نوع اول یا Baseline DCT از انواع دیگر بیشتر است. فراوانی این‌گونه تصاویر ۸۵٪ است. در این رساله تنها تصویر با این نوع فشرده‌سازی حمایت می‌شود و انواع دیگر فشرده‌سازی حمایت نمی‌شوند.

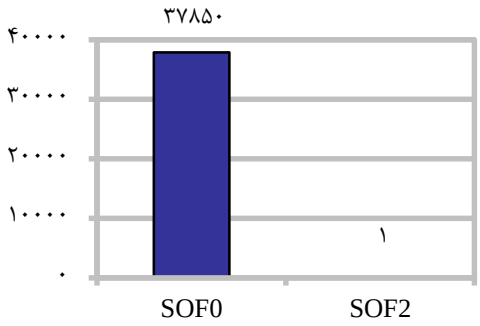
در واقع، قطعه شاخص آغاز فریم (SOF_0) مربوط به فایل‌های JPEG متداول، با FFC0 شروع می‌شود و اگر در فایل JPEG از قطعه شاخص آغاز فریم با شاخص آغازین FFC1، FFC2، FFC3، FFC5، FFC6، FFC7، FFC8، FFC9، FFCA، FFCB، FFCD، FFCE، FFCF استفاده شود، نشان از این دارد که فایل JPEG مربوطه از روش‌های دیگر فشرده‌سازی استفاده نموده است و به‌عنوان فایل JPEG غیرمتداول معرفی می‌شود. در این رساله تنها تصاویر JPEG با شاخص آغاز فریم FFC0 بررسی می‌شوند.



شکل ۵-۲۱: فراوانی انواع فشرده‌سازی در تصاویر JPEG

فراوانی انواع فشرده‌سازی برای تصویر بندانگشتی نیز بررسی شده است.

همان‌گونه که در شکل ۵-۲۲ مشاهده می‌شود فراوانی فشرده‌سازی نوع اول یا Baseline از انواع دیگر بیشتر است. این نوع فشرده‌سازی در بیش از ۹۹،۹ در صد از تصاویر بندانگشتی استفاده می‌شود.



شکل ۵-۲۲: فراوانی انواع فشرده‌سازی در تصاویر بندانگشتی JPEG

در حالت فشرده‌سازی Baseline DCT قطعه شاخص سرآیند اسکن از پارامترهایی شرح داده شده در بخش شاخص سرآیند اسکن تشکیل شده است که این پارامترها شامل دو بایت اندازه، یک بایت پارامتر Ns، یک بایت Cs_1، چهار بیت Td_1، چهار بیت Ta_1، یک بایت Cs_2، چهار بیت Td_2، چهار بیت Ta_2، یک بایت Cs_3، چهار بیت Td_3، چهار بیت Ta_3، یک بایت Ss، یک بایت Se ، چهار بیت Ah، چهار بیت A1 می‌باشند. مقادیر این پارامترها به‌صورت شکل ۵-۲۳ است:

0c 03 01 00 02 11 03 11 00 3f 00

شکل ۵-۲۳: پارامترهای قطعه شاخص سرآیند اسکن در حالت فشرده‌سازی Baseline DCT

۵-۵-۴ داده‌کاوی قطعه شاخص سرآیند فریم (SOF)

بخش قطعه شاخص سرآیند فریم در حالت فشرده‌سازی Baseline DCT معمولاً شامل ۱۷ بایت (۱۱ بایت در واحد هگز) است. بایت اول دقت نمونه است که در این حالت عدد هشت است. سپس تعداد سطرها در دو بایت و تعداد نمونه‌های هر سطر در دو بایت بعدی می‌آیند. این مقادیر متناسب با تصویر می‌باشند و در رابطه با تصویرهای مختلف متفاوت است. سپس پارامتر NF در یک بایت می‌آید که تعداد اجزای تصویر را مشخص می‌کند و در رابطه با این حالت عدد سه است. سپس همان‌گونه که در بخش سرآیند فریم شرح داده شد برای هر یک اجزاء تصویر پارامترهای C_i (۱ بایت)، H_i (چهار بیت)، V_i (چهار بیت)، Tq_i (یک بایت) می‌آیند که این پارامترها قبلاً شرح داده شده‌اند. برای سرآیند اصلی تصویر و برای سه جز مختلف تصویر در حالت Baseline DCT این پارامترها معمولاً به‌صورت شکل ۵-۲۴ هستند:

01 11 00 02 11 01 03 11 01

شکل ۵-۲۴: سه جز مختلف پارامترهای قطعه شاخص سرآیند فریم در تصویر اصلی در حالت فشرده‌سازی Baseline DCT

اگر کل قطعه شاخص سرآیند فریم را در نظر بگیریم به‌صورت شکل ۵-۲۵ است:

FF C0 00 11 08 xx xx xx xx 03 01 11 00 02 11 01 03 11 01

شکل ۵-۲۵: کل قطعه شاخص سرآیند فریم در تصویر در حالت فشرده‌سازی Baseline DCT

البته همان‌گونه که در بخش سرآیند فریم شرح داده شد، H_i و V_i می‌توانند شامل اعداد یک تا چهار شوند و شاخص سرآیند فریم می‌تواند به صورت‌های دیگری نیز در تصویر وجود داشته باشد که به دو مورد پر کاربرد آن در شکل ۵-۲۶ اشاره شده است:

FF C0 00 11 08 xx xx xx xx 03 01 22 00 02 11 01 03 11 01

FF C0 00 11 08 xx xx xx xx 03 01 21 00 02 11 01 03 11 01

شکل ۵-۲۶: دو مورد پر کاربرد کل قطعه شاخص سرآیند فریم در حالت فشرده‌سازی Baseline DCT

برای بخش تصویر بندانگشتی، پارامتر H1 و V1 معمولاً به‌صورت ۲۲ است و اگر کل قطعه شاخص سرآیند فریم برای تصویر بندانگشتی، را در نظر بگیریم معمولاً به‌صورت شکل ۵-۲۷ است:

FF C0 00 11 08 xx xx xx xx 03 01 22 00 02 11 01 03 11 01

شکل ۵-۲۷: کل قطعه شاخص سرآیند فریم در تصویر بندانگشتی در حالت فشرده‌سازی Baseline DCT

اطلاعات مربوط به‌اندازه تصویر علاوه بر سرآیند فایل، ممکن است در بخش‌های دیگر فایل نیز وجود داشته باشد. اندازه تصویر امکان دارد در یکی از دادگان کاربردی وجود داشته باشد. در بخش EXIF یا دادگان مربوط به نرم‌افزار فتوشاپ می‌توان اندازه تصویر را پیدا نمود.

در بخش EXIF اندازه تصویر پس از a002 و a003 می‌آید و اگر از ساختار Intel برای ذخیره‌سازی استفاده شود، اندازه تصویر پس از ۰۲a۰ و ۰۳a۰ و به‌صورت ساختار Intel (ابتدا بایت کم ارزش و بعد بایت پر ارزش) می‌آید. تمام اطلاعات مربوط اندازه تصویر باید با همدیگر همخوانی داشته باشند.

۵-۵-۵ داده‌کاوی بر روی جدول کوانتیزاسیون (DQT)

تمام جداول کوانتیزاسیون که بیش از ۲۰۰۰ جدول بودند، a002 و a003 از دیتابیس استخراج شده و به دادگان رساله اضافه شده است. جداول پر کاربرد کوانتیزاسیون در پیوست آمده‌اند. این جداول در دادگان نرم‌افزار JPEGSNOOP نیز وجود دارند.

۵-۵-۶ داده‌کاوی قطعه شاخص تعریف شروع مجدد (DRI)

این قطعه با FFDD آغاز می‌شود و اندازه آن فقط چهار بایت است و بعد از آن قطعه شاخص کدینگ هافمن یا قطعه شاخص بخش کاربردی می‌آید.

در این قطعه دو بایت اول معادل اندازه قطعه است که معادل چهار است و دو بایت دوم (بایت سوم و چهارم) تعداد MCU های موجود در بازه شروع مجدد را مشخص می‌کند. در واقع بایت سوم و چهارم از رابطه n×MCUR محاسبه می‌شود. مقدار n بیانگر تعداد سطرهای MCU در بازه شروع مجدد است

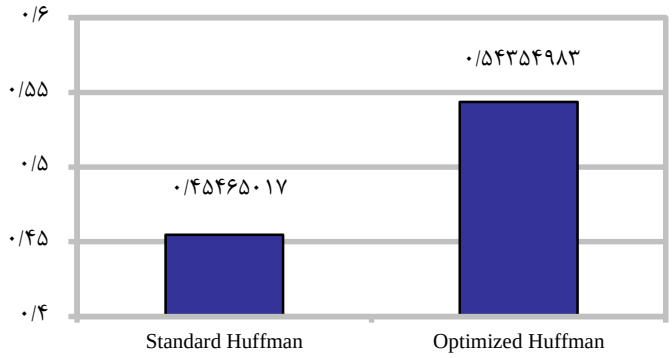
که معمولاً معادل با یک است. مقدار MCUR برابر با تعداد MCU های لازم برای ساختن یک سطر از نمونه‌های مربوط به هر یک از مولفه‌های تصویر در اسکن می‌باشد. در تصویر JPEG معمولاً هر MCU یک ماکرو بلاک ۸×۸ یا ۱۶×۱۶ است و از این‌رو مقدار MCUR معادل با تعداد ستون‌ها تقسیم بر هشت یا ۱۶ است. البته اگر این عدد صحیح نباشد گرد به بالا می‌شود.
مقادیر پارامترهای قطعه شاخص تعریف شروع مجدد به‌صورت شکل ۵-۲۸ است:

FF DD 00 04 xx xx

شکل ۵-۲۸: پارامترهای قطعه شاخص تعریف شروع مجدد

۵-۵-۷ داده‌کاوی جداول هافمن (DHT)

در حدود ۴۵٪ از تصاویر از جدول هافمن استاندارد استفاده شده است. فراوانی جداول هافمن استاندارد در شکل ۵-۲۹ نشان داده شده است.



شکل ۵-۲۹: فراوانی جداول هافمن

۵-۶ مقایسه روش پیشنهادی با روش‌های مبتنی بر فرمت

تکنیک‌های مبتنی بر فرمت، نوع دیگری از تکنیک‌های تشخیص جعل تصویر هستند. این روش‌ها مبتنی‌بر فرمت‌های تصویری هستند و عمدتا در فرمت JPEG کاربرد دارند. اگر تصویر فشرده شده باشد، تشخیص جعل بسیار دشوار است اما این تکنیک‌ها می‌توانند جعل را در تصویر فشرده، شناسایی کنند. با توجه به اهمیت آشکارسازی جعل در جرم‌شناسی در این رساله، روش جدیدی برای بهبود عملکرد احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه شد. در جدول ۵-۲ روش پیشنهادی، با چند روش متداول مبتنی بر فرمت از جنبه‌های مختلف مقایسه شد. با توجه به اطلاعات حاصل از جدول ۵-۲، روش پیشنهادی نسبت به روش‌های دیگر عملکرد بهتری در احراز هویت تصاویر دارد.

جدول ۵-۲: مقایسه روش پیشنهادی با روش‌های مبتنی بر فرمت در تشخیص جعلی تصویر منفعل

تکنیک‌های مبتنی بر فرمت			
عنوان تحقیق	**هدف اصلی تحقیق**	**مزایا و معایب**	**ردیف**
احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند **(روش پیشنهادی)**	روشی برای بهبود عملکرد احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه کردیم. این روش مدل دوربین و نرم‌افزار تغییر دهنده تصویر را مشخص می‌کند.	**معایب:** در برابر جاسازی اطلاعات سرآیند تصویر اصلی در تصویر جعلی آسیب‌پذیر است. **نکات قوت**: مدل دوربین یا نرم‌افزار تغییر دهنده تصویر را مشخص می‌کند. تغییرات در سرآیند تصاویر را تعیین می‌کند.	۱
احراز هویت دیجیتالی شده برای جرم‌شناسی تصویر [۲۷]	روشی برای شناسایی تصاویر دستکاری شده و هرگونه پیام پنهان در تصاویر ارائه شده است.		۲
تأیید اعتبار تصویر با استفاده از سرآیندهای JPEG [۴۳]	روشی برای شناسایی منبع تصویر و تعیین تغییر تصویر توسط نرم‌افزار ویرایشگر تصویر ارائه شده است.		۳
تأیید اعتبار تصویر دیجیتال از سرآیندهای JPEG [۱۰]	استفاده از فرمت JPEG به صورت‌های مختلف برای تایید اعتبار تصاویر که از نسخه اصلی خود تغییر کرده‌اند. تشخیص تصویری که در نرم‌افزار ویرایشگر عکس مورد تغییر قرار گرفته است.	**معایب:** در برابر حمله دوباره پخش استاندارد که در آن یک تصویر دیجیتال دستکاری، چاپ و عکس‌برداری مجدد می‌شود، آسیب-پذیر است. **نکات قوت**: هرگونه ویرایش عکس با فتوشاپ به‌راحتی و بدون ابهام قابل شناسایی است.	۴
شناسایی منبع جرم‌شناسی با استفاده از سرآیند تصاویر JPEG: در مورد تلفن‌های هوشمند [۴۴]	یک مطالعه در مقیاس بزرگ از اطلاعات سرآیند تصاویر JPEG از تلفن‌های هوشمند اپل انجام شده است. تا تأثیر این پیشرفت در امکان انجام شناسایی منبع تصویر را بررسی کنند. هدف پیوند یک تصویر به ساخت یک مدل دوربین خاص یا یک نرم‌افزار خاص از اطلاعات سرآیند تصاویر JPEG است.	**نکات قوت:** چندین برنامه خاص یا نسخه سیستم‌عامل باقابلیت اطمینان بالا قابل تشخیص است.	۵
بررسی ته نقش‌نگاری شکننده برای تأیید صحت تصویر [۴۵]	روشی برای تأیید صحت تصویر و تصحیح دستکاری ارائه شده است.		۶

۵-۷ جمع‌بندی

در این فصل، عملکرد الگوریتم روش پیشنهادی برای احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند بررسی شد. برای بررسی بهتر روش پیشنهادی، تعدادی از تصاویر پایگاه داده مورد استفاده قرار گرفتند. تصاویر جعلی با استفاده از روش پیشنهادی تشخیص داده شد. برای ارزیابی نتایج از چندین نرم‌افزار معروف ویرایشگر تصویر و نرم‌افزار برنامه‌نویسی استفاده شد.

فصل ٦ : نتیجه گیری و پیشنهادها برای کارهای آتی

۶-۱ مقدمه

امروزه بدون شک در قرنی زندگی می‌کنیم که در معرض تعداد بسیار زیادی از جلوه‌ها و محصولات تصویری قرار داریم. شاید اولین و به‌عبارت دیگر مهم‌ترین سوالی که در رویارویی با هر تصویری ذهن بیننده را درگیر می‌سازد آن باشد که آیا این تصویر حقیقت دارد یا دستخوش جعل و تحریف جاعلان حرفه‌ای و نرم‌افزارهای ویرایش تصویر قرار گرفته و یک تصویر جعلی است.

در ادامه این فصل ابتدا الگوریتم ارائه شده در این رساله را به‌طور مختصر توضیح داده و جمع‌بندی می‌کنیم. سپس پیشنهادهایی برای کارهای آتی در این حوزه ارائه خواهیم داد.

۶-۲ نتیجه‌گیری و پیشنهادها برای کارهای آتی

در این پژوهش برای بهبود عملکرد روش‌های مبتنی بر فرمت JPEG[۱] که جعل در تصویر فشرده را تشخیص می‌دهد، روش‌های جدیدی برای احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند ارائه شد. روش‌های جدیدی برای آشکارسازی جعل در جرم‌شناسی تصاویر با استفاده از اطلاعات سرآیند تصویر JPEG ارائه شد. با این روش تعیین شد که تصویر موردنظر، از دوربین اخذ شده یا در نرم‌افزاری مورد تغییر قرار گرفته است. در این روش ابتدا با توجه به اطلاعات اضافی در سرآیند تصویر JPEG، نوع نرم‌افزار ویرایشگر شناسایی شد و سپس با توجه به دیگر اطلاعات موجود در سرآیند، نرم‌افزار ویرایشگر و مدل دوربین شناسایی شد و سپس سرآیند تغییر یافته شناسایی گردید.

نتایج ارزیابی روش‌های پیشنهاد شده با پایگاه داده جمع‌آوری شده نشان دادند که روش پیشنهادی ما برای احراز هویت تصویر برای تشخیص مدل دوربین و نوع نرم‌افزار ویرایشگر تصویر به‌خوبی عمل می‌کند. همچنین در روش پیشنهادی هرگونه ویرایش عکس با فتوشاپ به‌راحتی و بدون ابهام قابل شناسایی است.

به‌طور مشخص می‌توان مسائل زیر را به‌عنوان معایب احراز هویت تصاویر JPEG به کمک اطلاعات سرآیند اشاره نمود:

۱. احراز هویت تصویر JPEG به کمک اطلاعات سرآیند: امضای دوربین شامل: جدول کوانتیزاسیون، کدینگ هافمن، اطلاعات دادگان کاربردی (نرم‌افزاری) است که از سرآیند تصویر JPEG استخراج می‌شود، از این امضا برای تأیید اعتبار تصویر دیجیتال استفاده می‌شود. با مقایسه این امضا با امضای دوربین‌های معتبر و شناخته شده، منبع عکس شناسایی می‌شود. اما این روش در برابر عکس‌برداری مجدد با دوربین اصلی از عکس جعل شده که اطلاعات سرآیند را بازسازی می‌کند، آسیب‌پذیر است [۱۰].

۲. تغییرات مداوم فن‌آوری دستگاه‌های تولید تصویر: قدرت تحلیل جرم‌شناسی در توانایی به دست آوردن امضا از طیف گسترده‌ای از دوربین‌ها و تلفن‌های همراه نهفته است. با توجه به اینکه دائماً دوربین‌ها و

---

۱. Format Based

تلفن‌های همراه جدید منتشر خواهد شد، چالش‌های مهمی را ایجاد می‌کند. برای پیگیری این تغییرات مداوم، نیاز به تداوم ساخت پایگاه داده از تصاویر و اطلاعات دوربین است [۱۰].

۳. پنهان کردن آثار دستکاری اطلاعات سرآیند تصویر: کسی که تصاویر را جعل می‌کند، می‌تواند با استخراج امضای دوربین، تغییر تصویر، و سپس ذخیره مجدد تصویر با فرمت EXIF مناسب و کلیه پارامترهای مناسب از جمله: اندازه تصویر، جدول کوانتیزاسیون تصویر، کدینگ هافمن تصویر، اندازه تصویر بندانگشتی، جدول کوانتیزاسیون تصاویر بندانگشتی و کدینگ هافمن تصویر بندانگشتی، اثر دستکاری آن‌ها را پنهان کند [۱۰].

با روش‌های چندی‌سازی مبتنی بر فرمت، شناسایی جعل به‌طور کامل در تصویر فشرده، امکان‌پذیر نیست. باید به کمک ترکیبی از روش‌های چندی‌سازی مبتنی بر فرمت و روش حسگر نویز مبتنی بر دوربین شناسایی جعل انجام شود.

در کارهای آتی، علاوه بر اطلاعات سرآیند می‌توان از اطلاعات تصویر نیز برای تشخیص جعل استفاده کرد و روشی ترکیبی از ویژگی‌های مبتنی بر تصویر و مبتنی بر سرآیند ارائه کرد.

پوست

جدول کوانتیزاسیون () PENTAX – PENTAX Optio S5i

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

جدول کوانتیزاسیون Canon – Canon EOS-1Ds Mark II (fine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	1	1	2	2	2	2
1	1	1	1	2	2	2	2
1	1	1	2	2	2	2	2
1	1	2	2	2	2	2	2
2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	2	2	1
1	1	1	1	1	2	2	2
1	1	1	1	2	2	2	2
1	1	2	2	2	2	2	2
1	2	2	2	2	2	2	2

جدول کوانتیزاسیون Canon – Canon PowerShot G1 (Superfine)

نمونه‌برداری رنگ ۱×۲

جدول کوانتیزاسیون رنگ

1	1	1	2	3	3	6	6
1	1	1	2	4	3	6	6
1	1	2	2	6	6	6	6
2	2	2	3	6	6	6	6
3	4	6	6	6	6	6	6
3	3	6	6	6	6	6	6
6	6	6	6	6	6	6	6
6	6	6	6	6	6	6	6

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	1	2	2
1	1	1	1	1	1	2	3
1	1	1	1	2	2	3	3
1	1	1	1	2	3	3	3
1	1	2	2	2	4	3	3
1	1	2	3	4	3	4	3
2	2	3	3	3	4	4	3
2	3	3	3	3	3	3	3

جدول کوانتیزاسیون NIKON – COOLPIX P2 (FINE)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	1	2	4	4	4	4
1	1	1	3	4	4	4	4
1	1	2	4	4	4	4	4
2	3	4	4	4	4	4	4
4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	2	2	2
1	1	1	1	1	2	2	2
1	1	1	1	2	2	3	2
1	1	1	1	2	3	3	2
1	1	1	2	3	4	4	3
1	1	2	3	3	4	5	4
2	3	3	3	4	5	5	4
3	4	4	4	4	4	4	4

جدول کوانتیزاسیون Canon – Canon EOS-1D Mark II N (fine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	1	2	5	5	5	5
1	1	1	3	5	5	5	5
1	1	3	5	5	5	5	5
2	3	5	5	5	5	5	5
5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	2	3	3
1	1	1	1	1	3	3	3
1	1	1	1	2	3	3	3
1	1	1	2	3	4	4	3
1	1	2	3	3	5	5	4
1	2	3	3	4	5	5	4
2	3	4	4	5	6	6	5
4	4	5	5	5	5	5	5

جدول کوانتیزاسیون Canon – Canon DIGITAL IXUS 40 (superfine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	2	4	6	11	11	11
1	1	2	4	8	11	11	11
2	2	3	4	11	11	11	11
4	4	4	5	11	11	11	11
6	8	11	11	11	11	11	11
11	11	11	11	11	11	11	11
11	11	11	11	11	11	11	11
11	11	11	11	11	11	11	11

جدول کوانتیزاسیون درخشندگی

1	1	1	1	1	2	3	3
1	1	1	1	1	3	3	3
1	1	1	1	2	3	3	3
1	1	1	1	2	4	4	3
1	1	3	4	4	6	6	4
1	2	3	3	4	5	6	5
2	3	4	4	5	6	6	5
5	5	5	5	5	5	5	5

جدول کوانتیزاسیون Canon – Canon EOS-1D(fine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	2	3	7	7	7	7
1	1	2	4	7	7	7	7
2	2	4	7	7	7	7	7
3	4	7	7	7	7	7	7
7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7

جدول کوانتیزاسیون درخشندگی

1	1	1	1	2	3	3	4
1	1	1	1	2	4	4	4
1	1	1	2	3	4	5	4
1	1	1	2	3	6	5	4
1	1	2	4	5	7	7	5
2	2	4	4	5	7	8	6
3	4	5	6	7	8	8	7
5	6	6	7	7	7	7	7

جدول کوانتیزاسیون NIKON - E8400 (FINE)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	2	4	8	8	8	8
1	2	2	5	8	8	8	8
2	2	4	8	8	8	8	8
4	5	8	8	8	8	8	8
8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8

جدول کوانتیزاسیون درخشندگی

1	1	1	1	2	3	4	5
1	1	1	2	2	5	5	4
1	1	1	2	3	5	6	4
1	1	2	2	4	7	6	5
1	2	3	4	5	9	8	6
2	3	4	5	6	8	9	7
4	5	6	7	8	10	10	8
6	7	8	8	9	8	8	8

جدول کوانتیزاسیون NIKON – COOLPIX P3 (FINE)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

1	1	2	5	10	10	10	10
1	2	2	7	10	10	10	10
2	2	6	10	10	10	10	10
5	7	10	10	10	10	10	10
10	10	10	10	10	10	10	10
10	10	10	10	10	10	10	10
10	10	10	10	10	10	10	10
10	10	10	10	10	10	10	10

جدول کوانتیزاسیون درخشندگی

1	1	1	1	2	4	5	6
1	1	1	2	2	6	6	6
1	1	1	2	4	6	7	6
1	1	2	3	5	9	8	6
1	2	4	6	7	11	11	8
2	3	6	7	8	11	12	10
5	7	8	9	11	13	13	11
7	10	10	10	12	11	11	10

جدول کوانتیزاسیون () NIKON –COOLPIX P4

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

2	2	2	5	11	11	11	11
2	2	3	7	11	11	11	11
2	3	6	11	11	11	11	11
5	7	11	11	11	11	11	11
11	11	11	11	11	11	11	11
11	11	11	11	11	11	11	11
11	11	11	11	11	11	11	11
11	11	11	11	11	11	11	11

جدول کوانتیزاسیون درخشندگی

1	1	1	1	2	4	6	7
1	1	1	2	3	6	7	6
1	1	1	2	4	6	8	6
1	2	2	3	6	10	9	7
2	2	4	6	8	13	12	9
2	4	6	7	9	12	13	11
5	7	9	10	12	14	14	12
8	11	11	11	13	12	12	11

جدول کوانتیزاسیون NIKON – COOLPIX L12 (FINE)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

2	2	3	6	12	12	12	12
2	3	3	8	12	12	12	12
3	3	7	12	12	12	12	12
6	8	12	12	12	12	12	12
12	12	12	12	12	12	12	12
12	12	12	12	12	12	12	12
12	12	12	12	12	12	12	12
12	12	12	12	12	12	12	12

جدول کوانتیزاسیون درخشندگی

2	1	1	2	3	5	6	7
1	1	2	2	3	7	7	7
2	2	2	3	5	7	8	7
2	2	3	3	6	10	10	7
2	3	4	7	8	13	12	9
3	4	7	8	10	12	14	11
6	8	9	10	12	15	14	12
9	11	11	12	13	12	12	12

جدول کوانتیزاسیون Canon-Canon PowerShot SD700 IS (fine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

4	4	5	9	15	26	26	26
4	4	5	10	19	26	26	26
5	5	8	9	26	26	26	26
9	10	9	13	26	26	26	26
15	19	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26

جدول کوانتیزاسیون درخشندگی

1	1	1	2	3	6	8	10
1	1	2	3	4	8	9	8
2	2	2	3	6	8	10	8
2	2	3	4	7	12	11	9
3	3	8	11	10	16	15	11
3	5	8	10	12	15	16	13
7	10	11	12	15	17	17	14
14	13	13	15	15	14	14	14

جدول کوانتیزاسیون NIKON – COOLPIX S10 (FINE)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

3	3	4	8	16	16	16	16
3	3	4	11	16	16	16	16
4	4	9	16	16	16	16	16
8	11	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16

جدول کوانتیزاسیون درخشندگی

3	2	2	3	4	6	8	10
2	2	2	3	4	9	10	9
2	2	3	4	6	9	11	9
2	3	4	5	8	14	13	10
3	4	6	9	11	17	16	12
4	6	9	10	13	17	18	15
8	10	12	14	16	19	19	16
12	15	15	16	18	16	16	16

جدول کوانتیزاسیون Photoshop – (Save For Web 070)

نمونه‌برداری رنگ: ۱×۱

جدول کوانتیزاسیون رنگ

4	5	8	15	20	20	20	20
5	7	10	14	20	20	20	20
8	10	14	20	20	20	20	20
15	14	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

جدول کوانتیزاسیون درخشندگی

4	3	3	4	6	7	8	10
3	3	3	4	5	6	8	10
3	3	3	4	6	9	12	12
4	4	4	7	9	12	12	17
6	5	6	9	12	13	17	20
7	6	9	12	13	17	20	20
8	8	12	12	17	20	20	20
10	10	12	17	20	20	20	20

جدول کوانتیزاسیون SONY – DSC-R1 (fine)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

3	4	5	9	20	20	20	20
4	4	5	13	20	20	20	20
5	5	11	20	20	20	20	20
9	13	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

جدول کوانتیزاسیون درخشندگی

3	2	2	3	5	8	10	12
2	2	3	4	5	12	12	11
3	3	3	5	8	11	14	11
3	3	4	6	10	17	16	12
4	4	7	11	14	22	21	15
5	7	11	13	16	21	23	18
10	13	16	17	21	24	24	20
14	18	19	20	22	20	21	20

جدول کوانتیزاسیون SONY – DSC-H9 (variable)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

4	4	6	11	24	24	24	24
4	5	6	16	24	24	24	24
6	6	13	24	24	24	24	24
11	16	24	24	24	24	24	24
24	24	24	24	24	24	24	24
24	24	24	24	24	24	24	24
24	24	24	24	24	24	24	24
24	24	24	24	24	24	24	24

جدول کوانتیزاسیون درخشندگی

4	3	2	4	6	10	12	15
3	3	3	5	6	14	14	13
3	3	4	6	10	14	17	13
3	4	5	7	12	21	19	15
4	5	9	13	16	26	25	18
6	8	13	15	19	25	27	22
12	15	19	21	25	29	29	24
17	22	23	24	27	24	25	24

جدول کوانتیزاسیون FUJIFILM – FinePix F700 (normal)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

4	4	6	12	26	26	26	26
4	5	6	14	26	26	26	26
6	6	14	26	26	26	26	26
12	17	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26

جدول کوانتیزاسیون درخشندگی

4	2	2	4	6	10	13	16
3	3	3	5	6	15	15	14
3	3	4	6	10	15	18	14
3	4	5	7	13	23	21	16
4	5	9	14	18	28	27	20
6	9	14	17	21	27	30	24
13	17	20	23	27	32	31	26
19	24	25	26	29	26	27	26

جدول کوانتیزاسیون Photoshop – (Save For Web 060)

نمونه‌برداری رنگ: ۱×۱

جدول کوانتیزاسیون رنگ

7	7	13	24	26	31	31	31
7	12	16	21	31	31	31	31
13	16	17	31	31	31	31	31
24	21	31	31	31	31	31	31
26	31	31	31	31	31	31	31
31	31	31	31	31	31	31	31
31	31	31	31	31	31	31	31
31	31	31	31	31	31	31	31

جدول کوانتیزاسیون درخشندگی

6	4	4	6	9	11	12	16
4	5	5	6	8	10	12	12
4	5	5	6	10	12	14	19
6	6	6	11	12	15	19	28
9	8	10	12	16	20	27	31
11	10	12	15	20	27	31	31
12	12	14	19	27	31	31	31
16	12	19	28	31	31	31	31

جدول کوانتیزاسیون FUJIFILM – FinePix S5000 (normal)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

4	6	8	17	35	35	35	35
6	7	9	20	35	35	35	35
8	9	19	35	35	35	35	35
17	23	35	35	35	35	35	35
35	35	35	35	35	35	35	35
35	35	35	35	35	35	35	35
35	35	35	35	35	35	35	35
35	35	35	35	35	35	35	35

جدول کوانتیزاسیون درخشندگی

4	3	3	5	8	14	18	22
4	4	5	6	9	21	21	19
5	4	5	8	14	20	25	20
5	6	7	10	18	31	29	22
6	7	13	20	24	39	37	27
8	12	19	23	29	37	41	33
17	23	28	31	37	43	43	36
26	33	34	35	40	36	37	35

جدول کوانتیزاسیون Photoshop – (Save For Web 051)

نمونه‌برداری رنگ: ۱×۱

جدول کوانتیزاسیون رنگ

8	9	16	29	32	38	38	38
9	14	20	26	38	38	38	38
16	20	21	38	38	38	38	38
29	26	38	38	38	38	38	38
32	38	38	38	38	38	38	38
38	38	38	38	38	38	38	38
38	38	38	38	38	38	38	38
38	38	38	38	38	38	38	38

جدول کوانتیزاسیون درخشندگی

8	5	5	8	11	13	15	17
5	6	6	7	10	12	12	15
5	6	6	8	12	13	17	23
8	7	8	13	13	18	23	34
11	10	12	13	19	25	33	38
13	12	13	18	25	33	38	38
15	12	17	23	33	38	38	38
17	15	23	34	38	38	38	38

جدول کوانتیزاسیون FUJIFILM – FinePix F40fd()

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

7	7	10	19	40	40	40	40
7	8	10	26	40	40	40	40
10	10	22	40	40	40	40	40
19	26	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40

جدول کوانتیزاسیون درخشندگی

6	5	6	6	7	10	20	29
4	5	5	7	9	14	26	37
4	6	6	9	15	22	31	38
6	8	10	12	22	26	35	39
10	10	16	20	27	32	41	45
16	23	23	35	44	42	48	40
20	24	28	32	41	45	48	41
24	22	22	25	31	37	40	40

جدول کوانتیزاسیون (080) – IrfanView

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

7	7	10	19	40	40	40	40
7	8	10	26	40	40	40	40
10	10	22	40	40	40	40	40
19	26	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40
40	40	40	40	40	40	40	40

جدول کوانتیزاسیون درخشندگی

6	4	4	6	10	16	20	24
5	5	6	8	10	23	24	22
6	5	6	10	16	23	28	22
6	7	9	12	20	35	32	25
7	9	15	22	27	44	41	31
10	14	22	26	32	42	45	37
20	26	31	35	41	48	48	40
29	37	38	39	45	40	41	40

جدول کوانتیزاسیون Canon – Canon PowerShot S30 (video)

نمونه‌برداری رنگ: ۱×۲

جدول کوانتیزاسیون رنگ

9	9	12	20	15	26	79	79
9	10	12	10	26	26	79	79
12	12	10	10	26	79	79	79
20	10	10	26	79	79	79	79
15	26	26	79	79	79	79	79
26	26	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79

جدول کوانتیزاسیون درخشندگی

9	6	5	9	13	22	29	35
6	6	8	11	15	33	34	30
8	7	9	13	22	33	39	31
8	9	12	16	28	49	45	34
10	12	21	32	39	61	58	42
13	19	31	36	45	58	63	51
28	36	44	49	58	68	66	55
41	52	54	55	62	56	57	54

جدول کوانتیزاسیون Photoshop - (Save For Web 040)

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

13	11	13	16	20	20	29	37
11	14	14	14	16	20	26	32
13	14	15	17	20	23	35	40
16	14	17	21	23	30	40	50
20	16	20	23	30	37	50	59
20	20	23	30	37	48	59	59
29	26	35	40	50	59	59	59
37	32	40	50	59	59	59	59

جدول کوانتیزاسیون درخشندگی

12	8	8	12	17	21	24	23
8	9	9	11	15	19	18	23
8	9	10	12	19	20	27	36
12	11	12	21	20	28	36	53
17	15	19	20	30	39	51	59
21	19	20	28	39	51	59	59
24	18	27	36	51	59	59	59
23	23	36	53	59	59	59	59

جدول کوانتیزاسیون Photoshop – (Save For Web 020)

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

20	19	22	27	26	33	49	62
19	25	23	22	26	33	45	56
22	23	26	29	33	39	59	65
27	22	29	36	39	51	65	65
26	26	33	39	51	62	65	65
33	33	39	51	62	65	65	65
49	45	59	65	65	65	65	65
62	56	65	65	65	65	65	65

جدول کوانتیزاسیون درخشندگی

18	14	14	21	30	35	34	39
14	16	16	19	26	24	30	39
14	16	17	21	24	34	46	62
21	19	21	26	33	48	62	65
30	26	24	33	51	65	65	65
35	24	34	48	65	65	65	65
34	30	46	62	65	65	65	65
39	39	62	65	65	65	65	65

جدول کوانتیزاسیون IrfanView - (060)

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

14	14	19	38	79	79	79	79
14	17	21	53	79	79	79	79
19	21	45	79	79	79	79	79
38	53	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79

جدول کوانتیزاسیون درخشندگی

13	9	8	13	19	32	41	49
10	10	11	15	21	46	48	44
11	10	13	19	32	46	55	45
11	14	18	23	41	70	64	50
14	18	30	45	54	87	82	62
19	28	44	51	65	83	90	74
39	51	62	70	82	97	96	81
58	74	76	78	90	80	82	79

جدول کوانتیزاسیون IrfanView – (040)

نمونه‌برداری رنگ: ۲×۲

جدول کوانتیزاسیون رنگ

21	23	30	59	124	124	124	124
23	26	33	83	124	124	124	124
30	33	70	124	124	124	124	124
59	83	124	124	124	124	124	124
124	124	124	124	124	124	124	124
124	124	124	124	124	124	124	124
124	124	124	124	124	124	124	124
124	124	124	124	124	124	124	124

جدول کوانتیزاسیون درخشندگی

20	14	13	20	30	50	64	76
15	15	18	24	33	73	75	69
18	16	20	30	50	71	86	70
18	21	28	36	64	109	100	78
23	28	46	70	85	136	129	96
30	44	69	80	101	130	141	115
61	80	98	109	129	151	150	126
90	115	119	123	140	125	129	124

مراجع

[1] S. K. Mankar and A. A. Gurjar, “Image forgery types and their detection: A review,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 4, pp. 174–178, 2015.

[2] N. Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Forensic techniques for classifying scanner, computer generated and digital camera images,” in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 1653–1656.

[3] A. Jeyalakshmi and D. R. Chitra, “Source Camera Identification using Image Features,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 1, pp. p490-504, 2018.

[4] J. Bunk *et al.*, “Detection and localization of image forgeries using resampling features and deep learning,” in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1881–1889.

[5] W. Luo, Z. Qu, F. Pan, and J. Huang, “A survey of passive technology for digital image forensics,” *Front. Comput. Sci. China*, vol. 1, no. 2, pp. 166–179, 2007.

[6] H. Farid, “Image forgery detection,” *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 16–25, 2009.

[7] ن. علی پور و ع. بهزاد, “تشخیص جعل در تصاویر دیجیتال با استفاده از تاثیر فشرده‌سازی مجدد بر ضرایب DCT کوانتیزه شده,” ۱۳۹۴.

[8] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still image data compression standard*. Springer Science & Business Media, 1992.

[9] E. Hamilton, “JPEG File Interchange Format, Version 1.02. Milpitas, CA: C-Cube Microsystems.” 1992.

[10] E. Kee, M. K. Johnson, and H. Farid, “Digital image authentication from JPEG headers,” *IEEE Trans. Inf. forensics Secur.*, vol. 6, no. 3, pp. 1066–1075, 2011.

[11] B. Bayar and M. C. Stamm, “Augmented convolutional feature maps for robust CNN-based camera model identification,” in *2017 IEEE International Conference on Image Processing (ICIP)*, 2017, pp. 4098–4102.

[12] Y. Zhang, J. Goh, L. L. Win, and V. L. L. Thing, “Image Region Forgery Detection: A Deep Learning Approach.,” *SG-CRC*, vol. 2016, pp. 1–11, 2016.

[13] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath, and A. K. Roy-Chowdhury, “Hybrid LSTM and encoder–decoder architecture for detection of image forgeries,” *IEEE Trans. Image Process.*, vol. 28, no. 7, pp. 3286–3300, 2019.

[14] R. M. Joseph and A. S. Chithra, “Literature survey on image manipulation detection,” *Int. Res. J. Eng. Technol.*, vol. 2, no. 4, pp. 56–2395, 2015.

[15] T. K. Huynh, K. V Huynh, T. Le-Tien, and S. C. Nguyen, “A survey on image forgery detection techniques,” in *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF)*, 2015, pp. 71–76.

[16] G. K. Birajdar and V. H. Mankar, “Digital image forgery detection using passive techniques: A survey,” *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, 2013.

[17] R. M. Raju and K. Gopakumar, “An image authentication technique based on cross chaotic map,” in *2014 First International Conference on Computational Systems and Communications (ICCSC)*, 2014, pp. 197–202.

[18] L. Mou, X. Chen, Y. Tian, and T. Huang, “Robust and discriminative image

authentication based on standard model feature," in *2012 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2012, pp. 1131–1134.
[19] M. Rajawat and D. S. Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 638–642.
[20] X. Wang, J. Xue, Z. Zheng, Z. Liu, and N. Li, "Image forensic signature for content authenticity analysis," *J. Vis. Commun. Image Represent.*, vol. 23, no. 5, pp. 782–797, 2012.
[21] A. Baumy, M. Abdalla, N. F. Soiliman, and F. E. Abd El-Samie, "Efficient implementation of pre-processing techniquesfor image forgery detection," in *2017 Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)*, 2017, pp. 53–56.
[22] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 1849–1853, 2015.
[23] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in *2014 IEEE International Conference on Image Processing (ICIP)*, 2014, pp. 5302–5306.
[24] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Multi-clue image tampering localization," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 125–130.
[25] L. Bondi, L. Baroffio, D. Güera, P. Bestagini, E. J. Delp, and S. Tubaro, "First steps toward camera model identification with convolutional neural networks," *IEEE Signal Process. Lett.*, vol. 24, no. 3, pp. 259–263, 2016.
[26] T. Gowda, K. Hundman, and C. A. Mattmann, "An approach for automatic and large scale image forensics," in *Proceedings of the 2nd International Workshop on Multimedia Forensics and Security*, 2017, pp. 16–20.
[27] D. S. Sellva Manoj and G. Sujatha, "Digitized authentication for image forensics," *Int. J. Sci. Eng. Res*, vol. 4, no. 5, pp. 1771–1774, 2013.
[28] F. de O. Costa, M. Eckmann, W. J. Scheirer, and A. Rocha, "Open set source camera attribution," in *2012 25th SIBGRAPI conference on graphics, patterns and images*, 2012, pp. 71–78.
[29] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 3, pp. 1003–1017, 2012.
[30] I.-C. Chang, J. C. Yu, and C.-C. Chang, "A forgery detection algorithm for exemplar-based inpainting images using multi-region relation," *Image Vis. Comput.*, vol. 31, no. 1, pp. 57–71, 2013.
[31] Y.-L. Chen and C.-T. Hsu, "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 396–406, 2011.
[32] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognit.*, vol. 42, no. 11, pp. 2492–2501, 2009.
[33] V. L. L. Thing, Y. Chen, and C. Cheh, "An improved double compression detection method for JPEG image forensics," in *2012 IEEE International Symposium on Multimedia*, 2012, pp. 290–297.

[34] W. Wang, J. Dong, and T. Tan, “Exploring DCT coefficient quantization effects for local tampering detection,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1653–1666, 2014.
[35] F. Zach, C. Riess, and E. Angelopoulou, “Automated image forgery detection through classification of JPEG ghosts,” in *Joint DAGM (German Association for Pattern Recognition) and OAGM Symposium*, 2012, pp. 185–194.
[36] C. Rey and J.-L. Dugelay, “A survey of watermarking algorithms for image authentication,” *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 6, pp. 1–9, 2002.
[37] T.-T. Ng, S.-F. Chang, C.-Y. Lin, and Q. Sun, “Passive-blind image forensics,” in *Multimedia security technologies for digital rights management*, Elsevier, 2006, pp. 383–412.
[38] T.-T. Ng, S.-F. Chang, and Q. Sun, “Blind detection of photomontage using higher order statistics,” in *2004 IEEE international symposium on circuits and systems (IEEE Cat. No. 04CH37512)*, 2004, vol. 5, pp. V–V.
[39] T.-T. Ng, S.-F. Chang, and Q. Sun, “A data set of authentic and spliced image blocks,” *Columbia Univ. ADVENT Tech. Rep.*, pp. 203–2004, 2004.
[40] W. Wang, J. Dong, and T. Tan, “A survey of passive image tampering detection,” in *International Workshop on Digital Watermarking*, 2009, pp. 308–322.
[41] T. S. Aditya, “Survey on passive methods of image tampering detection,” in *2010 International Conference on Communication and Computational Intelligence (INCOCCI)*, 2010, pp. 431–436.
[42] R. R. Ali and K. M. Mohamad, “Rx_myKarve carving framework for reassembling complex fragmentations of JPEG images,” *J. King Saud Univ. Inf. Sci.*, 2019.
[43] R. Parthiban, “Image Authentication using JPEG Headers,” vol. 3, no. 4, pp. 323–326, 2014.
[44] P. Mullan, C. Riess, and F. Freiling, “Forensic source identification using JPEG image headers: The case of smartphones,” *Digit. Investig.*, vol. 28, pp. S68–S76, 2019.
[45] P. Jain and A. S. Rajawat, “Fragile watermarking for image authentication: survey,” *Int. J. Electron. Comput. Sci. Eng.*, vol. 1, no. 3, pp. 1232–1237, 2012.
[46] R. Li, C.-T. Li, and Y. Guan, “Inference of a compact representation of sensor fingerprint for source camera identification,” *Pattern Recognit.*, vol. 74, pp. 556–567, 2018.
[47] A. Tuama, F. Comby, and M. Chaumont, “Camera model identification with the use of deep convolutional neural networks,” in *2016 IEEE International workshop on information forensics and security (WIFS)*, 2016, pp. 1–6.
[48] “http://www.jpeg.org/,” [Online]. Available: http://www.jpeg.org/.
[49] “http://www.jpeg.org/jpegls.html,” [Online]. Available: http://www.jpeg.org/jpegls.html.
[50] “https://www.wikipedia.org/.” https://www.wikipedia.org/.

واژه‌نامه مرتب براساس حروف الفبای انگلیسی

Application Data Marker	شاخص دادگان کاربردی
Associated Statistics Area	هم محدوده آماری مربوطه
Application Marker	شاخص‌های کاربردی
Abbreviated Format	فرمت مخفف شده
Arithmetic Coding Conditioning Tables	جدول‌های شرطی مربوط به کدینگ حسابی
Active Forgery Detection	تشخیص جعل فعال
Augmented Convolutional Feature Maps (ACFM)	نقشه‌های ویژگی درهم‌پیچیده افزودنی
Authentication	احراز هویت
Active	فعال
Automatic Weapons	سلاح‌های خودکار
Alternatives	جایگزین
Arithmetic Encoding	کدینگ حسابی
Blind	کور
Blur	تار کردن
Binary Mask	ماسک دودویی
Blocking	مسدود کردن
Baseline Sequential Process	فرآیند رشته‌ای (دنباله‌ای) پایهٔ مبتنی بر DCT
Component Identifier	معرف مؤلفه
Compression	فشرده‌سازی
Carving	بازسازی
Camera Based	مبتنی بر دوربین
Cloning	کپی و انتقال
Content-preserving	حفظ محتوا
Content-changing	بدون حفظ محتوا
Contrast Enhancement	تقویت کنتراست
Copy-move	کپی– انتقال
Convolutional Neural Networks (CNNs)	شبکه‌های عصبی درهم‌پیچیده
Content-Based	مبتنی بر محتوا
Compact Representation	نمایشی متراکم
Color Filter Array (CFA)	آرایه فیلتر رنگ
Capturing	ضبط کردن
Define Number of Lines (DNL)	تعریف تعداد سطرها
Define Number of Lines Marker	شاخص محل تعریف تعداد سطرها
Define Huffman Table Marker (DHT)	شاخص معرف جدول هافمن
Define Quantization Table Marker (DQT)	شاخص معرف جدول کوانتیزاسیون
Defind Restart Interval (DRI)	بازه شروع مجدد تعریف شده

DeQuantization	روند عکس کوانتیزاسیون
Digital Watermarking	ته نقش نگاری دیجیتال
Double Compression	فشرده‌سازی مضاعف
Download	بارگیری
Deep Learning	یادگیری عمیق
Downsampling	کاهش نمونه‌برداری
Decoder Network	شبکه کدگشا
Double	مضاعف
De-Noising	حذف نویز
Entropy Coded Data Segments	قطعات دادگان کد شدهٔ مبتنی بر آنتروپی
End of Image (EOI)	انتهای تصویر
End of Spectral Selection	پایان انتخاب طیفی
End Of Image Marker	شاخص انتهای تصویر
Encoder	کدگذار
Encoder Network	شبکه کدگذار
Evolutionary	تکاملی
Extreme Learning Machine (ELM)	ماشین یادگیری افراطی
Extension	پسوندها
Extend	گسترش
Entropy Encoding	کدگذاری آنتروپی
Exchangeable Image File Format (EXIF)	قالب فایل تصویری تعویض‌پذیر
Frame Header Length	طول سرآیند فریم
Facebook	فیس‌بوک
Fragmentation	تکه‌تکه شدن
Format Based	مبتنی بر فرمت
Forensics	جرم‌شناسی
Forgery Detection	تشخیص جعل
Frequency Domain Correlation	همبستگی دامنه فرکانس
Fingerprint	اثر انگشت
Fragile Watermarking	ته نقش نگاری شکننده
Semi-Fragile Watermarking	ته نقش نگاری نیمه شکننده
Frame Header	سرآیند فریم
Geometric Based	مبتنی بر هندسه
Genetic Algorithm	الگوریتم ژنتیک
Gaussian Conditional Random	تصادفی شرطی گوسین
Global Positioning System (GPS)	موقعیت مکانی
Horizontal Sampling Factor	فاکتور نمونه‌برداری افقی
Huffman tables	جدول‌های هافمن
Header	سرآیند
Huffman Coding	کدینگ هافمن

Heatmap	نقشه رنگی
Hierarchy Feature Learning	یادگیری ویژگی‌های سلسله مراتبی
Homomorphic Transform	تبدیل همگن
High-Pass Filtering	فیلتر بالا گذر
Huffman Encoding	کدینگ هافمن
Huffman Table Destination Identifier	معرف آدرس جدول هافمن
Image file directory (IFD)	راهنمای فایل تصویر
Image Metadata Forensics	جرم‌شناسی ابر اطلاعات تصویر
Illuminant Estimators	برآوردگرهای روشنایی
Image Metadata	ابر اطلاعات تصویر
International Mobile Equipment Identity (IMEI)	هویت بین‌المللی تجهیزات تلفن همراه
Illumination Components	مولفه‌های درخشندگی
Irfan View	نمایش تصاویر
Interoperability	قابلیت سازگاری
Joint Photographic Experts Group (JPEG)	گروه مشترک متخصصان عکاسی
Japanese Electronics Industry Development Association (JEIDA)	شرکت خدمات مهندسی الکترونیک در ژاپن
JPEG File Interchange Format (JFIF)	قالب تبادل فایل JPEG
Long Short-Term Memory (LSTM)	حافظه کوتاه مدت
Localize	محلی‌سازی
Low-Level Nonlinear Residuals	باقیمانده‌های غیرخطی سطح پایین
Linear Prediction Residuals	باقیمانده‌های پیش‌بینی خطی
Localize Image Manipulations	محلی‌سازی دستکاری‌های تصویر
Localize Tampered Region	محلی‌سازی نواحی دستکاری‌شده
Low-Resolution	وضوح پایین
Linear Discriminant Analysis (LDA)	آنالیز تبعیض آمیز خطی
Lossy	توأم با خطا
Lossless	بدون خطا
Miscellaneous Marker Segments	قطعات شاخص متفرقه
Minimum Coded Unit (MCU)	کوچک‌ترین واحد کد شده
Metadata	ابر اطلاعات
Marker Segment	قطعهٔ شاخص
Markers	شاخص‌ها
Markers Segments	قطعات شاخص
Marker	شاخص
Manipulation	دستکاری
Median Filtering	فیلترهای میانه
Median Filtering Residual (MFR)	باقیمانده فیلتر میانه
Media Forensics Community	جامعه جرم‌شناسی رسانه
Machine learning	یادگیری ماشین
Metric	معیار اندازه‌گیری

Multimedia	چند رسانه‌ای
Modes Of Operation	حالت‌های عملکرد
Number Of Line	تعداد سطرها
Nonlinear Residuals	باقیمانده غیرخطی
Quantization Table	ماتریس کوانتیزاسیون
Online	برخط
Options	گزینه‌ها
Point Transform	تبدیل نقطه‌ای
Predictor	پیش‌بینی کننده (تخمین گر)
Progressive DCT Based Process	فرآیند تصاعدی (جلوسوی) مبتنی بر DCT
Principal Component Analysis (PCA)	تحلیل مؤلفه‌های اصلی
Parameters	پارامترها
Passive Forgery Detection	تشخیص جعل منفعل
Pixel-Based	مبتنی بر پیکسل
Physics Based	مبتنی بر فیزیک محیطی
post-processing	پس پردازش
Passive	منفعل، غیرفعال
Pre-processing	پیش‌پردازش
Peak	نقطه اوج
Probability Density Functions (PDFs)	توابع چگالی احتمال
Principal Point	نقطه اصلی
Primary	اولیه
Quantization	چندی‌سازی
Quantization Table Element	المانی از جدول کوانتیزاسیون
Quantization Table Destination Identifier	معرف آدرس جدول کوانتیزاسیون
Quantization Table Destination Selector	انتخاب‌گر آدرس جدول کوانتیزاسیون
Quantization Table Element Precision	دقت المان‌های موجود در جدول کوانتیزاسیون
Restart Marker	شاخص شروع مجدد
Resampling	نمونه‌برداری مجدد
Reassembling	تجمع مجدد
Recompressed	فشرده‌سازی مجدد
Radon Transform	تبدیل رادون
Random Walker Segmentation	تقسیم‌بندی تصادفی واکر
Resizing	تغییر اندازه
Recovery	بازیابی
Residual Pattern Noise	الگوی نویز باقیمانده
Registering	ثبت
Run Length Encoding (RLE)	کدگذاری طول گام
Robust	مقاوم

Start of Image (SOI)	آغاز تصویر
Sampling Factors	فاکتورهای نمونه‌برداری
Start Of Frame Marker	شاخص آغاز فریم
Successive Approximation bit Position Low or Point Transform	موقعیت پائین بیت تخمینی در دنباله یا تخمین نقطه‌ای
Successive approximation bit Position High	موقعیت بالای بیت تخمینی در دنباله
Start Of Frame (SOF)	آغاز فریم
Star Of Image Marker	شاخص آغاز تصویر
Start Of Scan (SOS)	آغاز اسکن
Scan Component Selector	انتخاب‌گر مؤلفهٔ اسکن
Start of Spectral or Predictor Selection	محل شروع انتخاب طیفی یا تخمین‌گر
Sample precision	دقت هر نمونه
Start Of Scan Marker	شاخص آغاز اسکن
Scan Header	سرآیند اسکن
Scan Header Length	طول سرآیند اسکن
Semantic Meaning	مفهوم معنایی
Splicing	چسباندن
Statistical	آماری
Strategies	استراتژی‌ها
Statistical Fingerprints	اثرانگشت‌های آماری
Spatial Maps	نقشه‌های مکانی
Structure-Based	مبتنی بر محتوا
Stacked Auto-Encoders (SAE)	خود کدگذار پشته‌ای
Steganography	نهان‌نگاری
Subtle Inconsistencies	ناسازگاری‌های غیرقابل تشخیص
Support Vector Machine (SVM)	ماشین بردار پشتیبان
Software Stack	پشته نرم‌افزار
Signature	امضا
Sensor Noise	حسگر نویز
Supervised Learning	یادگیری با ناظر
Sensor Pattern Noise (SPN)	الگوی نویز حسگر
Sequential DCT Based Process	فرآیند رشته‌ای مبتنی بر DCT
Smartphones	تلفن‌های هوشمند
Table Class	کلاس (گروه) جدول
Table – Specification data	دادگان مربوط به مشخصات جدول
Tampered	دستکاری
Thumbnail	تصویر بندانگشتی
Texture Properties	خصوصیات بافت
Thresholding estimation	تخمین آستانه
Upsampling	افزایش نمونه‌برداری
Vertical Sampling Factor	فاکتور نمونه‌برداری عمودی

Watermark	ته نقش نگاری
Watermark Embedded	تعبیه نقش نگاری

واژه‌نامه مرتب براساس حروف الفبای فارسی

احراز هویت	Authentication
ابر اطلاعات	Metadata
آغاز تصویر	Start of Image (SOI)
انتهای تصویر	End of Image (EOI)
المانی از جدول کوانتیزاسیون	Quantization Table Element
آغاز فریم	Start Of Frame (SOF)
آغاز اسکن	Start Of Scan (SOS)
انتخاب‌گر مؤلفهٔ اسکن	Scan Component Selector
انتخاب‌گر آدرس جدول کوانتیزاسیون	Quantization Table Destination Selector
آرایه فیلتر رنگ	Color Filter Array (CFA)
اثر انگشت	Fingerprint
الگوریتم ژنتیک	Genetic Algorithm
ابر اطلاعات تصویر	Image Metadata
آنالیز تبعیض آمیز خطی	Linear Discriminant Analysis (LDA)
الگوی نویز باقیمانده	Residual Pattern Noise
آماری	Statistical
استراتژی‌ها	Strategies
اثرانگشت‌های آماری	Statistical Fingerprints
امضا	Signature
اولیه	Primary
الگوی نویز حسگر	Sensor Pattern Noise (SPN)
افزایش نمونه‌برداری	Upsampling
بازه شروع مجدد تعریف شده	Defind Restart Interval (DRI)
بازسازی	Carving
بدون حفظ محتوا	Content-changing
بارگیری	Download
برآوردگرهای روشنایی	Illuminant Estimators
باقیمانده‌های غیرخطی سطح پایین	Low-Level Nonlinear Residuals
باقیمانده‌های پیش‌بینی خطی	Linear Prediction Residuals
باقیمانده فیلتر میانه	Median Filtering Residual (MFR)
باقیمانده غیرخطی	Nonlinear Residuals
برخط	Online
بازیابی	Recovery
تخمین آستانه	Thresholding estimation
بدون خطا	Lossless
پیش‌بینی کننده (تخمین گر)	Predictor
پارامترها	Parameters

End of Spectral Selection	پایان انتخاب طیفی
post-processing	پس پردازش
Pre-processing	پیش‌پردازش
Software Stack	پشته نرم‌افزار
Extension	پسوندها
Entropy Encoding	کدگذاری آنتروپی
Watermark	ته نقش نگاری
Semi-Fragile Watermarking	ته نقش نگاری نیمه شکننده
Watermark Embedded	تعبیه نقش نگاری
Point Transform	تبدیل نقطه‌ای
Digital Watermarking	ته نقش نگاری دیجیتال
Fragile Watermarking	ته نقش نگاری شکننده
Define Number of Lines (DNL)	تعریف تعداد سطرها (DNL)
Number Of Line	تعداد سطرها
Active Forgery Detection	تشخیص جعل فعال
Blur	تار کردن
Contrast Enhancement	تقویت کنتراست
Evolutionary	تکاملی
Fragmentation	تکه‌تکه شدن
Forgery Detection	تشخیص جعل
Gaussian Conditional Random	تصادفی شرطی گوسین
Homomorphic Transform	تبدیل همگن
Principal Component Analysis (PCA)	تحلیل مؤلفه‌های اصلی
Passive Forgery Detection	تشخیص جعل منفعل
Probability Density Functions (PDFs)	توابع چگالی احتمال
Reassembling	تجمع مجدد
Radon Transform	تبدیل رادون
Random Walker Segmentation	تقسیم‌بندی تصادفی واکر
Resizing	تغییر اندازه
Thumbnail	تصویر بندانگشتی
Lossy	توأم با خطا
Smartphones	تلفن‌های هوشمند
Irfan View	نمایش تصاویر
Registering	ثبت
Huffman tables	جدول‌های هافمن
Arithmetic Coding Conditioning Tables	جدول‌های شرطی مربوط به کدینگ حسابی
Forensics	جرم‌شناسی، تشخیص تصاویر جعلی
Image Metadata Forensics	جرم‌شناسی ابر اطلاعات تصویر
Media Forensics Community	جامعه جرم‌شناسی رسانه
Alternatives	جایگزین

Quantization	چندی‌سازی
Splicing	چسباندن
Multimedia	چند رسانه‌ای
Content-preserving	حفظ محتوا
De-Noising	حذف نویز
Long Short-Term Memory (LSTM)	حافظه کوتاه مدت
Sensor Noise	حسگر نویز
Modes Of Operation	حالت‌های عملکرد
Stacked Auto-Encoders (SAE)	خود کدگذار پشته‌ای
Texture Properties	خصوصیات بافت
Sample precision	دقت هر نمونه
Quantization Table Element Precision	دقت المان‌های موجود در جدول کوانتیزاسیون
Table – Specification data	دادگان مربوط به مشخصات جدول
Manipulation	دستکاری
Tampered	دستکاری
Encoder	کدگذار
Image File Directory (IFD)	راهنمای فایل تصویر
Scan Header	سرآیند اسکن
Frame Header	سرآیند فریم
Automatic Weapons	سلاح‌های خودکار
Header	سرآیند
Japanese Electronics Industry Development Association (JEIDA)	شرکت خدمات مهندسی الکترونیک در ژاپن
Application Data Marker	شاخص دادگان کاربردی
Define Huffman Table Marker (DHT)	شاخص معرف جدول هافمن
Define Quantization Table Marker (DQT)	شاخص معرف جدول کوانتیزاسیون
Markers	شاخص‌ها
End Of Image Marker	شاخص انتهای تصویر
Star Of Image Marker	شاخص آغاز تصویر
Start Of Scan Marker	شاخص آغاز اسکن
Start Of Frame Marker	شاخص آغاز فریم
Application Marker	شاخص‌های کاربردی
Define Number of Lines Marker	شاخص محل تعریف تعداد سطرها
Marker	شاخص
Restart Marker	شاخص شروع مجدد
Convolutional Neural Networks (CNNs)	شبکه‌های عصبی درهم‌پیچیده
Decoder Network	شبکه کدگشا
Encoder Network	شبکه کدگذار

Capturing	ضبط
Scan Header Length	طول سرآیند اسکن
Frame Header Length	طول سرآیند فریم
Passive	غیرفعال، منفعل
Sampling Factors	فاکتورهای نمونه‌برداری
Vertical Sampling Factor	فاکتور نمونه‌برداری عمودی
Horizontal Sampling Factor	فاکتور نمونه‌برداری افقی
Progressive DCT Based Process	فرآیند تصاعدی (جلوسوی) مبتنی بر DCT
Abbreviated Format	فرمت مخفف شده
Active	فعال
Compression	فشرده‌سازی
Double Compression	فشرده‌سازی مضاعف
High-Pass Filtering	فیلتر بالا گذر
Median Filtering	فیلترهای میانه
Photoshop	فتوشاپ
Recompressed	فشرده‌سازی مجدد
Baseline Sequential Process	فرآیند رشته‌ای (دنباله‌ای) پایهٔ مبتنی بر DCT
Sequential DCT Based Process	فرآیند رشته‌ای مبتنی بر DCT
JPEG File Interchange Format (JFIF)	قالب تبادل فایل JPEG
Exchangeable Image File Format (EXIF)	قالب فایل تصویری تعویض‌پذیر
Marker Segment	قطعهٔ شاخص
Miscellaneous Marker Segments	قطعات شاخص متفرقه
Entropy Coded Data Segments	قطعات دادگان کد شدهٔ مبتنی بر آنتروپی
Interoperability	قابلیت سازگاری
Minimum Coded Unit (MCU)	کوچک‌ترین واحد کد شده
Blind	کور
Table Class	کلاس (گروه) جدول
Cloning	کپی و انتقال
Copy-move	کپی– انتقال
Downsampling	کاهش نمونه‌برداری
Huffman Coding	کدینگ هافمن
Options	گزینه‌ها
Extend	گسترش
Joint Photographic Experts Group (JPEG)	گروه مشترک متخصصان عکاسی
Quantization Table Destination Identifier	معرف آدرس جدول کوانتیزاسیون
Successive Approximation bit Position Low or Point Transform	موقعیت پائین بیت تخمینی در دنباله یا تخمین نقطه‌ای

Successive approximation bit Position High	موقعیت بالای بیت تخمینی در دنباله
Start of Spectral or Predictor Selection	محل شروع انتخاب طیفی یا تخمین‌گر
Component Identifier	معرف مؤلفه
Huffman Table Destination Identifier	معرف آدرس جدول هافمن
Binary Mask	ماسک دودویی
Blocking	مسدود کردن
Camera Based	مبتنی بر دوربین
Content-Based	مبتنی بر محتوا
Double	مضاعف
Extreme Learning Machine (ELM)	ماشین یادگیری افراطی
Format Based	مبتنی بر فرمت
Geometric Based	مبتنی بر هندسه
Global Positioning System (GPS)	موقعیت مکانی
Illumination Components	مولفه‌های درخشندگی
Localize	محلی‌سازی
Localize Image Manipulations	محلی‌سازی دستکاری‌های تصویر
Localize Tampered Region	محلی‌سازی نواحی دستکاری‌شده
Metric	معیار اندازه‌گیری
Quantization Table	ماتریس کوانتیزاسیون
Pixel-Based	مبتنی بر پیکسل
Physics Based	مبتنی بر فیزیک محیطی
Passive	منفعل، غیرفعال
Semantic Meaning	مفهوم معنایی
Structure-Based	مبتنی بر محتوا
Support Vector Machine (SVM)	ماشین بردار پشتیبان
Matlab	متلب
Peak	نقطه اوج
Augmented Convolutional Feature Maps (ACFM)	نقشه‌های ویژگی درهم‌پیچیده افزودنی
Compact Representation	نمایشی متراکم
Heatmap	نقشه رنگی
Principal Point	نقطه اصلی
Resampling	نمونه‌برداری مجدد
Spatial Maps	نقشه‌های مکانی
Steganography	نهان‌نگاری
Low-Resolution	وضوح پایین
Associated Statistics Area	هم محدوده آماری مربوطه
Frequency Domain Correlation	همبستگی دامنه فرکانس
International Mobile Equipment Identity (IMEI)	هویت بین‌المللی تجهیزات تلفن همراه
Deep Learning	یادگیری عمیق

Hierarchy Feature Learning	یادگیری ویژگی‌های سلسله مراتبی
Machine learning	یادگیری ماشین
Supervised Learning	یادگیری با ناظر

Abstract

Today, the creation of new imaging equipment and the possibility of easily processing and editing images has led to the production of large volumes of forged images. Therefore, new image Forensics methods for detecting forged images have been introduced. Format-based methods can detect forgery in the compressed image. These methods are mainly used in JPEG image format. among image formats, JPEG format has more abundance and application, So Most cases of image forgery are done in this format. In this paper, a new method for digital images authenticating using JPEG headers is presented. To forge an image, First the output image of the camera is transferred to the relevant software and then the necessary changes are applied to it. One of the most important parameters for detecting forged images is the image source. That is, it must be specified that the image in question was taken from the camera or changed in software. Forgery or changing images is done with the help of various softwares, including Photoshop. One way to identify image modifier software is to use header information. Each camera or software leaves its own footprint in the image header, which allows this footprint to identify the camera model or image modifier software. In this paper, a new algorithm for detecting forgery in image Forensics using information in the JPEG image header is introduced. In this method, first, With regards to the application data in the image JPEG header, the type of editor software or camera model is identifed, and then, according to the other existing information in the header, both the editor software and the camera model are re-identified, and then the header information is re-identifed if the information is inaccurate.

The evaluation results of the proposed methods with the collected database showed that the proposed image authentication method is well done and can be used in Operational systems. Also, in the proposed method, any photo editing with Photoshop can be easily identified without any ambiguity.

Keywords: Forensics, Authentication, Image Processing, Forgery Detection, JPEG Image

Shahrood University of Technology

Faculty of Computer Engineering

M.Sc. Thesis in Artificial Intelligence Engineering

Digital Image Authentication Using JPEG Headers

By: Enam Helalat

Supervisor:
Dr. Mansoor Fateh

Advisor:
Dr. Mohsen Rezvani
Dr. Alireza Tajary

June,2021