Scientific Journal of Electronic & Cyber Defense
Vol. 11, No. 4, Winter 2024, Serial No. 44
ISSN: 2322-4347 , E-ISSN: 2980-8979

Forgery detection in digital images using the hybrid deep learning method

fatemeh zare mehrjardi, ali mohammad latif *, mohsen sardari zarchi

* Professor, Yazd University, Yazd, Iran.

(Received: 2023/08/27, Revised: 2023/11/25, Accepted: 2023/12/16, Published: 2024/01/18)

DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.4.9.6

ABSTRACT

Today, images are used as powerful communication tools and sources of information. In certain applications, such as medicine, justice, and forensics, images serve as evidence. Therefore, the validity of an image is crucial. With the spread and availability of image editing tools, people can easily manipulate images to their advantage. They follow political, cultural, economic, and social issues by adding or removing elements from images, often distributing misinformation. Consequently, forgery detection is one of the most important and challenging topics in the field of computer vision. This research aims to identify forgery and healthy images and pixels using a hybrid deep learning network. In the proposed method, three pre-trained networks—VGG16, MobileNet, and EfficientNetB0—are employed in three different branches. To detect forgery at both the image and pixel levels, the output feature maps from these branches are merged in a concatenate layer. Subsequently, a global average pooling layer and a scoring layer are used to identify forgery and healthy images. Additionally, feature maps combined from the three branches are utilized to create a heat map image for forgery detection. Notably, pixel forgery detection is performed solely using the heat map image generated from the combined network, without relying on ground truth images that specify the forgery area during training. The proposed method is evaluated on the well-known CoMoFod dataset, demonstrating satisfactory performance against forgery images with various geometric transformations and post-processing operations

Keywords: Image forgery detection, Pixel forgery detection, Copy-move forgery, Deep learning.

*Corresponding Author Email: alatif@yazd.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۴، زمستان ۱۴۰۲، ص۹۷-۱۱۴
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی – پژوهشی

تشخیص جعل در تصاویر دیجیتالی با استفاده از روش یادگیری عمیق ترکیبی

فاطمه زارع مهرجردی [۱]، علی‌محمد لطیف *[۲]، محسن سرداری زارچی [۳]

۱. استادیار، دانشگاه میبد، یزد، ایران. ۲. استاد، دانشگاه یزد ، یزد، ایران. ۳. دانشیار، دانشگاه میبد، یزد، ایران.

(دریافت: ۱۴۰۲/۰۶/۰۵، بازنگری: ۱۴۰۲/۰۹/۰۴، پذیرش: ۱۴۰۲/۰۹/۲۵، انتشار: ۱۴۰۲/۱۰/۲۸)

DOR: https://dorl.net/dor/ 20.1001.1.23224347.1402.11.4.9.6

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

امروزه از تصاویر به‌عنوان ابزار ارتباطی قوی و منبعی از اطلاعات استفاده می‌شود. تصاویر در برخی از کاربردها مانند پزشکی، قضایی و پزشکی قانونی به‌عنوان مدرک و شاهد استفاده می‌شوند، بنابراین صحت تصویر مهم است. امروزه با گسترش و دردسترس‌بودن ابزارهای ویرایش تصویر، افراد می‌توانند به‌راحتی تصاویر را دست‌کاری کنند. آن‌ها با اضافه‌کردن بخشی به تصویر یا حذف‌کردن بخشی از تصویر و توزیع اطلاعات غلط اهداف و مشکل‌های سیاسی، فرهنگی، اقتصادی و اجتماعی را دنبال می‌کنند. ازاین‌رو تشخیص جعل تصاویر دیجیتال یکی از موضوع‌های مهم و چالش‌برانگیز در حوزه بینایی کامپیوتر است. در این پژوهش هدف شناسایی تصاویر و پیکسل‌های جعلی و سالم با استفاده از شبکه یادگیری عمیق ترکیبی است. در روش پیشنهادی از سه شبکه از پیش آموزش‌داده‌شده VGG16، MobileNet و EfficientNetB0 در سه انشعاب مختلف استفاده‌شده است. برای تشخیص جعل در دو سطح تصویر و پیکسل، ابتدا نقشه‌های ویژگی خروجی سه انشعاب با هم ادغام‌شده و با استفاده از لایه پولینگ میانگین جهانی و لایه امتیازدهی، تصاویر جعل و سالم تشخیص داده می‌شوند. در ادامه با استفاده از نقشه‌های ویژگی ترکیب‌شده از سه انشعاب بر روی تصاویر جعل، یک تصویر نقشه حرارتی ایجاد می‌شود و محدوده پیکسل‌های جعل مشخص می‌شوند. لازم به ذکر است تشخیص پیکسل‌های جعل تنها با استفاده از تصویر نقشه حرارتی ساخته‌شده از شبکه ترکیبی و بدون نیاز به استفاده از تصاویر حقیقی باینری مشخص‌کننده ناحیه جعل در فرآیند آموزش انجام‌شده است. روش پیشنهادی بر روی پایگاه‌داده CoMoFod ارزیابی‌شده است. نتایج ارزیابی‌ها عمل‌کردن مطلوب روش پیشنهادی را در برابر تصاویر جعل با انواع تبدیل‌های هندسی و عملیات پس‌پردازش نشان می‌دهد.

کلید واژه‌ها: تشخیص تصویر جعل، تشخیص پیکسل جعل، جعل کپی- انتقال، یادگیری عمیق.

۱. مقدمه

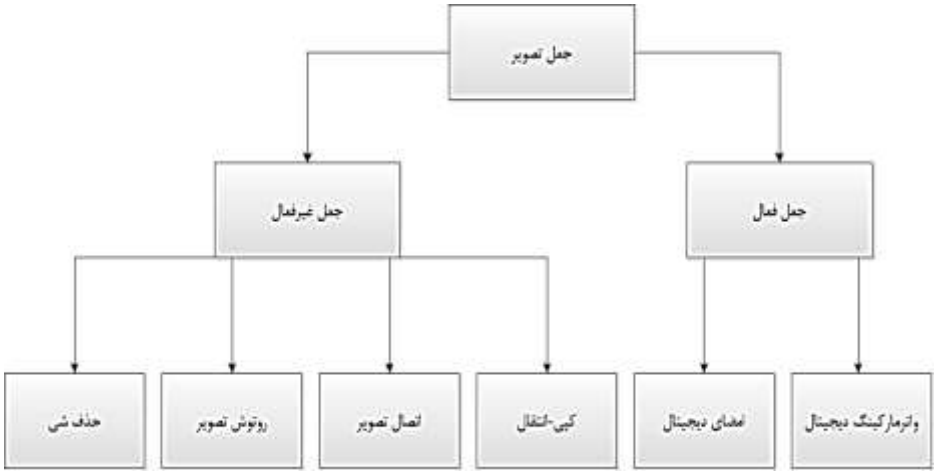
تصویر یکی از ابزارهای ارتباطی مهم بین انسان‌ها است. با توسعه و گسترش دوربین‌های دیجیتالی و گوشی‌های هوشمند در هر لحظه از زمان و مکان تصویربرداری به‌راحتی امکان‌پذیر شده است. در بعضی از کاربردها تصویر دیجیتال به‌عنوان مدرک مورداستفاده قرار می‌گیرد.

جعل تصویر به معنای دست‌کاری در تصویر دیجیتال است. این دست‌کاری برای اهدافی مانند پنهان‌کردن یا اضافه‌کردن اطلاعات به تصویر است. با جعل تصویر، یکپارچگی و اصالت تصویر در ساختار و بافت آن دست‌کاری می‌شود. اگر تصویر به‌عنوان مدرک دست‌کاری شود دیگر قابل‌اعتماد نخواهد بود [۱].

در تحقیق‌های موجود انواع روش‌های تشخیص جعل تصویر به‌صورت شکل ۱ گروه‌بندی‌شده است [۲و۳]. در این گروه‌بندی تشخیص جعل به دو گروه فعال[1] و غیرفعال[2] تقسیم می‌شود [۴]. گروه فعال با جاسازی اطلاعات درون تصاویر اصلی آن را دست‌کاری می‌کند. این گروه برای تشخیص جعل یکپارچگی اطلاعات را بررسی می‌کند تا مشخص شود تصویر دست‌کاری شده است یا خیر؟. این گروه شامل روش‌های واترمارکینگ دیجیتال و امضای دیجیتال است. این روش‌ها به نرم‌افزار و سخت‌افزار خاصی نیاز دارند تا اطلاعات احراز هویت را در تصاویر وارد یا از آن استخراج کنند [۵-۱۱]. گروه فعال به تصویر اصلی برای درج امضای دیجیتال یا واترمارکینگ دیجیتال نیاز دارد و در صورت کمبود آن‌ها این روش غیرممکن و غیر موثر است.

[1] Active Approach
[2] Passive Approach

*Corresponding Author E-mail: alatif@yazd.ac.ir



شکل۱: طبقه‌بندی جعل تصاویر [۱۲]

گروه غیرفعال با تجزیه‌وتحلیل محتوا و ساختار تصویر و کشف ناهماهنگی‌ها، جعل بودن یا نبودن تصویر را تشخیص می‌دهد [۳] . این گروه شامل روش‌های جعل کپی- انتقال[1]، اتصال[2] یا الحاق تصویر، روتوش کردن تصویر[3] یا حذف بخشی از تصویر[4] است. در گروه غیرفعال به دانش قبلی در مورد تصویر احتیاج نیست، ازاین‌رو این روش بیش‌تر موردتوجه محققان قرار گرفته است [۶و۷] . در این پژوهش از گروه غیرفعال استفاده‌شده است.

روش کپی- انتقال یکی از ساده‌ترین و رایج‌ترین روش‌های دست‌کاری تصاویر است. این روش بخشی از تصویر را کپی و در جای دیگر همان تصویر انتقال می‌دهد. انگیزه چنین جعلی پنهان‌کردن بخشی از تصویر، تأکید بر بخشی از تصویر و درج اطلاعات غلط در تصویر است. ازآنجاکه بخش کپی شده متعلق به همان تصویر است، از لحاظ پویایی رنگ با بقیه تصویر سازگاری دارد. همراه با عمل کپی و انتقال، عملیات دیگری مانند چرخش، مقیاس‌بندی، محوکردن، تغییر روشنایی، فشرده‌سازی و افزودن نویز هم انجام می‌شود تا ناحیه دست‌کاری شده برای انسان قابل‌توجه نباشد [۷و۱۳] .

روش اتصال با کپی‌کردن یک یا چند بخش از تصویر و انتقال آن به تصویر دیگر عمل دست‌کاری را انجام می‌دهد. انگیزه چنین دست‌کاری، اضافه‌کردن اطلاعات به تصویر است. هنگامی‌که تصاویر به هم متصل می‌شوند، تصویر حاصل دارای خطوط، لبه‌ها و نواحی تار در محل اتصال است. توسعه ابزارهای ویرایش تصویر باعث شده است که این موارد اضافی به‌خوبی با تصویر ادغام‌شده و انسان قادر به تشخیص جعل نیست [۷و۱۴] .

روتوش تصویر را می‌توان نوع خفیف دست‌کاری تصاویر دیجیتال دانست. این روش تصویر را به طور قابل‌توجهی دست‌کاری نمی‌کند و فقط ویژگی‌های خاصی از تصویر را تغییر می‌دهد. این روش برای ویراستاران مفید است، به‌گونه‌ای که اکثر جلد مجله‌ها از این روش و با افزایش یا کاهش ویژگی‌های خاصی از تصویر برای جذاب‌تر کردن آن استفاده می‌کنند [۷و۱۵] .

حذف شی در تصویر به‌عنوان یک جعل مخرب است؛ زیرا ممکن است محتوای معنایی تصویر را تغییر دهد. تکنیک‌های حذف شی با دو روش کپی - انتقال و نقاشی درون تصویر[5] انجام می‌شوند. روش کپی- انتقال با کپی کردن بخشی از تصویر و چسباندن آن بر شی موردنظر، شی را حذف می‌کند. روش نقاشی درون تصویر برای بازیابی اطلاعات آسیب‌دیده و حذف خراش‌های عکس‌های قدیمی ارائه شد. در این روش برای حذف اشیا از پر کردن محل شی با پیکسل‌های اطراف آن استفاده می‌شود. نقاشی درون تصویر می‌تواند به طور هم‌زمان هم سازگاری بافت و هم ساختار را حفظ کند [۱۶] .

در ادامه سایر بخش‌های پژوهش به‌صورت زیر سازمان‌دهی شده است. در بخش دوم پیشینه تحقیق و مروری بر ادبیات این موضوع آورده شده است. در بخش سوم معرفی مختصری درباره مفاهیم اولیه از قبیل پایگاه‌داده‌های موجود در زمینه جعل کپی – انتقال، معیارهای ارزیابی تشخیص جعل، معماری‌های یادگیری عمیق و اصطلاحات مورداستفاده در این پژوهش بیان‌شده است. روش پیشنهادی در بخش چهارم ارائه‌شده است و نوآوری تشخیص جعل در دو سطح تصویر و پیکسل توضیح داده شده است. در بخش پنجم نتایج روش پیشنهادی و مقایسه با سایر کارها ذکرشده است. در نهایت نتیجه‌گیری نهایی پژوهش در بخش ششم آورده شده است.

۲. پیشینه تحقیق

باتوجه‌به مطالعه‌های انجام‌شده، الگوریتم‌های تشخیص جعل کپی – انتقال را می‌توان به دو گروه سنتی و مبتنی بر یادگیری عمیق تقسیم کرد [۱۷] . روش سنتی خود به دو روش بلوک‌بندی و

[1] Copy-Move Forgery
[2] Image Splicing
[3] Image Retouching
[4] Object Removal
[5] Inpainting

یافتن نقاط کلیدی در تصویر طبقه‌بندی می‌شود.

در روش بر پایهٔ بلوک‌بندی ابتدا تصویر به نواحی مستطیلی یا دایره‌ای‌شکل همپوشان یا غیرهم‌پوشان تقسیم می‌شود. سپس برای هر کدام از این بلوک‌ها یک بردار ویژگی با استفاده از الگوریتم‌های تبدیل کسینوسی گسسته[1]، ویژگی‌های بافت، ویژگی‌های لحظات ثابت مانند روش زرنیک[2]، تبدیل قطبی[3] و روش‌های کاهش ابعاد و غیره محاسبه می‌شود. در مرحله بعد بردارهای ویژگی مشابه با استفاده از مرتب‌سازی، هم‌بستگی و فاصله اقلیدسی با هم انطباق می‌یابند و حمله کپی- انتقال تشخیص داده می‌شود. پیچیدگی محاسباتی این روش بالا است و در برابر برخی از تبدیل‌های هندسی و عملیات پس‌پردازش عملکرد ضعیفی دارند [۶ و ۱۸].

در روش‌های مبتنی بر نقاط کلیدی نیازی به تقسیم تصویر به بلوک نیست و از ویژگی‌های محلی مانند گوشه‌ها و یال‌ها استفاده می‌شود. هر ویژگی با یک توصیفگر بیان می‌شود و سپس ویژگی‌های مشابه تطبیق می‌یابند. در روش مبتنی بر نقاط کلیدی، ویژگی با استفاده از روش‌های مختلف مانند SIFT[4]، SURF[5] و FAST[6] بدون تقسیم‌بندی تصویر استخراج می‌شود. نقاط ویژگی با استفاده از رویکردهای مختلف مانند خوشه‌بندی، فاصله اقلیدسی و نزدیک‌ترین همسایگی با یکدیگر مطابقت داده می‌شوند و در صورت تطبیق، جعل مشخص می‌شود. این روش دارای محاسبه کم‌تر و مقاومت مناسبی در برابر تبدیل‌های هندسی است [۶ و ۱۹].

امروزه روش‌های یادگیری عمیق در بسیاری از مسائل بینایی کامپیوتر به‌صورت گسترده استفاده‌شده و نتایج خوبی را به دست آورده است. یادگیری عمیق زیرمجموعه‌ای از روش‌های یادگیری ماشین است و از مفهوم یادگیری بازنمایی استفاده می‌کند. برخلاف روش‌های مبتنی بر بلوک و نقاط کلیدی که شامل چندین مرحلهٔ مجزا برای حل مسائل هستند، روش‌های یادگیری عمیق ویژگی‌های سطح بالا را به‌صورت خودکار از داده‌ها استخراج می‌کنند و از استخراج ویژگی به‌صورت دستی جلوگیری می‌کند.

یکی از مشکل‌های مهم روش‌های یادگیری عمیق نیاز به داده زیاد برای آموزش شبکه است. برخی از مسائل موجود در حوزه بینایی کامپیوتر دارای مجموعه‌داده اندکی هستند. برای حل این مشکل، اکثر محققان به دلیل کمبود پایگاه‌داده از شبکه‌های از پیش آموزش‌داده‌شده[7] مانند VGG16، ResNet، AlexNet، MobileNet بر روی پایگاه‌داده بزرگ Imagenet، تکنیک یادگیری انتقالی[8] و تنظیم دقیق[9] شبکه با مجموعه‌داده موردنظر استفاده می‌کنند [۲۰و۲۱] . در ادامه چند نمونه تحقیق‌های انجام‌شده در زمینه تشخیص جعل بیان‌شده است.

هویدا و همکاران [۲۲] روش تشخیص جعل کپی- انتقال را بر اساس ویژگی‌های ترکیبی ارائه کردند. آن‌ها از ترکیب توصیفگرهای SIFT، KAZE، HOG و Zernike در جهت آشکارسازی جعل‌های کپی- انتقال استفاده کردند. در این روش برای کاهش محاسبات از الگوریتم ژنتیک در جهت بهینه‌سازی توصیفگرها و از الگوریتم تحلیل مؤلفه اصلی برای کاهش ابعاد ویژگی استفاده‌شده است.

Sreelakshmy و همکاران [۲۳] از ترکیب دو روش مبتنی بر بلوک‌بندی و نقاط کلیدی استفاده کردند. به این صورت که ابتدا تصویر اصلی به بلوک‌هایی تقسیم‌شده و از هر بلوک تصویر نقاط کلیدی استخراج می‌شود. اگر نقاط کلیدی مشابه مشخص‌شده دو بلوک، از حد آستانه فراتر باشد آن دو بلوک به‌عنوان نواحی جعل در نظر گرفته می‌شوند.

در مقاله [۲۴] تصویر به بلوک‌های مربعی تقسیم‌بندی شده و با استفاده از روش تبدیل موجک ویژگی‌هایی از هر بلوک استخراج می‌شود. برای کاهش ابعاد ویژگی از تبدیل گسسته کسینوسی استفاده‌شده است. بعد از تطبیق بردارهای ویژگی، نواحی جعل با استفاده از عملیات مورفولوژی گزارش می‌شوند.

Koshy و همکاران [۲۵] از هر دو روش تقسیم‌بندی بلوکی و تطبیق نقاط کلیدی استفاده کردند. ابتدا تصویر به بلوک‌های نامنظم و غیرهم‌پوشان تقسیم‌شده و سپس نقاط کلیدی هر بلوک به‌عنوان ویژگی‌های بلوک استخراج می‌شوند. سپس از الگوریتم‌های تطبیق برای مطابقت ویژگی‌های بلوک استفاده‌شده است. این روش مناطق مشکوک به جعل را مشخص می‌کند. برای تعیین مناطق دقیق و یکپارچه جعل، از عملیات مورفولوژی استفاده‌شده است.

در مقاله‌های [۲۶و۲۷]روشی با استفاده از شبکه عصبی پیچشی برای تشخیص جعل کپی- انتقال پیشنهادشده است. در این روش به دلیل کمبود داده در حوزه جعل از شبکه‌های از پیش آموزش‌دیده شده با پایگاه‌داده بزرگ Imagenet استفاده‌شده است و شبکه با داده‌های موجود تنظیم می‌شود. در خروجی تصاویر در دودسته تصاویر اصلی و تصاویر جعل دسته‌بندی می‌شوند.

Agarwal و همکاران [۲۸] از یادگیری عمیق برای شناسایی جعل استفاده کردند. در این روش تصاویر جعلی با استفاده از روش خوشه‌بندی خطی بخش‌بندی می‌شوند و سپس با استفاده از شبکه VGGNet ویژگی‌های این بخش‌ها استخراج می‌شوند. پس از استخراج ویژگی، عمق هر پیکسل برای مقایسه بلوک‌ها ساخته می‌شود. با استفاده از الگوریتم تطابق، بخش‌های مشکوک پیداشده و در پایان‌بخش‌هایی که بیش‌ترین تطابق بر اساس ویژگی کلیدی را دارند به‌عنوان بخش‌های جعل شناسایی می‌شوند.

[1] Discrete Cosine Transform(DCT)
[2] Zernike moments
[3] Polar Complex Exponentional Transform(PCET)
[4] Scale Invariant Feature Transform(SIFT)
[5] Speeded Up Robust Features(SURF)
[6] Features from Accelerated Segment Test(FAST)
[7] Pre-trained
[8] Transfer learning
[9] Fine tune

در مقاله [۲۹] دو معماری یادگیری عمیق برای تشخیص جعل پیشنهادشده است. در معماری اول، شبکه عصبی پیچشی طراحی‌شده و با تعداد لایه‌های پیچشی و لایه‌های کاملاً متصل و اندازه فیلترهای متفاوت مورد ارزیابی قرار گرفته است. در معماری دوم از مفهوم یادگیری انتقالی و شبکه VGGNet استفاده‌شده است. نتایج ارزیابی‌ها نشان داده است که معماری دوم عملکرد بهتری داشته است.

Goel و همکاران [۳۰] از شبکه عصبی پیچشی دو شاخه‌ای برای تشخیص جعل استفاده کردند. در هر شاخه فیلترها با اندازه متفاوت استفاده‌شده‌اند تا ویژگی‌ها با ابعاد مختلف استخراج شوند و ویژگی‌های استخراج‌شده از دوشاخه با هم ترکیب و تصاویر در دودسته اصلی و جعلی شناسایی شوند.

Abbas و همکاران [۳۱] برای تشخیص جعل از دو معماری VGGNet smaller و MobileNetv2 استفاده کردند. آن‌ها از ترکیب سه پایگاه‌داده CoMofod، MICC-F2000 و CASIA V2.0 برای ارزیابی استفاده کردند. نتایج ارزیابی‌ها نشان می‌دهد که معماری MobilenetV2 عملکرد بهتری در برابر حمله‌های تغییر روشنایی، تار شدن، اضافه‌کردن نویز و تغییرهای هندسی دارد.

Doegar و همکاران [۳۲] برای تشخیص و دسته‌بندی تصاویر جعل و سالم از یادگیری عمیق استفاده کردند. در این روش از معماری Alexnet برای استخراج ویژگی استفاده شد. برای هر یک از تصاویر برداری ۴۰۹۶تایی به دست آمد. سپس طبقه‌بند ماشین بردار پشتیبان با استفاده از این ویژگی‌ها تصاویر را در دودسته سالم و جعل طبقه‌بندی کرد.

در مقاله [۳۳] هدف طبقه‌بندی تصاویر سالم و جعل با کمک یادگیری عمیق برای کشف جعل به دو روش کپی- انتقال و اتصال است. در این روش از شبکه کانولوشنی از قبل آموزش‌داده‌شده با تعداد لایه‌های کم و بدون لایه پولینگ استفاده‌شده است.

پایگاه‌داده شامل تصاویر بدون انتقال و با تبدیل DCT و تصاویر انتقال‌یافته به فضای رنگی YCbCr است و شبکه آموزش داده می‌شود. از یادگیری انتقالی و شبکه‌های VGG16، VGG19 و ResNet152 استفاده‌شده است. لایه پولینگ، لایه رایج در مدل‌های کانولوشنی است که در این تحقیق حذف‌شده است. دلیل حذف این است که ویژگی‌هایی که برای تشخیص جعل مناسب هستند در لایه‌های اولیه هستند. لایه پولینگ بیشینه برای کاهش بعد استفاده می‌شود که باعث ازدست‌رفتن اطلاعات مهم می‌شود.

برای جبران عدم حضور لایه مذکور فیلترهای با اندازه‌بزرگ استفاده‌شده است. فیلترها با اندازه ۳۲ و ۲۰ در لایه اول و دوم استفاده‌شده است که باعث شده دستیابی به اطلاعات مفید و کاهش ابعاد هم‌زمان انجام شود. روش ذکرشده برای تصاویر بدون انتقال نتیجه خوبی دارد.

در مقاله [۳۴] از ترکیب روش بلوک‌بندی و یادگیری عمیق برای تشخیص تصاویر جعل استفاده می‌شود. در این روش ابتدا تصاویر به بلوک‌هایی تقسیم‌شده و بر روی هر بلوک تبدیل‌های مثلثاتی و تبدیل موجک گسسته اعمال می‌شود. سپس از شبکه عصبی کانولوشنی برای استخراج ویژگی استفاده‌شده و تصویر در دودسته سالم و جعل طبقه‌بندی می‌شود.

از مفهوم تلفیق در تصمیم‌گیری و ویژگی می‌توان استفاده کرد. Doegar و همکاران [۳۵] از روش تلفیق تصمیم‌گیری استفاده کردند و سه معماری یادگیری عمیق به نام‌های SqueezeNet، MobileNetV2 و ShuffleNet را با هم تلفیق کردند. استفاده از این سیستم تلفیقی در دوفاز انجام‌شده است. فاز اول از وزن‌های از پیش آموزش‌داده‌شده این معماری‌ها و فاز دوم از وزن‌های تنظیم‌شده استفاده کردند. در پایان خروجی معماری‌ها با هم ترکیب‌شده و به‌عنوان ورودی به طبقه‌بند ماشین بردار پشتیبان ارسال شد تا تصاویر در دودسته سالم و جعل طبقه‌بندی شوند.

۳. مفاهیم پایه

در این بخش پایگاه‌داده مورداستفاده، معیارهای ارزیابی و شبکه‌های مورداستفاده در این پژوهش آورده شده است.

۳-۱. پایگاه‌داده

پایگاه‌داده بخش جدایی‌ناپذیر و دلیل اصلی پیشرفت یک موضوع پژوهشی است. پایگاه‌داده یک ابزار ارزشمند برای اندازه‌گیری و مقایسهٔ الگوریتم‌های مختلف در یک موضوع است. محققان هنگامی‌که از یک پایگاه‌داده یکسان استفاده می‌کنند به‌راحتی می‌توانند عملکرد نتایج خود را با سایرین مقایسه کنند [۲۰].

تشخیص جعل هم مانند سایر موضوع‌ها، تصاویر و پایگاه‌داده‌های اختصاصی خود را دارد. تعدادی از این پایگاه‌داده‌ها به‌صورت برخط[1] در دسترس هستند و در بسیاری از تحقیق‌های اخیر استفاده‌شده‌اند. برخی از پایگاه‌داده‌ها فقط شامل تصاویر جعل و برخی علاوه بر تصاویر جعل شامل تصاویر اصلی هم هستند. برخی نیز شامل تصاویر باینری یا ماسک حقیقی[2] هستند که مکان جعل هر تصویر را مشخص می‌کنند.

[1] Online
[2] Ground Truth

جدول ۱: پایگاه داده‌های موجود با تصاویر جعلی کپی-انتقال [۲۰و۳۶و۳۷]

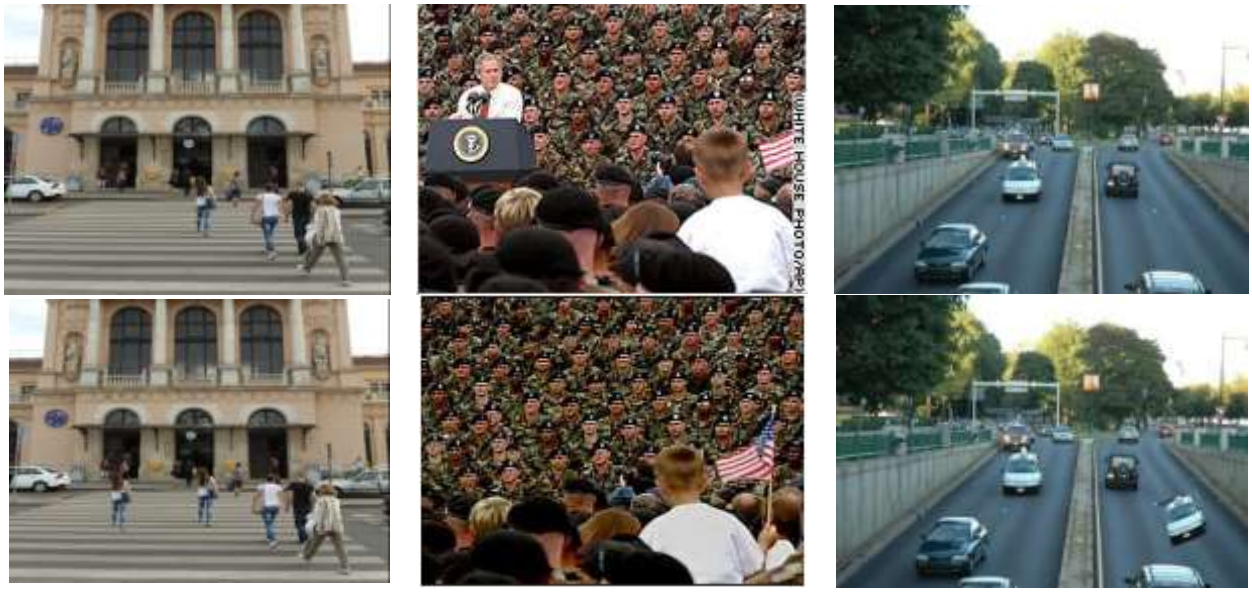
پایگاه‌داده	فرمت/اندازه	تعداد تصاویر سالم و جعل	شکل جعل	تبدیلات هندسی	عملیات پس‌پردازش	ماسک حقیقی
MICC-F220	JPEG ۷۲۲×۴۸۰ ۸۰۰× ۶۰۰	سالم:۱۱۰ جعل:۱۱۰	مستطیلی	مقیاس، چرخش	ندارد	ندارد
MICC-F2000	JPEG ۲۰۴۸×۱۵۳۶	سالم:۱۳۰۰ جعل:۷۰۰	مستطیلی	مقیاس، چرخش	ندارد	ندارد
MICC-F8multi	JPEG ۸۰۰×۵۳۲ ۲۰۴۸×۱۵۳۶	جعل:۸	دلخواه	مقیاس، چرخش	ندارد	ندارد
MICC-F600	JPEG, PNG ۸۰۰×۵۳۲ ۳۸۸۸×۲۵۹۲	سالم: ۴۴۰ جعل:۱۶۰	دلخواه	مقیاس، چرخش	ندارد	دارد
Small CoMoFod	JPEG ۵۱۲×۵۱۲	سالم:۵۰۰۰ جعل:۵۰۰۰	دلخواه	مقیاس، چرخش، انتقال، اعوجاج و ترکیبی	اضافه‌کردن نویز، فشرده‌سازی، کاهش رنگ، تنظیم کنتراست، تار کردن،	دارد
Large CoMoFod	JPEG ۳۰۰۰×۲۰۰۰	سالم:۱۵۰۰ جعل:۱۵۰۰	دلخواه	مقیاس، چرخش، انتقال، اعوجاج و ترکیبی	اضافه‌کردن نویز، فشرده‌سازی، کاهش رنگ، تنظیم کنتراست، تار کردن	دارد
FRITH	JPEG, TIFF, PNG, BMP Variety of dimensions	سالم: ۱۵۵ جعل: ۲۲۴	دلخواه	مقیاس، چرخش، تغییر شکل و اعوجاج	فشرده‌سازی، تار کردن، اضافه‌کردن نویز، کاهش رنگ، افزایش کیفیت عکس	ندارد
COVERAGE	TIFF	سالم: ۱۰۰ جعل:۱۰۰	دلخواه	مقیاس، چرخش، تغییر شکل، اعوجاج، تغییر روشنایی و ترکیبی	ندارد	دارد

نحوهٔ تولید تصاویر جعل در این پایگاه‌داده‌ها به‌گونه‌ای است که یک بخش با اشکال دل‌خواه از خود تصاویر و یا تصاویر دیگر در جاهای مختلف تصاویر چسبانده می‌شوند. در این عملیات همراه با عمل چسباندن، برخی از تغییرهای هندسی[1] از قبیل چرخش[2]، انتقال[3] و مقیاس[4] انجام می‌شود.

در برخی از تصاویر جعلی از عملیات پس‌پردازش[5] مانند فشرده‌سازی، اضافه‌کردن نویز، تار کردن برای مخفی‌کردن ناحیه جعل استفاده می‌شود تا انسان به‌راحتی ناحیه جعل را تشخیص ندهد. برخی از معروف‌ترین پایگاه‌داده‌های جعل کپی - انتقال در جدول ۱ آورده شده است.

در این پژوهش از پایگاه‌داده CoMoFod استفاده‌شده است. پایگاه‌داده CoMoFod در سال ۲۰۱۳ توسط Tralic و همکارانش در دو مجموعه کوچک و بزرگ تهیه‌شده است. مجموعه کوچک دارای ۱۰۰۰۰ تصویر (۵۰۰۰ تصویر سالم و ۵۰۰۰ تصویر جعل) با سایز ۵۱۲ ×۵۱۲ و مجموعه بزرگ آن دارای ۳۰۰۰ تصویر (۱۵۰۰ تصویر سالم و ۱۵۰۰ تصویر جعل) با سایز ۲۰۰۰×۳۰۰۰ است. تصاویر جعلی موجود در این پایگاه‌داده با استفاده از روش کپی-انتقال ایجادشده‌اند [۳۶] . در شکل ۲ چند نمونه از تصاویر موجود در پایگاه‌داده‌های نام‌برده آورده شده است.

[1] Geometric transformation
[2] Rotation
[3] Translation
[4] Scaling
[5] Post processing



CoMoFod FRITH MICC-F220

شکل۲: نمونه‌هایی از تصاویر سالم و جعل از پایگاه‌داده‌های CoMoFod، FRITH و MICC-F220
(سطر اول: تصاویر سالم، سطر دوم: تصاویر جعل)

۳-۲. معیارهای ارزیابی

معیارهای ارزیابی ابزاری برای بررسی عملکرد یک مدل و روش است. معمولاً برای ارزیابی روش‌ها از معیارهای متداول در پژوهش‌های مرتبط استفاده می‌شود. معیارهای ارزیابی در مسئله تشخیص جعل در دو سطح تصویر و پیکسل انجام می‌شود. این معیارها که عبارت‌اند از معیار دقت، صحت، معیار فراخوان، معیار اندازه‌گیری F1 و نرخ مثبت کاذب در جدول ۲ آورده شده است و با استفاده از مولفه‌های ماتریس آشفتگی محاسبه می‌شوند [۵].

جدول ۲: معیارهای ارزیابی

معیار	فرمول
دقت[1]	$\mathrm{ACC} = \frac{TP+TN}{TP+TN+FP+FN}$
صحت[2]	$\mathrm{P} = \frac{TP}{TP+FP}$
فراخوان[3]	$\mathrm{R} = \frac{TP}{TP+FN}$
F1[4]	$\mathrm{F_1} = \frac{2\times R\times P}{R+P}$
نرخ مثبت کاذب[5]	$\mathrm{FPR} = \frac{FP}{FP+TN}$

در ماتریس آشفتگی TP بیان‌کننده تعداد تصاویری است که به‌درستی توسط الگوریتم به‌عنوان جعل شناسایی‌شده است. FN بیان‌کننده تعداد تصاویری است که جعل بوده؛ ولی الگوریتم آن‌ها را تصاویر سالم پیش‌بینی کرده است. FP بیان‌کننده تعداد تصاویر سالمی است که الگوریتم به نادرستی آن‌ها را جز تصاویر جعل گزارش کرده است و TN بیان‌کننده تعداد تصاویر سالمی که توسط الگوریتم سالم تشخیص‌داده‌شده است. لازم به ذکر است در مسائل تشخیص جعل در سطح پیکسل، منظور از مولفه‌های ماتریس آشفتگی پیکسل‌ها هستند.

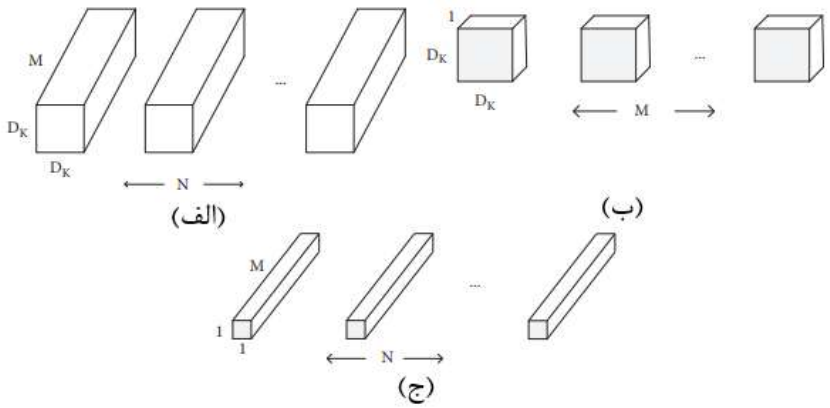
۳-۳. شبکه VGG16

در سال ۲۰۱۴ یک شبکه عصبی عمیق به نام VGG16 معرفی شد [۳۸]. این شبکه از ۱۶ لایه، شامل ۱۳ لایه کانولوشن و ۳ لایه کاملا متصل تشکیل‌شده است. در لایه آخر از یک بیشینه هموار[6] برای طبقه‌بندی کلاس‌ها استفاده‌شده است.

برای آموزش‌دادن شبکه VGG16 نیاز به داده و وقت زیادی است که در عمل انجام این کار دشوار است. برای رفع این مشکل اکثر پژوهش‌ها به دلیل کمبود داده از شبکه VGG16 از پیش آموزش‌داده‌شده استفاده می‌کنند، یعنی شبکه را از قبل با یک پایگاه‌داده بزرگ (Imagenet) که شامل میلیون‌ها تصویر از ۱۰۰۰ کلاس است، آموزش داده‌اند و وزن‌های شبکه تنظیم‌شده‌اند.

در اکثر پژوهش‌ها لایه‌های اولیه شبکه آموزش‌داده‌شده بدون تغییر باقی می‌مانند و لایه‌های انتهایی شبکه متناسب با مسئله طراحی می‌شوند. پارامترهای شبکه جدید با پایگاه‌داده پژوهش موردنظر تنظیم می‌شوند. ازآنجایی‌که شبکه با مجموعه‌داده عظیمی آموزش‌داده‌شده است، بازنمایی خوبی از ویژگی‌های سطح پایین را آموخته است و این ویژگی‌ها را در سراسر شبکه به اشتراک می‌گذارد.

[1] Accuracy
[2] Precision
[3] Recall
[4] F1-measure
[5] False Positive Rate(FPR)
[6] Softmax



شکل ۳: (الف) فیلترهای کانولوشن استاندارد، (ب) کانولوشنال در عمق فیلترها و (ج) فیلترهای کانولوشن نقطه‌ای[۳۹].

در برخی از پژوهش‌ها از شبکه VGG16 از پیش آموزش‌داده‌شده به‌عنوان استخراج‌کننده ویژگی استفاده می‌شود و نقشه ویژگی حاصل از لایه‌های کاملاً متصل به‌عنوان بردار ویژگی[1] برای داده‌ها در نظر گرفته می‌شوند.

۳-۴. شبکه *MobileNet*

شبکهٔ دیگری که توسط گوگل به وجود آمد شبکه MobileNet است که برای سیستم‌های تعبیه‌شده‌ای مانند موبایل بهینه‌سازی شده است. شبکه MobileNet نوعی از شبکه مبتنی بر کانولوشن است، با این تفاوت که در هسته اصلی این شبکه به‌جای لایه کانولوشن استاندارد، از لایه کانولوشن مبتنی بر کانال تفکیک‌پذیر[2] برای ساخت شبکه‌ای سبک‌تر استفاده‌شده است.

این مدل از کانولوشن به‌منظور کاهش بار محاسبات از دولایه با نام‌های کانولوشن عمقی[3] و کانولوشن نقطه‌ای[4] استفاده می‌کند. نحوهٔ کار این نوع کانولوشن به این صورت است که ابتدا، در لایهٔ کانولوشن عمقی از یک عدد کرنل با سایز k×k استفاده‌شده و در همهٔ عمق‌های ورودی عمل کانولوشن انجام می‌شود. نتیجهٔ حاصل برخلاف کانولوشن استاندارد با هم ادغام نمی‌شود، بلکه در ادامه، لایهٔ کانولوشن نقطه‌ای از N کرنل1×1×M (N تعداد نقشه‌های ویژگی لایه خروجی و M تعداد کانال‌های رنگی تصویر ورودی است) برای تولید نقشه‌های ویژگی جدید استفاده می‌کند. این نوع کانولوشن با کاهش قابل‌توجه پارامترها، دقت را در حد مطلوبی باقی نگه داشته است. شکل ۳ این نوع کانولوشن را نشان می‌دهد [۳۹].

۳-۵. شبکه *EfficientNetB0*

هدف معماری‌های یادگیری عمیق طراحی‌شده، استفاده بهینه از توان محاسباتی موجود و افزایش عملکرد شبکه است. در معماری‌های طراحی‌شده در شبکه‌های کانولوشنی، سه روش برای افزایش دقت وجود دارد، این سه روش شامل افزایش عمق شبکه، افزایش عرض شبکه و افزایش رزولوشن تصاویر ورودی است. افزایش هر کدام از آنها باعث بهبود عملکرد شبکه خواهد شد.

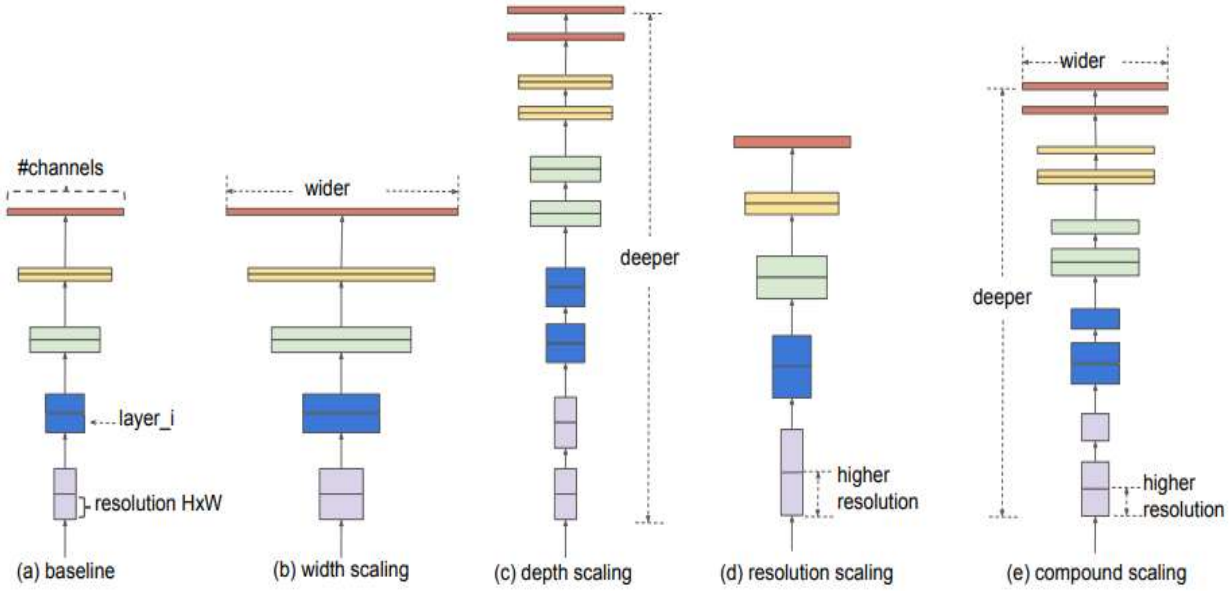
معماری EfficientNet یک روش شبکه عصبی کانولوشنی است که از مفهوم مقیاس‌بندی مدل ترکیب[5] به دنبال یافتن کارآمدترین شبکه باتوجه‌به میزان توان محاسباتی است. ایده معماری EfficientNet بدین صورت است که ابتدا یک مدل پایه[6] در نظر گرفته می‌شود، سپس با افزایش در سه بعد عمق و عرض و رزولوشن در مدل پایه بهبود ایجاد می‌شود. تنظیم‌کردن ابعاد عمق، عرض و رزولوشن فرآیندی مهم، زمان‌بر و نیاز به فضای بزرگی برای جستجو دارد.

معماری EfficientNet از مفهوم مقیاس‌بندی ترکیبی و ضریب ترکیبی ϕ برای مقیاس‌بندی یکنواخت و با رشد ثابت در سه بعد عمق، عرض و رزولوشن استفاده می‌کند. فرمول ۱ نحوه تنظیم ابعاد مختلف با استفاده از مقیاس‌بندی ترکیبی را نشان می‌دهد.

$$\begin{aligned} &depth: d = \alpha^{\phi} \\ &width: w = \beta^{\phi} \\ &resolution: r = \gamma^{\phi} \\ &s.t. \quad \beta^2 . \gamma^2 \sim 2 \\ &\alpha \geq 1, \beta \geq 1, \gamma \geq 1 \end{aligned} \qquad (۱)$$

در این فرمول γ، β و α ضرایب ثابتی هستند که با جستجوی شبکه‌ای کوچک محاسبه می‌شوند. ϕ یک ضریب مشخص‌شده توسط کاربر است که تعداد منابع بیش‌تر را کنترل می‌کند درحالی‌که ضرایب γ، β و α به ترتیب نحوه تخصیص این منابع اضافی را به ابعاد عرض، عمق و رزولوشن شبکه مشخص می‌کند. شکل ۴ عمل‌کرد مقیاس‌بندی مدل در شبکه EfficientNet را نمایش می‌دهد [۴۰].

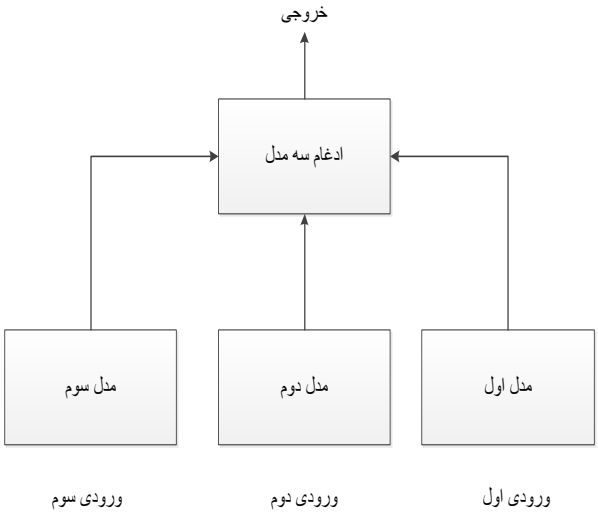
[1] Feature Vectors
[2] Depthwise separable convolution
[3] Depthwise convolution
[4] Pointwise convolution
[5] Compound model scaling
[6] Baseline



شکل ۴: مقیاس‌بندی مدل [۴۰]

۳-۶. مفهوم *API* عملکردی

اکثر معماری‌های یادگیری عمیق مطرح‌شده از مدل ترتیبی[1] پیروی می‌کنند. به این معنی که معماری همانند یک پشته خطی از لایه‌ها که هر لایه یک ورودی و یک خروجی دارد متصور است. اما باتوجه‌به مسائل مختلف، شبکه ممکن است به تعدادی ورودی مستقل نیاز داشته باشد، برخی از شبکه‌ها باید بیش از یک خروجی داشته باشند و یا دارای انشعابات داخلی در بین لایه‌ها باشند، این موارد با مفهوم API عملکردی شناخته می‌شوند [۴۱] . شکل ۵ نمونه‌ای از مفهوم API را نمایش می‌دهد.



شکل۵: نمایی از مفهوم API عملکردی

API عملکردی می‌تواند مدل‌هایی با توپولوژی غیرخطی، لایه‌های مشترک و حتی چندین ورودی یا خروجی را مدیریت کند. در مسائلی که نیاز به تعدادی ورودی مستقل است، روش کار به این صورت است که هر ورودی به‌صورت مجزا به تعدادی لایه داده می‌شود. در نهایت بعد از تعدادی لایه، نقشه‌های ویژگی این مسیرهای مجزا با هم ادغام[2] می‌شوند و تصمیم‌گیری نهایی بر اساس این ادغام و لایهٔ امتیازدهی صورت می‌گیرد. در این پژوهش از این مفهوم استفاده‌شده است که در بخش روش پیشنهادی توضیح تکمیلی داده شده است.

۳-۷. یادگیری انتقالی

استفاده از شبکه‌های از پیش آموزش‌داده‌شده به‌عنوان نقطه شروع و تغییر کاربری آنها برای حل مسائل جدید با مفهوم یادگیری انتقالی شناخته می‌شود. در معماری‌های یادگیری عمیق از جمله شبکه عصبی کانولوشنی، لایه‌های ابتدایی شبکه وظیفه استخراج ویژگی‌های سطح پایین مانند گوشه‌ها و یال‌ها را بر عهده دارند. هر چه لایه‌ها جلوتر می‌روند، معناگرایی در آنها قوت پیدا می‌کند و ویژگی‌های سطح بالا استخراج می‌شوند [۴۱] .

شبکه‌های معروفی مانند VGG16 و Mobilenet با پایگاه‌داده بزرگی به نام Imagenet که دارای میلیون‌ها تصویر از ۱۰۰۰ کلاس است آموزش داده‌شده‌اند. به دلیل قابلیت تعمیم بالای این شبکه‌های آموزش‌دیده بر روی مسائل جدید، برای اکثر مسائلی که دارای پایگاه‌داده محدودی هستند مورداستفاده قرار می‌گیرند. برای این منظور در اغلب مسائل جدید لایه‌های ابتدایی شبکه بدون تغییر باقی می‌مانند، اصطلاحا فریز می‌شوند و لایه‌های پایانی با توجه به مساله موردنظر طراحی‌شده و با پایگاه‌داده مربوطه در فرآیند آموزش شرکت داده می‌شوند.

[1] Sequential

[2] Merge

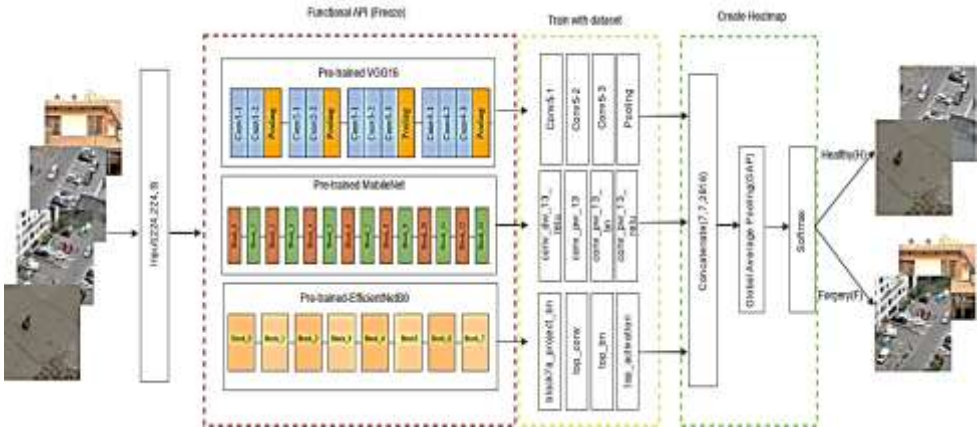
۴. روش پیشنهادی

تشخیص جعل در دو سطح تصویر و پیکسل انجام می‌شود. در تشخیص جعل در سطح تصویر کل تصویر در یکی از دسته‌های سالم یا جعل قرار می‌گیرد، درحالی‌که در تشخیص جعل در سطح پیکسل هر یک از پیکسل‌های تصویر در این دودسته قرار می‌گیرند. در این پژوهش تشخیص جعل در هر دو سطح بررسی‌شده است.

برای این منظور ابتدا تصاویر با استفاده از شبکه‌های از پیش آموزش‌داده‌شده، مفهوم یادگیری انتقالی و API عملکردی در دودسته سالم و جعل طبقه‌بندی می‌شوند. سپس در تصاویر جعل از ترکیب نقشه‌های ویژگی لایهٔ ادغام، تصویر نقشه حرارتی ساخته می‌شود و با استفاده از این مفهوم ناحیه جعل شناسایی می‌شود. در ادامه فرآیند تشخیص جعل در هر دو سطح به‌صورت مفصل‌تر آورده شده است.

۴-۱. تشخیص جعل در سطح تصویر

مراحل تشخیص جعل در سطح تصویر به‌صورت خلاصه در شکل ۶ آورده شده است. همان‌طور که در شکل نشان داده‌شده است در روش پیشنهادی از مفهوم API عملکردی برای ساخت شبکه‌ای با سه ورودی یکسان از تصاویر رنگی و انشعاب‌های متفاوت به‌صورت ترکیب سه شبکه از پیش آموزش داده‌شده‌ی VGG16، MobileNet و EfficientNetB0 استفاده‌شده است.



شکل۶: روند نمای تشخیص جعل در سطح تصویر

تصاویر ورودی هر سه انشعاب دارای اندازه یکسان ۳×۲۲۴×۲۲۴ می‌باشند و به لایه‌های مختلف سه شبکه مذکور داده می‌شوند. از مفهوم یادگیری انتقالی برای استفاده از وزن‌های از پیش آموزش‌داده‌شده هر شبکه استفاده‌شده است، هم‌چنین با استفاده از مفهوم تنظیم دقیق[1] وزن‌ها، تنها چهار لایه‌ی انتهایی هر یک از شبکه‌ها با استفاده از پایگاه‌داده موردنظر در فرآیند آموزش شرکت داده می‌شوند.

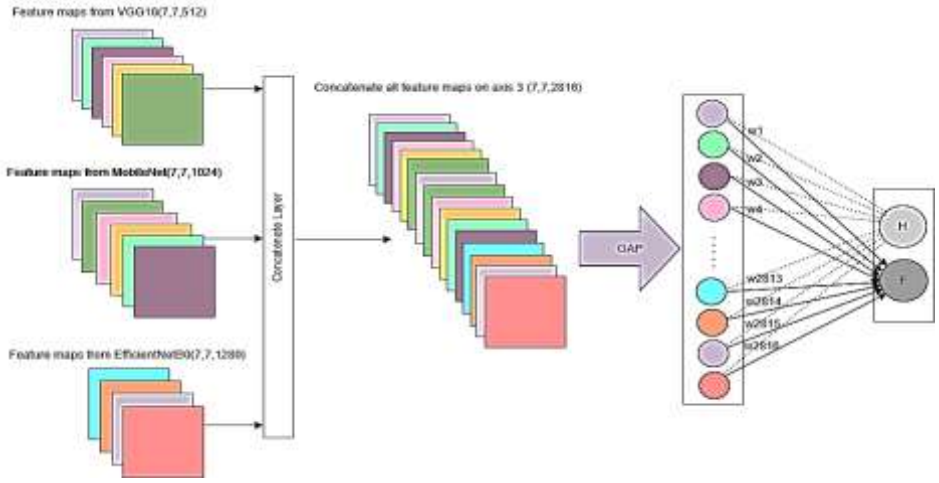
در انتهای شبکه پیشنهادی نقشه‌های ویژگی حاصل از لایه‌های نهایی سه شبکه با استفاده از لایه concatanate با هم ادغام‌شده و یک نقشه ویژگی با اندازه ۲۸۱۶×۷×۷ به دست می‌آید. در ادامه پس از لایه ادغام از لایه پولینگ میانگین جهانی[2] به‌جای لایه کاملا متصل[3] استفاده‌شده است. دلیل انتخاب این است که لایه GAP یک لایه بومی[4] است و وابستگی قوی را بین نقشه‌های ویژگی و هر یک از دسته‌ها ایجاد می‌کند. این لایه بدون پارامتر است و از احتمال بیش‌برازش[5] در فرآیند آموزش جلوگیری می‌کند. این لایه اطلاعات فضایی را خلاصه می‌کند و در برابر انتقالات فضایی مقاوم است [۴۲]. عملکرد لایه GAP در شکل ۷ آورده شده است. ورودی این لایه نقشه‌های ویژگی ترکیب‌شده در لایه ادغام است. لایه GAP با استفاده از عمل میانگین‌گیری بر روی هر یک از نقشه‌های ویژگی ادغام‌شده، هر کدام از آنها را به یک عدد تبدیل می‌کند. بنابراین خروجی لایه GAP در شبکه پیشنهادی، ۲۸۱۶ عدد است که به‌عنوان ورودی در لایه متمایزکننده استفاده می‌شود. در پایان لایه متمایزکننده softmax با دو کلاس در انتهای شبکه پیشنهادی قرار گرفته است و تصاویر را در دودسته سالم و جعل طبقه‌بندی می‌کند. در نهایت شبکه‌ی طراحی‌شده با استفاده از پایگاه‌داده موردنظر و طی ۵۰ بار تکرار آموزش‌داده‌شده است. سایر پارامترهای شبکه‌ی مذکور در جدول ۳ آورده شده است.

جدول ۳: پارامترهای شبکه‌ی ترکیبی پیشنهادی

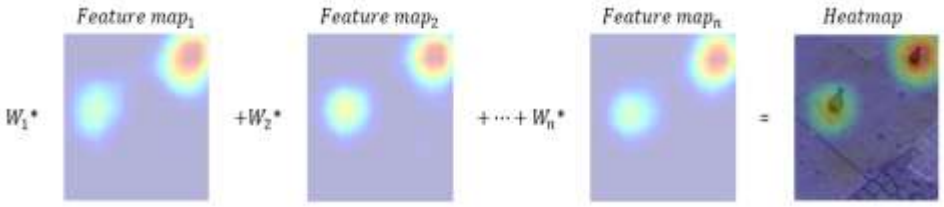
پارامتر	مقدار
تعداد تکرار[6]	۵۰
اندازه دسته[7]	۳۲
نرخ یادگیری[8]	۰,۰۰۰۰۱
بهینه‌ساز[9]	Adam
تابع هزینه[10]	Categorical-cross entropy

[1] Fine tune
[2] Global Average Pooling (GAP)
[3] Fully Connected Layer
[4] Native
[5] Overfitting

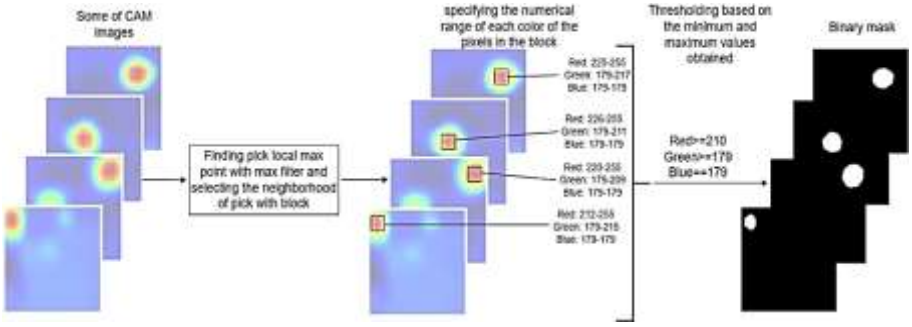
[6] Epoch
[7] Batch size
[8] Learning rate
[9] Optimizer
[10] Loss function



شکل۷: نحوهٔ عملکرد لایه ادغام و لایه GAP در شبکه پیشنهادی



شکل۸: نحوه ساخت نقشه حرارتی و اعمال آن بر روی تصویر جعل



شکل ۹: فرآیند تولید ماسک باینری جهت مشخص کردن محل جعل

۴-۲. تشخیص جعل در سطح پیکسل

همان‌طور که در شکل ۷ نشان داده‌شده است، هر یک از اعداد یا نودهای حاصل از لایه *GAP* با تمام نودهای موجود در لایه *softmax* با استفاده از یک وزن متصل شده‌اند. از این وزن‌ها در تصاویر جعل برای ساخت تصویر نقشه حرارتی[1] استفاده می‌شود.

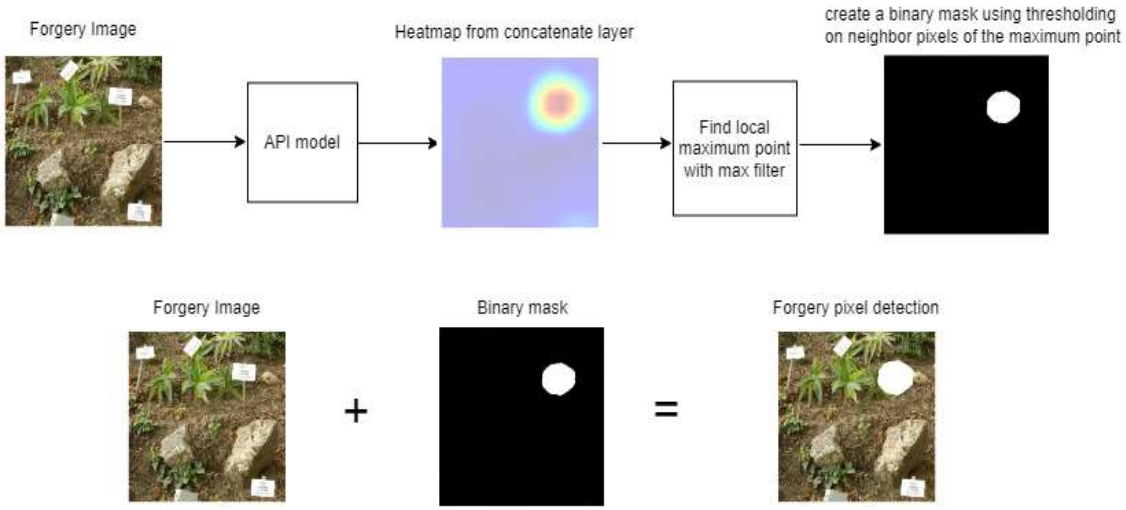
نقشه حرارتی یک ابزار قدرتمند در بینایی ماشین برای حل مسائل کلاسه‌بندی است. در این پژوهش از آن برای تشخیص نواحی جعل استفاده‌شده است. این ابزار برای تجسم و شناسایی این‌که کدام بخش از تصویر برای تصمیم‌گیری کلاس اهمیت دارد، مفید است.

نقشه حرارتی یک تصویر است که از نمره‌دهی هر یک از خروجی‌های کلاس بر روی کل موقعیت‌های تصویر ورودی به وجود آمده است. از حاصل‌ضرب نقشه‌های ویژگی ترکیب‌شده در لایه ادغام با وزن‌های محاسبه‌شده از لایه آخر، نقشه حرارتی ساخته می‌شود. شکل۸ نحوه ساخت این فرآیند را نشان می‌دهد.

باتوجه‌به شکل ۸، ازآنجایی‌که هدف این پژوهش تعیین مناطقی از تصویر که جعل هستند است، برای ساخت نقشه حرارتی در تصاویر جعل از مقادیر وزن‌های بین نودهای حاصل از لایه *GAP* با نود کلاس جعل استفاده می‌شود. اگر نود کلاس سالم در لایه *softmax* را با عدد ۱ و نود کلاس جعل را با عدد ۲ نشان داده شود، عبارت W_{3-2} نشان‌دهنده وزن بین نود سوم از لایه *GAP* و نود کلاس جعل است.

پس از این‌که با استفاده از مدل ترکیبی تصویر جعل تشخیص داده شد و بر اساس خروجی لایه ادغام و وزن‌های لایه آخر نقشه حرارتی ساخته شد، آخرین مرحله مشخص‌کردن نواحی جعل با استفاده از نقشه حرارتی ساخته‌شده است. فرآیند این مرحله در شکل ۹ آورده شده است.

[1] Heatmap



شکل ۱۰: مشخص‌کردن نواحی جعل با استفاده از نقشه حرارتی و آستانه‌گذاری

برای این منظور ابتدا بر روی تعدادی از تصاویر نقشه حرارتی، فیلتر ماکسیمم اعمال شده و حداکثر نقطه ماکسیمم محلی[1] هر تصویر جستجو می‌شود. در ادامه پیکسل‌های همسایه این نقاط مورد بررسی قرار گرفته و محدوده رنج سه کانال رنگی قرمز، سبز و آبی به دست می‌آیند. سپس با استفاده از آستانه‌گذاری بر روی محدودهٔ این سه کانال رنگی نقاط همسایه با هم ادغام می‌شوند. در نتیجه با استفاده از این روش یک ماسک باینری ایجادشده که محل جعل را نشان می‌دهد. در نهایت می‌توان با جمع‌کردن تصویر جعل و ماسک باینری محل جعل را بر روی تصویر مشخص کرد. شکل ۱۰ مراحل ذکرشده را به‌صورت خلاصه نشان می‌دهد.

۵. نتایج ارزیابی

بررسی روش پیشنهادی در دو سطح تصویر و پیکسل در این بخش انجام و مورد بررسی قرار گرفته است. لازم به ذکر است تمامی کدهای روش پیشنهادی با استفاده از زبان برنامه‌نویسی پایتون و با کتابخانه‌های متن‌باز *Tensorflow* و *Keras* نوشته‌شده است. پیاده‌سازی روش پیشنهادی بر روی *GPU* و در محیط *Colab* انجام‌شده است.

۵-۱. ارزیابی نتایج تشخیص جعل در سطح تصویر

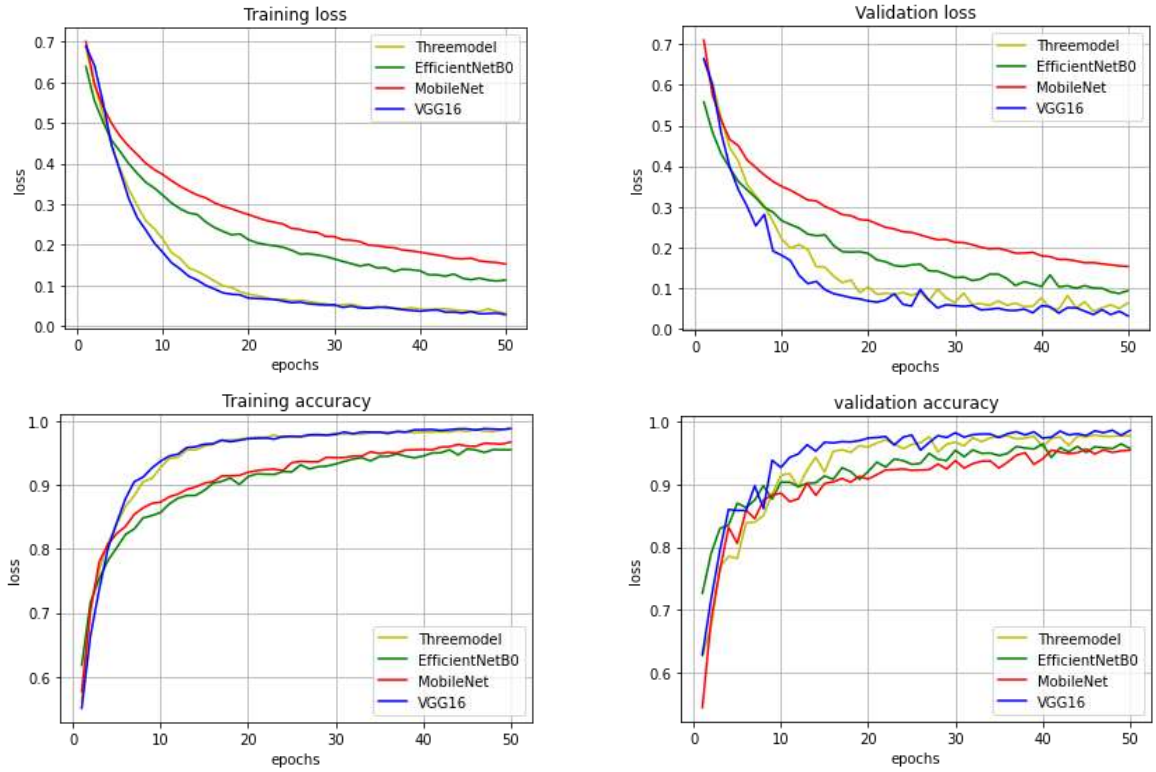
برای ارزیابی تشخیص جعل در سطح تصویر از پایگاه‌داده *Small CoMoFod* که دارای هر دو تصاویر سالم و جعل از نوع کپی- انتقال است، استفاده‌شده است. برخی از تصاویر جعلی موجود در این پایگاه‌داده دارای جعل کپی-انتقال چندگانه[2] هستند . این نوع جعل به دو صورت ایجادشده است: ۱-یک بخش از تصویر کپی و در چند مکان مختلف از همان تصویر چسبانده شده است. ۲- بیش از یک بخش از تصویر کپی و در مکان‌های مختلفی از همان تصویر چسبانده شده است.

نکته مثبت دیگر پایگاه‌داده مذکور داشتن عملیات پس‌پردازش مختلف است. این عملیات که هم بر روی تصاویر سالم و هم تصاویر جعلی اعمال‌شده‌اند عبارت‌اند از: فشرده‌سازی *JPEG*[3] با فاکتورهای کیفیت[4] مختلف (۲۰, ۳۰, ۴۰, ۵۰, ۶۰, ۷۰, ۸۰ و۹۰)، تاری تصویر[5] با $\sigma^2=(0.009,\ 0.005,\ 0.0005)$ و $\square = 0$، اضافه کردن نویز[6] با فیلترهای به اندازه‌های (۳×۳، ۵×۵، ۷×۷)، تغییر روشنایی[7]، کاهش رنگ[8] و تنظیم کنتراست[9].

تصاویر سالم و جعلی موجود در این پایگاه‌داده با نسبت ۷۰٪، ۱۵٪ و ۱۵٪ به‌عنوان داده‌های آموزش، اعتبارسنجی و آزمایش در فرآیند آموزش و ارزیابی مدل مورداستفاده قرار می‌گیرند. فرآیند آموزش شبکه ترکیبی پیشنهادی و شبکه‌های تشکیل‌دهنده آن به‌صورت جدا از هم طی ۵۰ دور تکرار، با بهینه‌ساز *Adam* انجام‌شده است. نمودار تابع هزینه و دقت هر چهار شبکه مذکور برای داده‌های آموزش و اعتبارسنجی در شکل ۱۱ آورده شده است.

[1] Peak Local Max

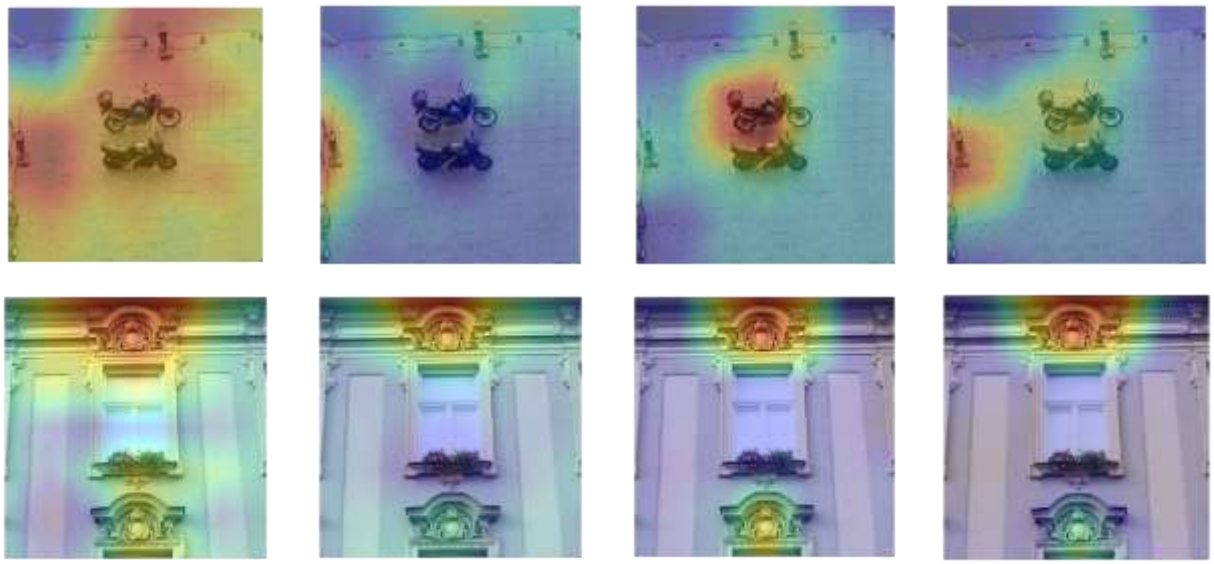
[2] Multiple Copy-Move forgery
[3] JPEG Compression(JC)
[4] Quality factors (QF)
[5] Image Blurring (IB)
[6] Noise Adding (ND)
[7] Brightness Change (BC)
[8] Color Reduction (CR)
[9] Contrast Adjustments (CA)



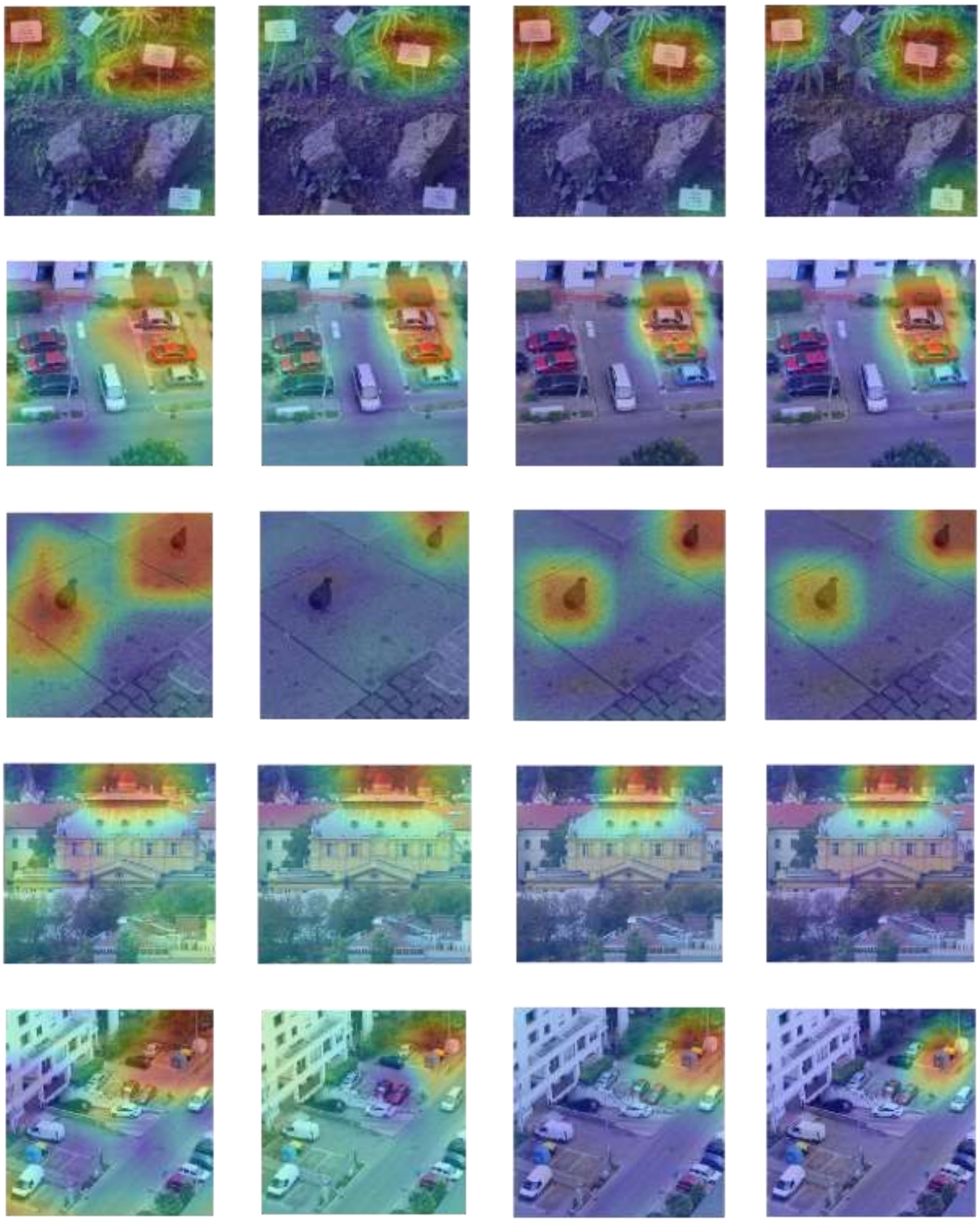
شکل۱۱: نمودار تابع هزینه و دقت چهار شبکه بر روی پایگاه‌داده CoMoFod

۵-۲. ارزیابی نتایج تشخیص جعل در سطح پیکسل

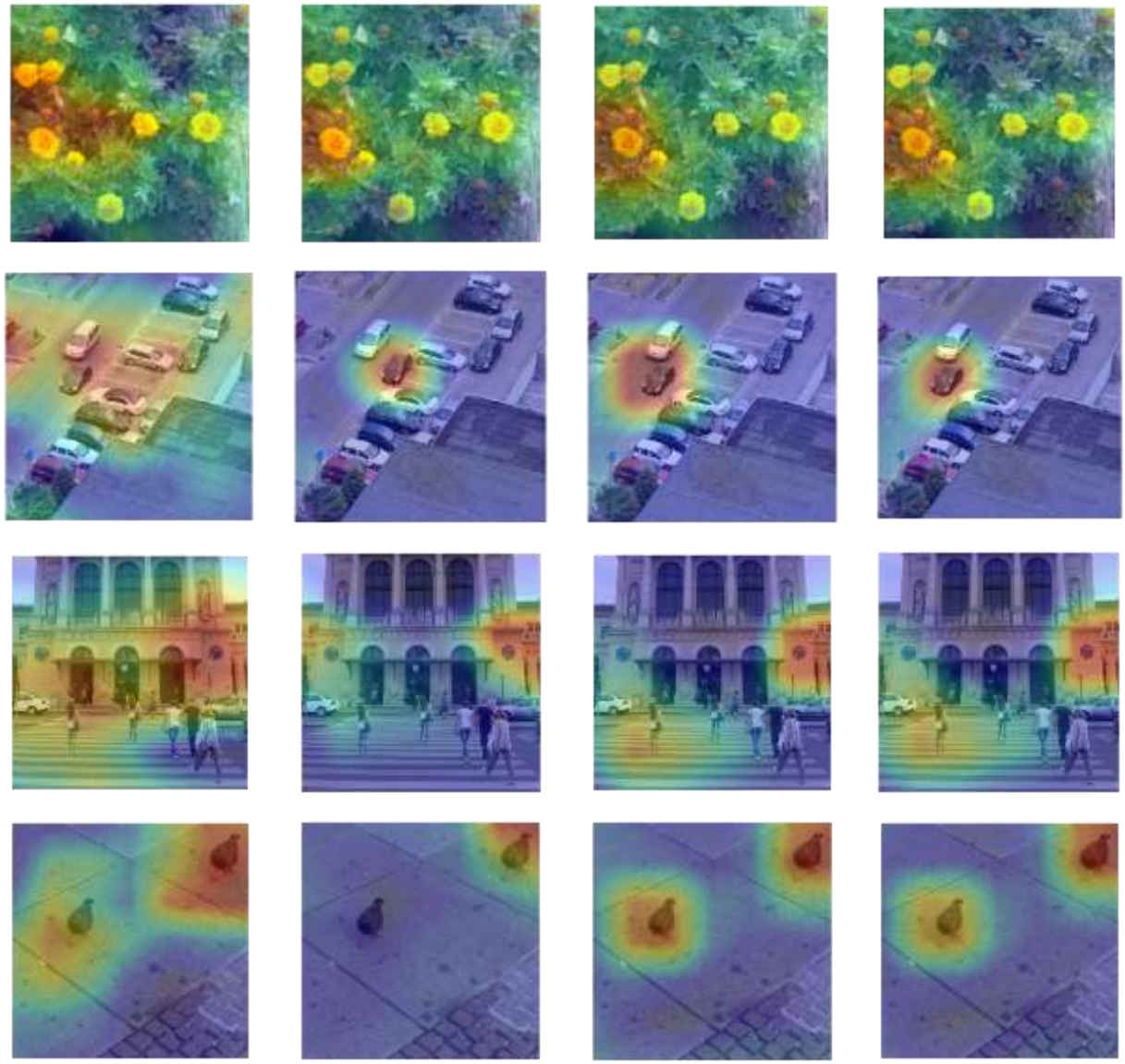
پس از آموزش شبکه‌ها، تصاویر موجود در مجموعه آزمایش در دودسته سالم و جعل طبقه‌بندی می‌شوند. نقشه حرارتی مربوط به تصاویر جعل با استفاده از چهار شبکه مذکور تهیه شدند. برای این منظور در شبکه *VGG16* از نقشه‌های ویژگی به‌دست‌آمده از لایه *block5_pool*، در شبکه *MobileNet* از نقشه‌های ویژگی لایه *conv_pw_13_relu*، در شبکه *EfficientNetB0* از نقشه‌های ویژگی لایه *top_activation* و در شبکه پیشنهادی ترکیبی از نقشه‌های ویژگی لایه ادغام و وزن‌های لایه *GAP* هر شبکه برای ساخت نقشه حرارتی استفاده‌شده است. شکل ۱۲ نقشه حرارتی چند نمونه تصاویر پایگاه‌داده *CoMoFod* با استفاده از چهار شبکه مذکور را نمایش می‌دهد.



شکل۱۲: نقشه حرارتی ساخته‌شده توسط شبکه‌های MobileNet، EfficientNetB0، VGG16 و مدل ترکیبی(از چپ به راست)



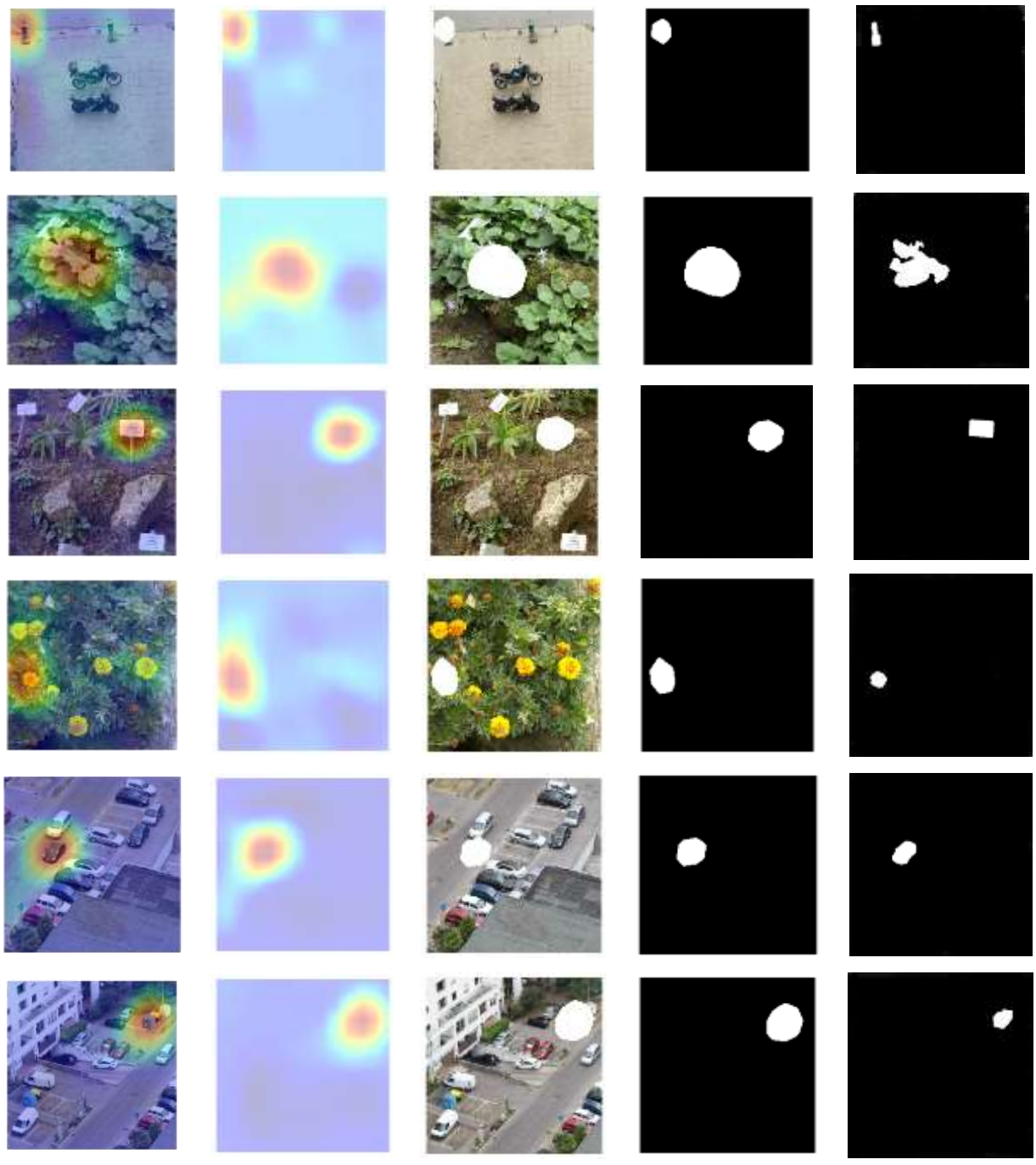
ادامه شکل۱۲: نقشه حرارتی ساخته‌شده توسط شبکه‌های MobileNet، EfficientNetB0، VGG16 و مدل ترکیبی(از چپ به راست)



ادامه شکل ۱۲: نقشه حرارتی ساخته‌شده توسط شبکه‌های MobileNet، EfficientNetB0، VGG16 و مدل ترکیبی(از چپ به راست)

باتوجه‌به نمودارهای شکل ۱۱، این نتیجه برداشت می‌شود که شبکه VGG16 و شبکه ترکیبی در تشخیص تصاویر جعلی عملکرد نزدیک به هم و مشابهی را دارند. درحالی‌که با توجه به نقشه‌های حرارتی ساخته‌شده در شکل ۱۲ برای مرحله تشخیص نواحی جعل این مهم به دست می‌آید که شبکه ترکیبی با استفاده از نقشه‌های ویژگی ادغام‌شده در تشخیص محل صحیح و دقیق‌تر عملکرد بهتری نسبت به شبکه‌های مجزا دارد.

در نهایت برای تشخیص محل جعل با اعمال فیلتر ماکسیمم بر روی نقشه حرارتی حاصل از شبکه ترکیبی نقطه اوج یافته می‌شود. سپس با استفاده از این نقطه و آستانه‌گذاری بر روی آن، نقاط همسایه کشف‌شده و یک ماسک باینری نشان‌دهنده محل جعل ساخته می‌شود. شکل ۱۳ محل جعل یافته شده توسط روش پیشنهادی بر روی برخی از تصاویر پایگاه‌داده CoMoFod را نشان می‌دهد.



شکل ۱۳: تشخیص نواحی جعل توسط روش پیشنهادی (مدل ترکیبی)

۵-۳. مقایسه با کارهای دیگران

مقایسه روش پیشنهادی در تشخیص تصاویر جعل با کارهای دیگران در جدول ۴ آورده شده است. Doegar و همکاران [۳۲] از شبکه AlexNet از پیش‌آموزش داده‌شده به‌عنوان استخراج‌کننده ویژگی برای شناسایی تصاویر جعل استفاده کردند. برای این منظور از هر تصویر یک بردار ویژگی ۴۰۹۶ تایی استخراج‌شده و با ماشین بردار پشتیبان تصاویر در دودسته سالم و جعل طبقه‌بندی شدند. در مقاله [۲۹] شبکه‌هایی با تعداد لایه‌های کانولوشن متفاوت همراه با فیلترها با سایز کرنل و تعداد مختلف از ابتدا طراحی شدند. از هشت پایگاه‌داده مختلف برای آموزش این شبکه‌های طراحی‌شده استفاده‌شده است. در مقاله [۲۶] از شبکه از پیش آموزش‌داده‌شده MobileNetV2 برای شناسایی تصویر جعل از تصاویر سالم استفاده‌شده است.

جدول۴: مقایسه تشخیص تصاویر جعل با دیگران

روش	دقت	تابع هزینه
Pre-trained AlexNet+SVM [32]	۹۴/۴۶	۰/۱۶۸۹
Custom CNN network [29]	۹۲/۶۰	۰/۱۹۵۶
Pre-trained MobileNetv2 [26]	۹۳/۳۸	۰/۱۷۳۷
Pre-trained Mobilenet+GAP layer	۹۵/۴۵	۰/۱۵۲۷
Pre-trained EfficientNetB0+GAP layer	۹۷/۴۰	۰/۰۴۸۶
Pre-trained VGG16+GAP layer	۹۸/۵۰	۰/۰۳۱۰
API model(MobileNet+EfficientNetb0, VGG16)	۹۸/۷۶	۰/۰۲۸۶

مقایسه روش پیشنهادی در تشخیص پیکسل جعل با یک روش مبتنی بر بلوک‌بندی [۴۳] و یک روش مبتنی بر نقاط کلیدی [۴۴] در جدول ۵ آورده شده است. باتوجه‌به نتایج به‌دست‌آمده می‌توان دریافت که روش مبتنی بر بلوک‌بندی در برابر برخی از تغییرهای هندسی مانند چرخش و مقیاس عملکرد ضعیفی دارد. روش مبتنی بر نقاط کلیدی در برابر تغییرهای هندسی و عملیات پس‌پردازش مقاوم است، اما در تشخیص نواحی جعل کوچک و همچنین تشخیص نواحی یکنواخت به‌عنوان نواحی جعل عملکرد ضعیفی دارد.

در مقابل روش پیشنهادی با استفاده از ترکیب سه شبکه یادگیری عمیق از پیش آموزش‌داده‌شده از مزایای این سه شبکه استفاده کرده و در برابر تبدیلات هندسی و عملیات پس‌پردازش مقاوم است. همچنین روش پیشنهادی تنها با استفاده از مفهوم نقشه حرارتی تولیدشده با استفاده از نقشه‌های ویژگی ترکیبی و بدون نیاز به شرکت تصاویر ماسک حقیقی در فرآیند آموزش، ناحیه جعل را شناسایی کرده است.

جدول۵: مقایسه روش تشخیص پیکسل جعل با دیگران

روش	دقت	صحت	نرخ مثبت کاذب
Block-based with DCT [43]	۹۵	۹۹/۲۱	۲۵/۷۹
Key-point based with DWT and Sift [44]	۹۰/۱۱	۷۵/۷۱	۴۸/۴۹
Proposed method(VGG16)	۹۷/۲۳	۹۷/۸۰	۳۴/۶۳
Proposed method(API model)	۹۸/۰۶	۹۸/۵۹	۲۳/۹۸

۶. نتیجه‌گیری

جعل کپی- انتقال از ساده‌ترین و معروف‌ترین روش‌های دست‌کاری تصاویر است. ازآنجایی‌که بخش جعل از لحاظ روشنایی و پویایی رنگ با سایر قسمت‌های تصویر سازگار است تشخیص این نوع جعل دشوار است. در این پژوهش هدف تشخیص جعل هم در سطح تصویر و هم در سطح پیکسل با استفاده از روش یادگیری عمیق است. این مهم در دو مرحله انجام می‌شود، در مرحله اول با استفاده از شبکه‌های از پیش آموزش‌داده‌شده از قبیل *VGG16*، *MobileNet*، *EfficientNetB0*، مفاهیم یادگیری انتقالی و مدل *API* عملکردی سه شبکه مذکور با هم ترکیب‌شده و نقشه‌های ویژگی حاصل از لایه‌های نهایی آنها با هم ادغام می‌شود. در ادامه از لایه پولینگ میانگین جهانی به‌جای لایه کاملاً متصل استفاده می‌شود که وابستگی قوی را بین نقشه‌های ویژگی و کلاس‌ها ایجاد می‌کند. سپس تصاویر با لایه متمایزکننده *softmax* در دودسته سالم و جعل قرار می‌گیرند. در مرحله دوم پس از شناسایی تصاویر جعل، نقشه حرارتی با استفاده از نقشه‌های ویژگی لایه ادغام و وزن‌های لایه *GAP* ساخته می‌شود. ناحیه جعل با استفاده از فیلتر ماکسیمم و آستانه‌گذاری بر روی نقشه حرارتی شناسایی می‌شود. روش پیشنهادی بر روی پایگاه‌داده *CoMoFod* که دارای تصاویر جعل با انواع تبدیلات هندسی و عملیات پس‌پردازش هست مورد ارزیابی قرار گرفته است و عملکرد رضایت‌بخشی به‌دست‌آمده است.

۹. مراجع

[1] N. B. Abd Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R., Salleh, S. Shamshirband, & K. K. R. Choo, "Copy-move forgery detection: survey, challenges and future directions," Journal of Network and Computer Applications, vol. 75, pp. 259-278, 2016, doi: g/10.1016/j.jnca.2016.09.008.

[2] Z. J. Barad, & M. M. Goswami, "Image forgery detection using deep learning: a survey," In 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 571–576, 2020, doi: 10.1109/ICACCS48705.2020.9074408.

[3] A. H. Saber, M. A. Khan, & B. G. Mejbel, "A survey on image forgery detection using different forensic approaches," Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 3, pp. 361–370, 2020, doi: 10.25046/aj050347.

[4] Z. Zhang, C. Wang, & X. Zhou, "A survey on passive image copy-move forgery detection," Journal of Information Processing Systems, vol. 14, no. 1, pp. 6-31, 2018, doi: 10.3745/JIPS.02.0078.

[5] I. A. Zedan, M. M. Soliman, K. M. Elsayed, & H. M. Onsi, "Copy move forgery detection techniques: a comprehensive survey of challenges and future directions," International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, 2021,

[6] B. Shwetha, & S. V. Sathyanarayana, "Digital image forgery detection techniques: a survey," ACCENTS Transactions on Information Security, vol. 2, no. 5, pp. 22–31, 2016, doi: 10.19101/TIS.2017.25003.

[7] D. Chauhan, D. Kasat, S. Jain, & V. Thakare, "Survey on keypoint based copy-move forgery detection methods on image," Procedia Computer Science, vol. 85, pp. 206–212, 2016, doi: 10.1016/j.procs.2016.05.213.

[8] R. Agarwal, D. Khudaniya, A. Gupta, & K. Grover, "Image forgery detection and deep learning techniques: a review," In 4th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1096–1100, IEEE, 2020, doi: 10.1109/ICICCS48265.2020.9121083.

[9] F. Z. Mehrjardi, A. M. Latif, M. S. Zarchi, & R. Sheikhpour, "A survey on deep learning-based image forgery

Processing (ICCSP), IEEE, pp. 41-45, 2020, doi: 10.1109/ICCSP48568.2020.9182066.

[26] J. Ouyang, Y. Liu, & M. Liao, "Copy-move forgery detection based on deep learning," In 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), IEEE, pp. 1–5, 2017, doi: 10.1109/CISP-BMEI.2017.8301940.

[27] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. El Banby, O. A. Elshakankiry, & F. E. Abd El-Samie, "A novel deep learning framework for copy-move forgery detection in images," Multimedia Tools and Applications, vol. 79, no. 27, pp. 19167–19192, 2020, doi: 10.1007/s11042-020-08751-7.

[28] R. Agarwal, & O. P. Verma, "An efficient copy-move forgery detection using deep learning feature extraction and matching algorithm," Multimedia Tools and Applications, vol. 79, no. 11, pp. 7355–7376, 2020, doi: 10.1007/s11042-019-08495-z.

[29] Y. Rodríguez-Ortega, D. M. Ballesteros, & D. Renza, "Copy-move forgery detection (CMFD) using deep learning for image and video forensics," Journal of Imaging, vol. 7, no. 3, 2021, doi: 10.3390/jimaging7030059.

[30] N. Goel, S. Kaur, & R. Bala, "Dual branch convolutional neural network for copy-move forgery detection," IET Image Processing, vol. 15, no. 3, pp. 656–665, 2021, doi: 10.1049/ipr2.12051.

[31] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill, & B. Lee, "Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks," In IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI), pp. 125-130, IEEE, 2021, doi: 10.1109/SAMI50585.2021.9378690.

[32] A. Doegar, M. Dutta, & K. Gaurav, "CNN-based image forgery detection using pre-trained AlexNet model," International Journal of Computational Intelligence and IoT, 2019, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355402.

[33] M. T. H. Majumder, & A. A. Islam, "A tale of a deep learning approach to image forgery detection," In 5th International Conference on Networking, Systems and Security (NSysS), pp. 1–9, IEEE, 2018, doi: 10.1109/NSysS.2018.8631389.

[34] F. M. Al_Azrak, A. Sedik, M. I. Dessowky, G. M. El Banby, A. A. Khalaf, A. S. Elkorany, & F. E. Abd. El-Samie, "An efficient method for image forgery detection based on trigonometric transforms and deep learning," Multimedia Tools and Applications, vol. 79, no. 25, pp. 18221-18243, 2020, doi: 10.1007/s11042-019-08162-3.

[35] A. Doegar, S. Hiriyannaiah, S. G. Matt, S. K. Gopaliyengar, & M. Dutta, "Image forgery detection based on the fusion of lightweight deep learning models," Turkish Journal of Electrical Engineering and Computer Sciences, vol. 29, no. 4, pp. 1978–1993, 2021, doi: 10.3906/elk-2005-37.

[36] D. Tralic, I. Zupancic, S. Grgic, & M. Grgic, "CoMoFoD - new database for copy-move forgery detection," in Proceedings of 55th International Symposium ELMAR, pp. 49–54, IEEE, 2013.

[37] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, & G. Serra, "A sift-based forensic method for copy-move attack detection and transformation recovery," IEEE transactions on information forensics and security, vol. 6, no. 3, pp. 1099–1110, 2011, doi: 10.1109/TIFS.2011.2129512.

[38] S. Tammina, "Transfer learning using VGG-16 with deep convolutional neural network for classifying images," International Journal of Scientific and Research (IJSRP), vol. 9, no. 10, 2019, doi: 10.29322/IJSRP.9.10.2019.p9420.

[39] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, & H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," arXiv preprint arXiv:1704.04861, 2017, doi: 10.48550/arXiv.1704.04861.

[40] M. Tan, & Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," In International conference on machine learning, pp. 6105-6114, 2019, [Online]. Available:https://proceedings.mlr.press/v97/tan19a/tan19a.pdf F. Chollet, "Deep learning with Python," Simon and Schuster, 2021, doi: : 10.31211/interacoes.n42.2022.r1.

detection," Pattern Recognition, vol. 144, pp. 1-31, 2023, doi: 10.1016/j.patcog.2023.109778.

[10] F. Z. Mehrjardi, A. M. Latif, M. S. Zarchi, " Copy-Move Forgery Detection and Localization Using Deep Learning," International Journal of Pattern Recognition and Artificial Intelligence, vol. 37, no. 9, pp. 1-21, 2023, doi: 10.1142/S0218001423520122.

[11] F. Z. Mehrjardi, A. M. Latif, M. S. Zarchi, "An Optimal Hybrid Method to Detect Copy-move Forgery," Journal of AI and Data Mining, vol. 11, no. 3, pp. 429-442, 2023, doi: 10.22044/jadm.2023.13166.2453.

[12] S. Bravo-Solorio, & A. K. Nandi, "Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics," Signal Processing, vol. 91, no. 8, pp. 1759–1770, 2011, doi: 10.1016/j.sigpro.2011.01.022.

[13] B. Diallo, T. Urruty, P. Bourdon, & C. Fernandez-Maloigne, "Robust forgery detection for compressed images using CNN supervision," Forensic Science International: Reports, vol. 2, pp. 100-112, 2020, doi: 10.1016/j.fsir.2020.100112.

[14] R. Thakur, & R. Rohilla, "Recent advances in digital image manipulation detection techniques: A brief review," Forensic Science International, 2020, doi: 10.1016/j.forsciint.2020.110311.

[15] Z. Mohamadian, & A. A. Pouyan, "Detection of duplication forgery in digital images in uniform and non-uniform regions," 15th International Conference on Computer Modelling and Simulation, pp. 455–460, IEEE, 2013, doi: 10.1109/UKSim.2013.94.

[16] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, & X. Sun, "A robust forgery detection algorithm for object removal by exemplar-based image inpainting," Multimedia Tools and Applications, vol. 77, no. 10, pp. 11823–11842, 2018, doi: 10.1007/s11042-017-4829-0.

[17] C. Yang, H. Li, F. Lin, B. Jiang, & H. Zhao, "Constrained R-CNN: a general image manipulation detection model," In IEEE International Conference on Multimedia and Expo (ICME), pp. 1-6, IEEE, 2020, doi: 10.1109/ICME46284.2020.9102825.

[18] T. Mahmood, T. Nawaz, R. Ashraf, M. Shah, Z. Khan, A. Irtaza, & Z. Mehmood, "A survey on block-based copy-move image forgery detection techniques," In International Conference on Emerging Technologies (ICET), pp. 1–6, IEEE, 2015, doi: 10.1109/ICET.2015.7389169.

[19] W. D. Ferreira, C. B. Ferreira, G. da Cruz Júnior, & F. Soares, "A review of digital image forensics," Computers & Electrical Engineering, vol. 85, 2020, doi: 10.1016/j.compeleceng.2020.106685.

[20] O. M. Al-Qureshi, & B. E. Khoo, "Evaluation of copy-move forgery detection: datasets and evaluation metrics," Multimedia Tools and Applications, vol. 77, no. 24, pp. 31807–31833, 2018, doi: 10.1007/s11042-018-6201-4.

[21] S. Sharma, & U. Ghanekar, "A hybrid technique to discriminate natural images, computer generated graphics images, spliced, copy move tampered images and authentic images by using features and ELM classifier," Optik, pp. 470–483, 2018, doi: 10.1016/j.ijleo.2018.07.021.

[22] F. Hoveida, & A. Shahbahrami, "Evaluating the effectiveness of block-based copy-move forgery detection," Promotional scientific journal of soft computing, vol. 7, no. 1, pp. 62-79, 2017. (in Persian), doi: 10.22052/7.1.62.

[23] I. J. Sreelakshmy, & B. C. Kovoor, "Hybrid method for copy-move forgery detection in digital images," In Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering (ISMAC-CVB), pp. 119–127, 2018, doi: 10.1007/978-3-030-00665-5_13.

[24] T. Mahmood, Z. Mehmood, M. Shah, & T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," Journal of Visual Communication and Image Representation, vol. 53, pp. 202–214, 2018, doi: 10.1016/j.jvcir.2018.03.015.

[25] L. Koshy, & S. PraylaShyry, "Copy-move forgery detection and performance analysis of feature detectors," In International Conference on Communication and Signal

[41] M. A. Ghiahban, M. H. Shojaeifard, & A. Amirkhani, "Detection of Slippery Road Conditions using the Road CCTV Images based on the Convolutional Neural Networks and Transfer Learning," Scientific Journal of Electronic and Cyber Defense, vol. 10, no. 2, pp. 103-114, 2022. (in Persian), dor: 20.1001.1.23224347.1401.10.2.9.5.

[42] T. Y. Hsiao, Y. C. Chang, H. H. Chou, & C. T. Chiu, "Filter-based deep-compression with global average pooling for convolutional networks," Journal of Systems Architecture. Vol. 95, pp. 9–18, 2019, doi: 10.1016/j.sysarc.2019.02.008.

[43] T. Mahmood, "Copy move forgery detection technique for forensic analysis in digital images," Mathematical Problems in Engineering. 2016, doi: 10.1155/2016/8713202.

[44] M. F. Hashmi, A. R. Hambarde & A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," In 13th International conference on intelligent systems design and applications, pp. 188–193, IEEE, 2013, doi: 10.1109/ISDA.2013.6920733.