اولین همایش منطقه ای رویکردهای نوین در مهندسی کامپیوتر و فناوری اطلاعات
۵ خرداد ۱۳۹۰ - رودسر
Roudsar 2011

ارزیابی روش های تشخیص تصاویر دیجیتالی جعلی با استفاده از الگوریتم های پردازش تصاویر دیجیتال

احمد پهلوان تفتی[۱]، محمد ملکوتی [۲]، صفورا جانوسپاه [۳] مژده سالکی مزینانی محصل [۴]
[۱]گروه کامپیوتر، واحد امارت، دانشگاه آزاد اسلامی، دوبی، امارات ahmad.pahlavantafti@poug.org
[۲]عضو هیات علمی گروه کامپیوتر ، واحد امارات ، دانشگاه آزاد اسلامی malakooti@iau.ae
[۳] عضو هیات علمی گروه کامپیوتر ،واحد شهر مجلسی، دانشگاه آزاد اسلامی safoura.janosepah@iaumajlesi.ac.ir
[۴]دانشجوی کارشناسی کامپیوتر، دانشگاه علمی کاربردی جهاد کشاورزی، خراسان رضوی (شهید هاشمی نژاد) mo.saleki@gmail.com

چکیده

توسعه‌سیستم های مبتنی بر فناوری اطلاعات و ارتباطات و به کارگیری آن ارتقاء آن‌ها ، تهدید های بسیار جدی را به دنبال داشته باشد تبادل اسناد و اطلاعات به صورت الکترونیکی، بدون توجه به زیر ساخت های امنیتی، یک تهدید در حوزه فناوری اطلاعات و ارتباطات به حساب می‌آید. روش‌های شناسایی تصاویر دیجیتالی جعلی به مجموعه ای از الگوریتم هایی اشاره دارد که صرفنظر از ابزارها و درجه پیچیدگی، تلاش مشترک همه آن دیجیتالی است.تصاویر دیجتالی استفاده روزمره در نشریات، روزنامه‌ها، گردش الکترونیکی پول و اسناد حقوقی و تعهد آور دارد و عدم توجه به آن می

در این مقاله قصد داریم سه روش از روش دیجیتال کار میکنند، مورد ارزیابی و بررسی قرار دهیم کارآیی، قابلیت اطمینان و درجه پیچیدگی زمانی این الگوریتم ها، معیارهایی است که در این مقاله مورد ارزیابی قرار گرفته است‌برای ارزیابی این معیارها، از بانک اطلاعاتی تصاویر دیجیتالی پروانه - های گمرکی در گمرکات استان خراسان رضوی استفاده گردیده است‌تعیین بهترین روش برای شناسایی تصاویر دیجیتالی جعلی، هدف اصلی این مقاله است .

کلمات کلیدی

پردازش تصویر، امنیت، تشخیص جعل تصاویر دیجیتال

۱- مقدمه

تصاویر نقش اساسی در ادراک آدمی دارند و حس‌بینایی یکی از پیچیده ترین حواس پنجگانه است بر خلاف انسان که در درک طیف های الکترومغناطیس دارای محدودیت است ، ماشین های تصویر برداری کلیه این طیف ها را تحت پوشش قرار می دهند و همچنین آن ها می توانند بر رو ی منابع تصویری که انسان قادر به درک آنها نیست عمل نمایند.از جمله این تصاویر می توان به تصاویر میکروسکوپ های الکترونیکی اشاره نمود

در واقع مرزهای مشخصی بین پردازش تصویر در یک سمت و بینایی ماشین در سمت دیگر وجود ندارد اما به هر حال یک الگوی مناسب در این راستا توجه به سه فرآیند محاسباتی در این زمینه است که عبارتند از فرآیندهای سطح پایین، فرآیندهای سطح متوسط و فرآیندهای سطح بالا [۱].

فرآیندهای سطح پایین شامل عملیات های اولیه مانند پردازش تصویر برای کاهش نویز ،ارتقاء وضوح تصویر و تغییر کنتراست می باشد. مشخصه مهم فرآیندهای سطح پایین این است که ورودی و خروجی همه آنها تصویر است . فرآیندهای سطح متوسط شامل عملیاتی نظیر قطعه بندی و توصیف اشیاء در راستای تسهیل پردازش تصویر و طبقه بندی آن ها است و فرآیندهای سطح بالا شامل "ایجاد حس" از شیء تشخیص داده شده(به عنوان مثال شادمانی یا غصه) [۱]. پردازش تصاویر دیجیتالی در طراحی ، ساخت و کارکرد سیستم های مهندسی

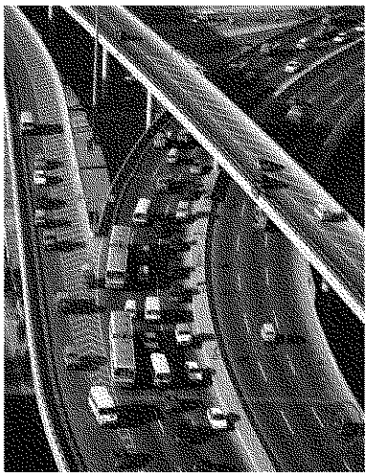
پزشکی، حمل و نقل، ترافیک، تشخیص پزشکی، ارتباطات، هوش مصنوعی و ... کاربردی غیر قابل انکار دارد .

در حال حاضر و بواسطه وجود ابزارهای قدرتمند نرم افزاری در حوزه دستکاری و تغییر تصاویر دیجیتال (مانند Photoshop) ، برخی بدنبال جعل و سوء استفاده از عکس ها و تصاویری می باشند که در حال تهیه و تولید دیجیتالی است. اسناد دولتی و حکومتی، اوراق مالکیت، تصاویر مجلاتی که در حوزه سیاست و اقتصاد فعالیت دارند ، حوزه ای مستعد از جعل تصاویر دیجیتال را شامل می شوند. روش های مختلفی برای شناسایی و تشخیص تصاویر دیجیتالی جعلی وجود دارد. تمام این روش ها به دو دسته تقسیم بندی می شوند: روش های Active و Passive [۶] [۸]. دسته اول روش های Active نامیده می شود که در آن ها تصویر مبداء وجود داشته و با مخفی سازی یکسری داده ها و اطلاعات در تصویر مبداء، از جعل آن جلوگیری به عمل می‌آید [۱۴] [۲]. دسته دوم که Passive نامیده می‌شوند، مبتنی بر حالت‌هایی می‌باشندکه تصویر مبداء وجود ندارد و منحصرا با رویت تصویر و بر اساس الگوریتم های پردازش تصویر می بایست پی به جعلی بودن یا نبودن تصویر برد [۱۲]. ما در این مقاله به بررسی دو روش از روش های Passive پرداخته ایم. این روش ها عبارتند از Double JPEG و Cloning . در این روش ها بدون داشتن تصویر مبداء می توان صحت تصویر را تشخیص داد. قابلیت اطمینان، زمان اجرا و درجه پیچیدگی حافظه ی این روش ها، معیارهای اصلی می‌باشند که می توان بواسطه آن ها کارآیی این روش ها را با هم مقایسه و ارزیابی نمود. قابلیت اطمینان و زمان اجرای این دو روش، معیارهای می‌باشند که در این مقاله مورد ارزیابی قرار گرفته اند.

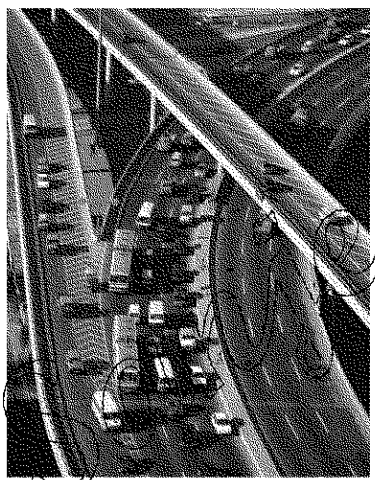
ساختار ادامه این مقاله به این شرح است: در بخش ۲ به معرفی دو روش مذکور پرداخته و نحوه انجام کار و الگوریتم این دو روش را به صورت اجمالی بیان کرده ایم. در ادامه و در بخش ۳ این دو روش را از نقطه نظر قابلیت اطمینان مورد ارزیابی قرار داده ایم. برای ارزیابی از بانک اطلاعاتی تصاویر دیجیتالی پروانه - های گمرکی در اداره کل گمرکات استان خراسان رضوی استفاده گردیده است. نتایج ارزیابی در بخش ۴ ارائه گردیده است و در پایان، نتیجه گیری و پیشنهاد برای کارهای تحقیقاتی آتی انجام شده است.

۲- روش های شناسایی دیجیتالی جعلی

روش های شناسایی تصاویر دیجتالی جعلی که در دسته بندی Passive قرار دارند، نیازی به تصویر مبداء یا همان تصویر اصلی برای شناسایی جعل ندارند. این روش ها بر پایه تشخیص تغییرات غیر نرمال در تصویر یا عدم وابستگی و هم بستگی پیکسل های یک تصویر، بدنبال شناسایی موارد جعل تصویر می- باشند. پیکسل کوچکترین جز ساختاری (element) یک تصویر است. اگر تابع f زیر را با دو متغیر حقیقی مستقل x و y را در نظر بگیریم، آن وقت $f(x,y)$ که در آن $-\infty \le x \le \infty$ و $-\infty \le y \le \infty$ است، می‌توان با نسبت دادن ارزشی (مثل روشنایی و یا شدت) به f آن را بر روی صفحه‌ای نمایش داد. در این صورت f یک تصویر نامیده می‌شود، و نقطه (x,y) یک پیکسل نامیده می‌شود [۱]. یک نمونه از جعل تصاویر دیجتالی در شکل ۱ نمایش داده شده است .



(الف)



(ب)

شکل(۱)-تصویر دیجیتالی اصلی (الف) ، تصویر دیجیتالی جعلی(ب)

۲-۱- روش Double Jpeg

فایل های JPEG (Joint Photographic Experts)، دارای ۲۴ بیت رنگ از نوع True color با روش فشرده سازی

Lossy است. هنگامی که یک تصویر فشرده می شود بسیاری از اطلاعات پاک شده و در نتیجه فایل کوچکتر خواهد شد. در کنار عمل فشرده کردن، ممکن است تصویر خراب شود(یا از کیفیتش کاسته شود). معمولا این فشرده کردن برای ساختن فایل های کوچک که سریع بارگذاری شوند بسیار مفید و کمک کننده است[۱۴] [۵].

الگوریتم های فشرده سازی بهینه معمولاً فراوانی آماری پیکسل های یک تصویر دیجیتالی را به طریقی به کار می گیرند که بتوان اطلاعات تصویر را اجمالی تر و بدون خطا نمایش داد. فشرده سازی بهینه امکان پذیر است چون اغلب اطلاعات و محتویات تصاویر دیجیتالی ، دارای فراوانی آماری هستند [۹]. برای مثال در یک تصویر دیجیتالی مربوط به صورت یک انسان، تمامی پیکسل های مربوط به گونه یا پیشانی و یا لب ها، دارای فراوانی آماری یکسان می‌باشند. فشرده سازی تصویر به روش JPEG طوری عمل می کند که از بخشی از اطلاعات کم ارزش تر "صرف نظر" می کند.

معیار سنجش این روش به این گونه است که تمامی ابزارهای نرم افزاری شناخته شده و پرکاربرد برای دستکاری و تغییر تصاویر دیجیتالی، عمدتا فایل های مورد کار خود را بعد از تغییر و دستکاری تصویر، مجددا با فرمت JPEG ذخیره می سازندکه این مسئله در هدر فایل JPEG با عنوان Double JPEG ذخیره می شود. بدین معنی که پس از انجام تغییرات در یک فایل تصویری دیجیتال، هدر فایل دستخوش تغییر شده و می توان با بررسی آن به دستکاری شدن تصویر دیجیتالی پی برد[۱۰] [۷]. تصاویر دیجیتالی که حاوی این مشخصه در هدر فایلشان می باشند دارای ریسک در حوزه جعل تصاویر خواهند بود .

۲-۲- روش Cloning

در این روش، فرض بر این است که تکه هایی از خود تصویر مبداء در همان تصویر جابه جا یا کپی برداری شده است. به بیان دیگر، تصویر پس از انجام عمل جعل، دارای ناحیه های احتمالا کوچک یکسانی از نقطه نظر رنگ یا مولفه های تصویری خواهد بود. در این روش همبستگی پیکسل ها در کل تصویر دیجیتالی مورد بررسی قرار می گیرد. می توان با توابع استخراج ویژگی تصاویر دیجیتالی همچون DCT که همان تبدیل گسسته کسینوسی است نسبت به انجام این کار اقدام نمود [۳] [۴].

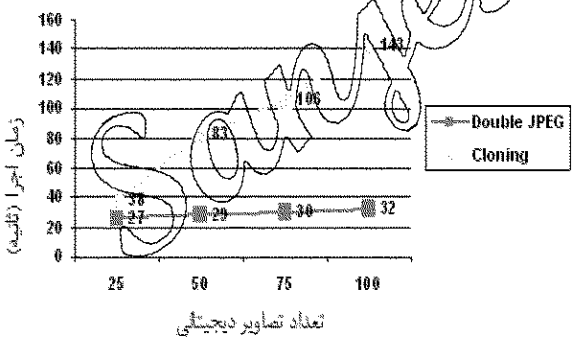
DCT در استخراج ویژگی های تصاویر کاربرد دارد. DCT یک تکنیک مفید ریاضی است که کاربرد آن در زمینه های از قبیل : تشخیص چهره،فشرده سازی تصویر و یک تکنیک رایج برای شناسایی یک نمونه در داده هااست. تبدیل گسسته کسینوسی در صورت کافی بودن داده ورودی می تواند تبدیل بهینه را استخراج کند. آنالیز اجزای اصلی یک روش اختیاری چند متغیری است. DCT با داشتن تصویر ورودی در این حوزه ، می تواند میزان همبستگی پیکسل ها را به عنوان یک مشخصه بارز از تصویر دیجیتالی تولید و ارائه نماید [۱۳] [۱۱].

۳- ارزیابی روش ها

به منظور تست و ارزیابی کارآیی و قابلیت اطمینان این دو روش در درستی و نحوه تشخیص جعل در تصاویر دیجیتالی، یک مجموعه از تصاویر دیجتالی مربوط به پروانه های گمرکی گمرکات خراسان رضوی انتخاب گردید. از این مجموعه آماری، تعداد ۱۰۰ تصویر دیجتالی انتخاب گردید و برخی از آن ها به صورت دستی مورد جعل قرار گرفت. کد و برنامه های نرم افزاری این دو روش ، هر دو در محیط نرم افزاری MATLAB R2009 پیاده سازی و اجرا گردید. اندازه تمامی تصاویر این مجموعه آماری، ۶۰۰ * ۸۰۰ پیکسل بود. ارزیابی قابلیت اطمینان و کارآیی این دو روش در درستی تشخیص جعل صورت پذیرفته در تصاویر در جدول ۱ نشان داده شده است. زمان اجرای این دو روش بر روی مجموعه تصاویر ذکر شده در نمودار شکل ۲ ارائه شده است.

جدول ۱- تعداد تشخیص درست و تشخیص اشتباه در مجموعه آماری حاوی ۱۰۰ تصویر دیجیتالی

روش	تشخیص درست (٪)	تشخیص نادرست (٪)
Double JPEG	۸۱	۱۹
Cloning	۹۳	۷



شکل (۲)-زمان اجرا برای هر دو روش بر اساس ثانیه

۴- نتایج

به منظور بررسی و ارزیابی کارآیی و قابلیت اطمینان و همچنین پیچیدگی زمانی این دو روش، هر کدام از روش ها به صورت مستقل بر روی مجموعه ۱۰۰ تصویر دیجیتالی انتخاب شده به اجرا در آمدند. همانطور که در جدول ۱ مشاهده می کنیم، روش Cloning ،۰قابلیت اطمینان بیشتری در تشخیص جعل صورت گرفته در تصاویر دیجیتالی دارد. روش Double JPEG در مقایسه با روش Cloning از صحت تشخیص کمتر و قابلیت اطمینان پایین تری برخوردار است.

شکل ۲ پیچیدگی زمانی یا همان زمان اجرای این دو روش را نشان می‌دهد. همانطور که مشاهده می‌شود، زمان اجرای روش Cloning بالاتر از روش Double JPEG است. به عبارت دیگر، روش Cloning در مقایسه با روش Double JPEG به مدت زمان بیشتری نیاز دارد. به طور مثال مدت زمان اجرای روش Cloning بر روی ۵۰ عدد تصویر دیجیتالی برابر ۸۳ ثانیه و مدت زمان اجرای روش Double JPEG بر روی همان تصاویر برابر ۲۹ ثانیه است. نمودار شکل ۲ نشان می دهد که زمان اجرای روش Double JPEG نرخ رشد ثابت تری در مقایسه با روش Cloning دارد.

۵- نتیجه گیری و پیشنهادات

در این مقاله دو روش تشخیص جعل تصاویر دیجیتالی مورد بررسی قرار گرفت. همانطور که در جدول و نمودار مشاهده می شود ، روش Cloning مطمئن تر از روش Double JPEG است در حالی که زمان اجرای روش Double JPEG سریع تر از Cloning است. بر این اساس پیشنهاد می شود در آینده روشی ارائه شود که دارای پیچیدگی زمان کمتری نسبت به روش های مذکور باشد و نرخ رشد ثابتی از نظر زمان اجرا داشته باشد.

مراجع

[۱] Al Bovik, (2009). The Essential Guide To Image Processing, Austin, Texas.

[۲] Arnold, M. & Schmucker, M. & Wolthusen, S.D. (2003). Techniques and Applications of Digital Watermarking and Content Protection, *Artech House, Inc.* Norwood, MA, USA.

[۳] Avcibas, I. & Bayram, S. & Memon, N. & Sankur, B (2006). Image manipulation detection. *J. Electron. Imaging.* vol. 15, no. 4, p. 41102.

[۴] Avcibas, I. & Bayram, S. & Memon, N. & Sankur, B. (2005). Image manipulation detection with binary similarity measures. *European Signal Processing Conf.* Turkey.

[۵] Farid, H. & Lyu, S. (2003). Higher-order wavelet statistics and their application to digital forensics. *IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR).* Madison, WI.

[۶] Gallagher, A.C. (2005). Detection of linear and cubic interpolation in jpeg compressed images. *2nd Canadian Conf. Computer and Robot Vision, Victoria, British Columbia.* Canada, vol. 171, pp. 65–72.

[۷] Kirchner, M. (2008). Fast and reliable resampling detection by spectral analysis
of fixed linear predictor residue. *ACM Multimedia and Security Workshop.* pp. 11–20.

[۸] Lukas, J. (2000). Digital image authentication using image filtering techniques. *Proceedings of ALGORITMY 2000, Conference on Scientific Computing.* Podbanske, Slovakia, pp. 236–244.

[۹] Farid, H. & Lyu, S. (2006). Steganalysis using higher-order image statistics. *IEEE*
Trans. Inform. Forensics Security. vol. 1, no. 1, pp. 111–119.

[۱۰] Prasad, S & Ramakrishnan, K. R. (2006). On resampling detection and its application to image tampering. *IEEE Int. Conf. Multimedia and Exposition.* Toronto, Canada, pp. 1325–1328.

[۱۱] Boyle, R. & Hlavac, V. & Sonka, M. (2008). Image Processing, Analysis, and Machine Vision. *Thomson Learning.*

[۱۲] Akansu, A.N. & Ramkumar, M. & Sencar, H.T. (2004). Data Hiding Fundamen- tals and Applications: Content Security in Digital Multimedia. *Academic Press, Inc.* Orlando, FL, USA.

[۱۳] Wu, M. (2001). Multimedia data hiding, Ph.D. Thesis, A dissertation presented to the faculty of Princeton university in candidacy for the degree of doctor of philosophy.

[۱۴] Liu, B. & Wu, M. (2002). Multimedia Data Hiding. *Springer-Verlag.* New York, NJ, USA.

Sanjesh