بررسی امنیت در واترمارکینگ تصاویر دیجیتالی با روش SVM-SS ، با استفاده از الگوریتم ژنتیک

رهام افضل
Roham87.afzal@gmail.com, مهندسی کامپیوتر هوش مصنوعی دانشگاه شهید باهنر
دانشگاه شهید باهنر کرمان
مسئول مکاتبات: رهام افضل

چکیده
از آنجا که ذخیره و ارسال اطلاعات پزشکی به صورت دیجیتال و با فرمت استاندارد می‌باشد امکان دستکاری مغرضانه این اطلاعات وجود دارد. لذا اطلاعات پزشکی تا حد امکان باید از امنیت بالایی برخوردار باشد. یکی از تکنیک‌های جدیدی که از آن می‌توان به عنوان سدی در برابر این خطرات استفاده کرد، نهان‌نگاری یا همان واترمارکینگ است که در آن اطلاعات بیمار به گونه ای در تصاویر قرار داده می‌شود که با دید انسان غیر قابل تشخیص باشد، بدون آنکه فرمت و اندازه ی تصاویر تغییر کند. در اینجا برای نهان‌نگاری اطلاعات از مدل SVM-SS (ماشین بردار پشتیبان و طیف‌گسترده) استفاده شده است. SVM تصویر را به دو ناحیه سودمند و غیرسودمند تقسیم می‌کند و SS برای تعبیه اطلاعات که به صورت باینری در آمده اند، استفاده می‌شود. نهان‌نگاری در حوزه فرکانس و با استفاده از تبدیل گسسته کسینوسی صورت می‌گیرد. اطلاعات در فرکانس‌های بالای تصویر که در ناحیه غیرسودمند واقع شده است تعبیه می-شود. در این تحقیق از تکنیکی جدید برای امنیت بیشتر تصاویر استفاده شده است. به این ترتیب که اطلاعات باینری قبل از تعبیه با اعمال الگوریتم ژنتیک رمزنگاری می‌شود. فرآیند استخراج عکس عمل تعبیه می‌باشد که در آن تصویر اصلی برای بازیابی اطلاعات مورد استفاده قرار می‌گیرد.
کلمات کلیدی: نهان نگاری، ماشین بردار پشتیبان، طیف گسترش، تبدیل کسینوس گسسته

مقدمه

نهان‌نگاری هنر و علم جاسازی اطلاعات در یک رسانه حامل است که با توجه به پیشرفت قابل توجه ارتباطات دیجیتال ، استفاده از آن رو به افزایش است . اگرچه رمزنگاری نیز مفهومی مشابه با نهان‌نگاری دارد ، اما تفاوت‌هایی بین آن‌ها وجود دارد . در رمزنگاری ، هدف صرفا نامفهوم ماندن و عدم توانایی دیگران در دستیابی به محتوای پیام است. اما در نهان‌نگاری باید اصل ارتباط از دید دیگران مخفی بماند . با این توصیف در رمزشکنی حمل هایی موفق است که به محتوای پیام پی ببرد و در نهان شکنی حمل‌هایی موفق است که به وجود ارتباط پی ببرد .

بنابراین ، نهان‌نگاری به نوعی امنیت بیش‌تری نسبت به رمزنگاری دارد . از تمام رسانه‌های دیجیتال، می‌توان جهت نهان‌نگاری استفاده کرد . امروزه یکی از مهم‌ترین رسانه‌های مورد استفاده در اینترنت تصاویر است . به دلیل این که درک انسان از تصاویر محدود است ، امکان تغییرات در تصاویر وجود دارد . این رسانه به عنوان نوعی پوشش مناسب در نهان‌نگاری معرفی می‌شود .

در رمزنگاری برای جلوگیری از دسترسی به محتوای پیام از مخدوش نمودن آن استفاده می‌شود ؛ به طوری‌که این پیام مخدوش و غیر قابل درک شده توسط شخص مجاز و با استفاده از یک کلید سری قابل بازسازی است و اطلاعات به راحتی استخراج می‌شود لیکن همین امر برای شخص غیرمجاز که به اطلاعات رمزشده و الگوریتم رمزنگاری دسترسی دارد بدون داشتن کلید ناممکن است (اندرس ۲۰۰۰) .

برای انجام هر روش پنهان‌سازی دو کار زیر باید صورت پذیرد(متیو ۲۰۰۱):

الف) در آنچه به عنوان میزبان به کار می‌رود باید تحقیق شود که چه تغییراتی را می توان روی آن اعمال نمود بدون این که تفاوت قابل درکی بین نمونه‌ی اصلی و نمونه‌ای که در آن تغییرات ایجاد شده به وجود آید . این تحقیق برای انجام عملیات فشرده‌سازی نیز جهت حذف اجزای زائدی که وجود یا عدم وجود آن‌ها در کیفیت تاثیر چندانی ندارد انجام می‌شود .

ب) از مشخصه تحقیق شده در قسمت (الف) برای پنهان‌کردن اطلاعات استفاده شود .

اگر خواسته باشیم پنهان‌سازی اطلاعات رابه صورت فرمولی عنوان کنیم، می‌توان گفت : برای قطعه‌ی اصلی از داده (d) که به عنوان میزبان مطرح است حد آستانه‌ای وجود دارد (t) که چنان‌چه زیر این حد آستانه ، تغیراتی در d به وجود آوریم قابل تشخیص برای حسگرهای انسانی نیست ؛ این حد

Archive of SID
www.SID.ir

آستانه از راه آزمایش بدست می‌آید ودرافراد مختلف متفاوت است لیکن کم‌ترین مقدار آن از لحاظ حس انسانی برای t در نظر گرفته می‌شود . بنابراین ما همواره می‌توانیم تغییر c در d را زیر حد آستانه t به وجود آوریم طوری که قابل تشخیص به وسیله احساس نباشد($d + c < t$) .

روش‌های نهان‌نگاری در تصاویر به دو دسته کلی تقسیم می‌شود: روش‌های مبتنی بر حوزه مکانی و روش‌های مبتنی بر حوزه تبدیل. تکنیک پنهان-سازی اطلاعات در بیت کم‌ارزش،(لیزا ۱۹۹۹) یکی از روش‌های مبتنی‌بر حوزه مکانی است که سیگنال مخفی را در بیت‌های کم ارزش تصویر اصلی پنهان می‌کند که روش بسیار ساده‌ای می‌باشد. تغییرات در کم ارزش‌ترین بیت در تصویر تأثیری مشابه با اثر نویز در تصویر را دارد و تغییر زیادی را در تصویر ایجاد نمی‌کند. مهم‌ترین اشکال موجود ایـن است که اطلاعات در اثر تکنیک‌های فشرده‌سازی از بین می‌رود. هم‌چنین این نوع مخفی‌سازی به نویز حساس است و با وجود نویز کم اطلاعات از بین می‌رود و به این دلیل ضریب اطمینان کمی دارد.

روش‌های حوزه تبدیل مانند تبدیل فوریه[1](جوراوی ۲۰۰۰)، تبدیل موجک[2](لین ۲۰۰۱)، یا تبدیل کسینوسی گسسته[3](کاکس میلر ۱۹۹۹) از ضرایب حوزه فرکانس برای مخفی‌سازی اطلاعات استفاده می‌شود. در این نوع پنهان‌سازی، انتخاب بهترین فرکانس برای مخفی‌سازی مساله مهمی است. در این روش بعد از اعمال عمل تبدیل، اطلاعات مخفی شده در حوزه مکان در کل تصویر پراکنده می‌شود. در مقایسه با روش‌های حوزه مکان، روش‌های حوزه تبدیل ضریب اطمینان بالاتری در برابر تکنیک‌های فشرده‌سازی دارند. روش‌های نهان‌نگاری بر مبنای نیاز یا عدم‌نیاز به تصویر در گیرنده برای استخراج داده به دو گروه تقسیم می‌شوند. به روش‌هایی که به تصویر اصلی نیاز دارد، روش‌های غیرکور(Non blind) و به روش‌هایی که به تصویر اصلی نیاز ندارند و فرآیند استخراج آن‌ها مستقل از داده‌ی اصلی صورت می‌گیرد، روش‌های نهان‌نگاری کور(Blind)، گویند.

به عنوان مثال، برای پنهان‌سازی در قالب تصویر ابتدا تصویر به بلوک‌های ۸×۸ پیکسل تقسیم شده سپس روی این بلوک‌ها تک‌تک DCT گرفته می‌شود . بیت های پیام با دستکاری ضرایب به دست آمده از این تبدیلات روی این ضرایب پیاده شده و در پایان معکوس DCT گرفته می‌شود یا در تکنیک طیف گسترده[4] با شبیه‌سازی پیام به صورت نویز آن را روی طیف فرکانسی میزبان می‌گسترانند (گسترش باند باریک روی باند وسیع) (لیزا ۱۹۹۹).

واترمارکینگ تکنیکی است که مقدار مشخصی از اطلاعات محرمانه یا اطلاعات وابسته به محتوا را در میزبان یا فایل پوشش داده به صورت شفاف با اطمینان از صحت آن‌ها و حفاظت از اطلاعات ذخیره شده حتی در هنگام انتقال جاسازی (تعبیه) می‌کند . واترمارکینگ در اشکال مختلف مانند ویدئو ، صوت ، متن و مدل3D و کد نرم افزار به کاربرده می‌شود و با موفقیت در برنامه های مختلف مانند احراز هویت ، حفاظت از کپی رایت و تجارت و همچنین رادیو و تلویزیون مورد استفاده قرار می‌گیرد (زاین ۲۰۰۵).

در میان روش‌های محبوب در واترمارکینگ، واترمارکینگ تصویر دیجیتالی است که روشی برای تعبیه و انتقال مقدار مشخصی از داده درون تصویر میزبان است . مزیت اصلی واترمارکینگ تصویر دیجیتال این است که داده‌ها به صورت مستقیم در تصویر تعبیه می‌شوند (زاین ۲۰۰۶).

بنابراین ، اطلاعات می‌تواند در تغییرات مختلف باقی بماند . در مدل واترمارکینگ تصویر دیجیتالی، دو مرحله مورد بحث وجود دارد که تعبیه و استخراج می‌باشد . داده های تعبیه می تواند در قالب متن ، تصویر و... باشد (پلانتیز ۲۰۰۵).

یکی از انواع مهم تصاویر دیجیتالی ، تصویر پزشکی است . تصاویر پزشکی برای ذخیره و ثبت اطلاعات بیماران که بسیار محرمانه است مورد استفاده قرار می‌گیرد . این تصاویر باید از هرگونه تغییر و دستکاری در امان باشند (رائول ۲۰۰۷) .

در طراحی یک واترمارکینگ خوب ۳ شرط اصلی باید در نظر گرفته شود : استحکام ، نامحسوس بودن و ظرفیت . استحکام ، قابلیت واترمارکینگ تصویر برای مقاومت در برابر حملات پردازش مخرب تصویر است . نامحسوس بودن، برای حفظ کیفیت تصویر نوع واترمارکینگ دیجیتالی است . درحالی‌که ظرفیت، تعداد بیت به منظور واترماکینگ مورد استفاده است(۳۰).

در میان تکنیک‌های محاسبات نرم، شبکه های عصبی (NN)، الگوریتم ژنتیک (GA)، منطق فازی (FL) و ماشین بردار پشتیبان (SVM)، SVM در طبقه‌بندی از جمله طبقه بندی تصویر برتری دارد و در واترماکینگ به منظور بهبود عملکرد آن مورد استفاده قرار می‌گیرد (تاسی ۲۰۰۶).

ماشین بردار پشتیبان (SVM) یک طبقه‌بندی کننده دودویی است که دو کلاس را با استفاده از یک مرز خطی از هم جدا می‌کند . نخستین بار SVM توسط وپنیک در اوایل دهه ۱۹۹۰ میلادی مطرح شد(شاوو ۲۰۰۸). SVM در بسیاری از مسائل مربوط به طبقه بندی داده‌ها و شناسایی الگو ، همچون دسته بندی متون ، تشخیص چهره در تصاویر ، تشخیص ارقام دستنویس بیوانفورماتیک کارکرد بسیار موفقی داشته است . از ویژگی‌های مهم SVM طبقه‌بندی داده‌ها بر اساس مینیمم‌سازی خطای تجربی یا همان خطای آموزش است . SVM در بخش آموزش به حل یک مساله بهینه‌سازی محدب می-پردازد و قادر به یافتن جواب مطلق مساله است و برخلاف روش‌هایی چون شبکه های عصبی ، مشکل مینیمم محلی را نخواهد داشت (هانگ ۲۰۰۹). به طور-کلی ، هدف SVM یافتن مرز تصمیمی است که علاوه بر طبقه‌بندی داده‌های دو کلاس با حداقل خطا ، بیش‌ترین حاشیه را نیز دارا باشد (هانگ ۲۰۰۹) .

[1] Fourier transform
[2] wavelet transform
[3] discrete cosine transform
[4] Spread-Spectrum

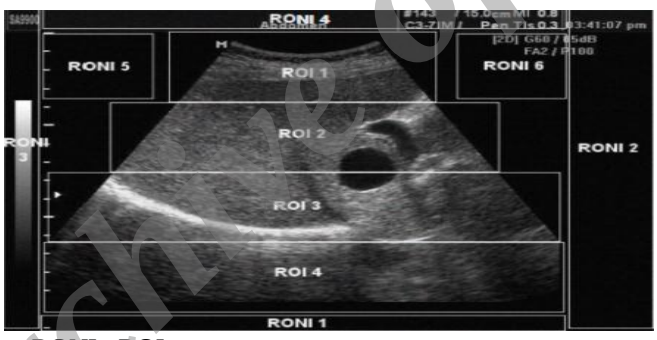
Archive of SID

www.SID.ir

SS یکی از اولین روش‌ها است. اما هنوز قابل توجه بوده و به طور مداوم به کار برده می‌شود (عبدالله ۲۰۰۹) . معمولا SS با فرمت تصویر JPEG به صورت مکرر با همدیگر در حوزه تبدیل مورد استفاده قرار می‌گیرند (عبدالله ۲۰۰۹). شبیه‌سازی SS نسبت به رایج ترین پردازش سیگنال و تحریفات هندسی به منظور حفظ تصاویر میزبان قدرتمند است (تودورو ۲۰۰۴) .

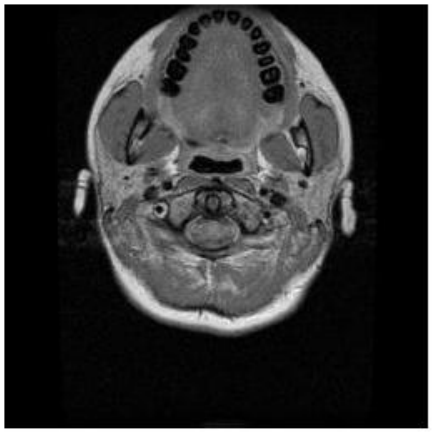
روند تعبیه

به منظور اعمال اطلاعات بیمار در تصاویر انتخابی ابتدا اطلاعات مورد نیاز را از سربرگ تصاویر (مثل سن ، سابقه بیماری ، جنسیت و ...) انتخاب و سپس متنی (*.txt) شامل این اطلاعات ایجاد می‌شود . پس از آن کد اسکی هر کاراکتر موجود درمتن در پایه دودویی بدست می‌آید و با قرار دادن آن‌ها در کنار هم دنباله‌ای از صفر و یک (w) ایجاد می‌گردد .سپس این دنباله داده باینری شده با الگوریتم ژنتیک رمزنگاری می‌شود. به این ترتیب که دنباله باینری اطلاعات بیمار را به دو قسمت والد ۱ و والد ۲ فرض کرده و عملگرهای ترکیب و جهش بر روی آن انجام می‌شود. برای اعمال عمل ترکیب، از ترکیب چند نقطه‌ای استفاده می‌شود. یک کلید(k_2) هم در این مرحله به عنوان کلید رمز درج می شود. سپس برای درج این دنباله داده‌ی رمزنگاری شده به تصویر، از روش طیف‌گسترده (SS) استفاده می‌شود. SS در این مدل برای تعبیه واترمارک با تنظیم یک باند باریک بر روی یک حامل مورد استفاده قرار می‌گیرد. درنتیجه چگالی آن که اغلب زیر سطح نویز است کاهش می‌یابد. بنابراین، تصویر با پهنای باند بالا به نظر می‌رسد که اجازه می‌دهد واترمارک به خوبی در تصویر تعبیه شود، بدون این که قابل تشخیص باشد. این روش از یک تبدیل حوزه‌ی فرکانس برای تبدیل پیکسل‌های ورودی در حوزه‌ی DCT استفاده می کند. پس از بردن تصویر به حوزه‌ی تبدیل گسسته کسینوسی (DCT) در سطح تجزیه دوم، ضرایب موجود در زیرباند انتخابی، در بلوک های ۸×۸ بلوک-بندی می‌شود. به دلیل این که چشم انسان به فرکانس‌های پایین تصویر حساسیت بیشتری دارد، اطلاعات بیماردرفرکانس بالای تصویر تعبیه می‌شود. قبل از فرآیند تعبیه تصویر، با روش ماشین بردار پشتیبان به دو ناحیه سودمند (ROI) وغیرسودمند (RONI) طبقه‌بندی می‌شود. چون نواحی غیرسودمند در هنگام تشخیص بیماری اثری ندارند و اغلب در تصاویر پزشکی سیاه می باشند، دنباله داده رمزنگاری شده به عنوان واترمارک در فرکانس بالای تصویر که در ناحیه ی غیرسودمند قرار دارد تعبیه می‌شود. در شکل زیر می‌توان نوعی از این ناحیه‌بندی را در تصویر سونوگرافی مشاهده کرد.

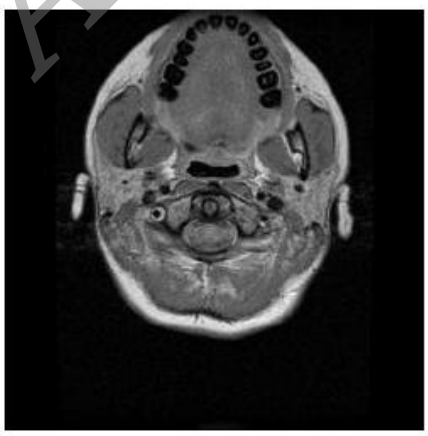


شکل۱- مثالی از تقسیم بندی تصویر پزشکی به دو ناحیه ROI و RONI

سپس معکوس تبدیل کسینوسی گسسته اعمال شده و تصویر واترمارک شده که مشابه تصویراصلی می‌باشد به دست می‌آید. این تصاویر با معیارهای سنجش الگوریتم‌های نهان‌نگاری مورد ارزیابی قرار می‌گیرد.



شکل ۲- (الف) تصویر اصلی



شکل ۲- (ب) تصویر واترمارک شده

Archive of SID
www.SID.ir

روند استخراج داده

فرآیند استخراج معکوس فرآیند تعبیه واترمارک می‌باشد. برای بازخوانی اطلاعات بیمار از تصویر نهان‌نگاری شده، تصویر اصلی هم استفاده می‌شود. تصویراصلی و تصویر نهان‌نگاری شده هر دو به بلوک‌های ۸×۸ پیکسل تقسیم شده و سپس به حوزه‌ی DCT برده می شود. مطابق فرآیند وارد کردن اطلاعات بیمار به تصویر همان سطح تجزیه و زیر باندها انتخاب می‌شود. کلید مخفی k_1 هم اولین بار برای تعیین هویت کاربر وارد خواهد شد. مشابه آن‌چه که در وارد کردن داده انجام شد، بلوک‌ها تشکیل و هر آرایه پیکسل تصویر با هر دو تصاویر مقایسه می‌شود. اگر تفاوتی میان پیکسل‌های تصویراصلی و تصویر واترمارک‌شده وجود داشت، پیکسل تصویر داده واترمارک شده برای به دست آوردن بیت استخراج محاسبه خواهد شد. بعد از استخراج بیت های تعبیه شده، کلید k_2 برای رمزگشایی مورد استفاده قرار می‌گیرد. حال تمام بیت‌ها ترکیب شده و کد اسکی مربوط به هر کاراکتر به دست می‌آید که با تبدیل آن به کاراکتر، اطلاعات بیمار که در تصویر واترمارک شده بود، حاصل می‌گردد.

معیارهای سنجش

برای اطمینان از یکپارچگی و محرمانه ماندن اطلاعات بیماران، یک نمونه اولیه از تصویر پزشکی سیاه و سفید JPEG در اندازه ی ۲۵۶×۲۵۶ توسعه داده شده و آزمایش شده است.در مرحله طبقه بندی، تعدادکل ۲۰ مجموعه داده استفاده شده است. هر مجموعه داده یک تصویر سیاه و سفید با اندازه ۲۵۶×۲۵۶ است. بنابراین، تعداد کل نقاط داده برای تصویر ۶۵۵۳۶ می‌باشد. از این تعداد کل نقاط داده،۲۰۰۰ یا ۳٪ برای آموزش استفاده می‌شود. درحالی‌که ۶۵۳۵۶ بقیه یا ۹۷٪ برای آزمایش مورد استفاده قرار می گیرد. درخشنگی و ارزش لبه تصاویر استخراج شده و جمعیتی از ویژگی‌ها برای فرآیند طبقه‌بندی به وجود می آید. بهترین آستانه با آزمایش مقادیر مشخص انتخاب می‌شود و نتیجه بر اساس سیستم بینایی انسان تعیین می‌شود.تاثیر SVM به انتخاب هسته، پارامترهای هسته و پارامتر حاشیه نرم C بستگی دارد. در این تحقیق از هسته RBF استفاده شده است. دقت طبقه‌بندی SVM بر اساس دو پارامتر ورودی که پارامترهای هزینه (C) و گاما (γ) هستند، سنجیده می شود. بهترین ترکیب C و گاما اغلب توسط یک شبکه جستجو با دنباله رشد تصاعدی از SVM و گاما انتخاب می‌شود. بر اساس انجام شبکه جستجو مقدار پارامترها مشخص شده است، که ۱۰۰۰ برای C و ۱.۰ برای گاما به دست آمده است. در نتیجه ، پیکسل‌های تصویر با موفقیت بـه ROI و RONI طبقه‌بندی شده‌اند نتایج آزمایش نشان می‌دهد که میانگین دقت برای طبقه‌بندی M′ (۳-۱۶) ٪ می باشد. این مقدار حاکی از طبقه بندی خوب SVM به نواحی ROI وRONI است. در مرحله تعبیه SS ، همه‌ی مکان‌های با بالاترین ضریب برای هر بلوک DCT انتخاب می‌شوند، برچسب شناسایی برای این مکان بر اساس نتیجه مرحله طبقه‌بندی شناسایی خواهد شد. تنها مکان‌های با بالاترین ضریب و برچسب‌گذاری شده با ۱- یعنی RONI به عنوان محل تعبیه استفاده خواهد شد. بعد معکوس DCT انجام خواهد شد. پیکسل جمع‌آوری شده به شکل تصویر واترمارک شده استفاده خواهد شد. به منظور بررسی یکپارچگی و محرمانه ماندن اطلاعات بیماران بر اساس روش ارائه شده، استحکام و نامحسوس بودن تصاویر واترمارک شده، اندازه‌گیری شده است استحکام با محاسبه نسبت شباهت (SR) میان تصویر اصلی و واترمارک شده، آزمایش می‌شود. که این محاسبه طبق یک مقایسه میان واترمارک اصلی و استخراج شده انجام می‌شود. معدله آن به شرح زیر است:

$$SR = \frac{S}{S+D} \qquad (۱)$$

در این معادله S نشان دهنده‌ی تعداد مقـادیر پیکسل‌های تطبیـقی و D نشان دهنده‌ی مقـدار پیکسل‌های متفاوت می‌باشد.

محدوده مقادیر SR از ۰ تا ۱ می‌باشد، و مقادیر SR نزدیک به ۱ نشان دهنده‌ی تعدا پیکسل‌های تطبیقی بالا می‌باشد. یعنی واترمارک مستحکم‌تر است و از این رو اصالت آن حفظ می‌شود .

جدول ۱ نتایج SR را که با استفاده از چند اندازه مختلف از واترمارک (ظرفیت) اندازه‌گیری شده را نشان می‌دهد. طبق این جدول می‌بینیم که وقتی اندازه اطلاعات واترمارک افزایش می‌یابد، متناظر با آن ارزش SR کاهش می‌یابد. این منطقی است، درنتیجه دلالت بر این دارد که وقتی اندازه اطلاعات واترمارک بزرگ‌تر می‌شود، استحکام تصویر کاهش می‌یابد.

جدول -۱ نسبت شباهت برای مقادیر آزمایش شده

نسبت شباهت	اندازه نهان نگار
0.9951	40 byte
0.9939	60 byte
0.9927	80 byte
0.9878	100 byte
0.9853	120 byte
0.9910	Average

Archive of SID
www.SID.ir

با استفاده از طبقه‌بندی SVM، تنها ناحیه RONI که در بالاترین ضریب بلوک DCT قرار دارد می‌تواند برای تعبیه واترمارک مورد استفاده قرار بگیرد. اگرچه محدوده آن در اندازه بیت‌های واترمارک تعبیه شده است، نتیجه نهایی آن یک تصویر واترمارک شده قوی‌تر می باشد. در غیر این صورت، اگر طبقه-بندی SVM استفاده نشود، بیت های واترمارک می‌تواند در همه‌ی بالاتر بلوک DCT تعبیه شود. این امر نه تنها اجازه خواهد داد بیت‌های واترمارک بیش از حد بسیاری در تصویر تعبیه شوند، درنتیجه باعث کم شدن استحکام تصویر واترمارک شده خواهد شد که آن بیشتر قابل توجه است. که به این ترتیب، یکپارچگی تصویر پزشکی را به خطر خواهد انداخت.

جدول ۲ -مقایسه استحکام نتایج نسبت شباهت

WORKS	SR
method (79)	**1.0**
method (80)	**0.9181**
method (82)	**0.8496**
method (34)	**0.991**
Proposed Model	**0.991**

جدول ۲ نتایج مقایسه استحکام چند اثر قبلی که اخیرا مورد استفاده قرار گرفته است را با مدل ارائه شده نشان می‌دهد.. همه این مقادیر SR بیش از ۰.۸هستند. درحالی‌که مقدار مدل ارائه شده ۰.۹۹۱ است، که بسیار نزدیک به ۱.۰ می‌باشد. این حاکی از استحکام واترمارک دستکاری نشده است و از این رو صحت اثر حفظ می‌شود.

جدول۳ -نتایج PSNR، انحراف معیار متوسط و استاندارد برای آزمایش نامحسوس بودن

Original Images			Watermarked Images		MSE	PSNR (dB)
Name	Mean	Standard Deviation	Mean	Standard Deviation		
brain_001.jpg	42.184	55.071	41.445	54.865	0.952	48.554
brain_002.jpg	46.507	59.455	45.766	59.238	0.949	48.486
brain_003.jpg	46.450	60.995	45.708	60.783	0.934	48.720
brain_004.jpg	42.997	57.841	42.264	57.628	0.947	48.433
brain_005.jpg	43.750	59.346	43.026	59.132	0.950	48.577
brain_006.jpg	40.071	55.216	39.347	55.005	0.961	48.474
brain_007.jpg	44.562	58.942	43.832	58.720	0.968	48.416
brain_008.jpg	42.624	52.883	41.896	52.653	0.954	48.473
brain_009.jpg	50.271	60.184	49.541	59.947	0.955	48.530
brain_010.jpg	54.938	63.621	54.205	63.375	0.956	48.449
brain_011.jpg	56.557	64.658	55.832	64.406	0.944	48.633
brain_012.jpg	54.420	62.259	53.695	62.013	0.953	48.548
brain_013.jpg	56.041	64.935	55.316	64.688	0.955	48.527
brain_014.jpg	54.702	64.232	53.975	63.992	0.963	48.460
brain_015.jpg	50.259	60.643	49.523	60.412	0.943	48.434
brain_016.jpg	49.093	61.055	48.355	60.834	0.938	48.308
brain_017.jpg	43.286	56.190	42.547	55.975	0.939	48.678
brain_018.jpg	46.005	63.269	45.262	63.076	0.923	48.831
brain_019.jpg	39.181	57.918	38.437	57.737	0.927	48.792
brain_020.jpg	35.708	57.874	34.961	57.713	0.923	48.828
				Average:	0.947	48.558

معیار دوم نامحسوس بودن تصویر واترمارک شده است، که با استفاده از نسبت پیک سیگنال به نویز اندازه‌گیری می‌شود. مقادیر بزرگتر PSNR نشان دهنده-ی شباهت بیشتر بین تصویر اصلی و نهان‌نگاری شده می‌باشد. به منظور سنجش میزان شباهت بین تصویر اصلی و نهان‌نگاری شده با ابعاد(N,N) از معیار PSNR مطابق رابطه‌ی(۲) استفاده می‌شود.

$$PSNR = 10Llog_{10}\left(\frac{255^2}{MSE}\right)(db) \qquad (۲)$$

MSE متوسط مربع خطا بین تصویر اصلی و واترمارک شده است.

$h(N \times N)$: سایز تصویر میزبان

h^*: تصویر نهان نگاری شده

$$MSE = \frac{1}{N \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|h(i,j) - h^*(i,j)|^2 \qquad (۳)$$

برای اندازه‌گیری نامحسوس بودن، ظرفیت اطلاعات واترمارک استفاده شده، ثابت است(۱۲۰ bytes) و همان برای همه‌ی تصاویر تست شده است.جدول ۳ نتایج را نشان می‌دهد.

متوسط مقدار PSNR برای ۲۰ تصویر پزشکی ۴۸.۵۵۸ db می‌باشد، که بیشتر از ارزش قابل قبول نا محسوس بودن PSNR مقدار ۴۰ db است. بنابراین، نتایج نشان می‌دهد که این تصاویر واترمارک شده در بالاترین حد نامحسوس بودن می‌باشد.

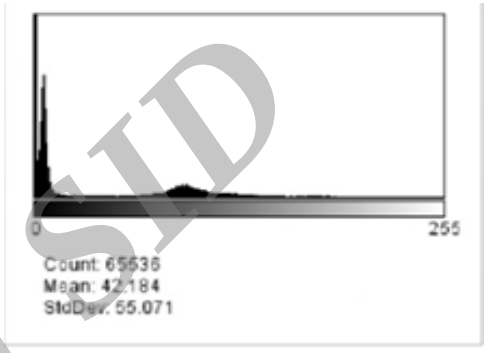
مبنی بر نتایج آثار اخیر، به عنوان نمونه در جدول ۴ ، اگرچه مقدار PSNR به دست آمده از این مدل در بالاترین حد نامحسوس بودن است، آثار دیگری که بهتر انجام شده اند وجود دارد.

Archive of SID
www.SID.ir

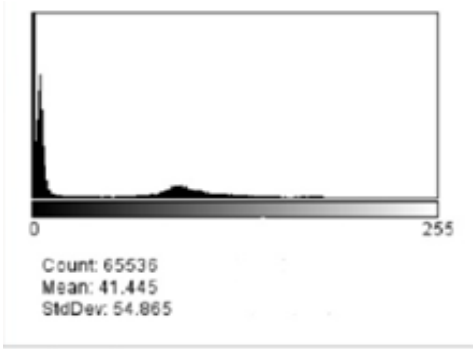
جدول۴ -مقایسه نامحسوس بودن نتایج PSNR

WORKS	PSNR
method (79)	**54.1047**
method (80)	**42.14**
method (82)	**59.1168**
method (34)	**48.558**
Proposed Model	**48.558**

شکل ۴ -نمودار هیستوگرام برای هر دو تصاویر اصلی و واترمارک‌شده را نشان می‌دهد. انحراف استاندارد در شکل۵-۴ (الف) برای تصویر اصلی ۵۵.۰۷۱ و برای تصویر واترمارک شده در شکل ۴ (ب)، ۵۴.۸۶۵ است.



شکل ۴ -(الف) هیستوگرام تصویر اصلی



شکل ۴ -(ب) هیستوگرام تصویر واترمارک شده

نتیجه گیری

با نهان‌نگاری در تصاویر دیجیتال پزشکی می‌توان اهدافی همچون بهبود سطح امنیت، محرمانگی اطلاعات خصوصی بیمار و ذخیره‌ی یک پارچه‌ی فایل تصویری با فایل اطلاعات بیمار را به دست آورد. در این تحقیق با بردن تصویر به حوزه‌ی DCT و به دست آوردن ضرایب فرکانسی آن، برای اضافه کردن اطلاعات بیمار که پیش از این به داده ی باینری تبدیل و با الگوریتم ژنتیک رمزنگاری شده اند، از الگوریتم متقارن SS استفاده شده است به نحوی که این اطلاعات در بالاترین ضرایب فرکانس تصویر که در ناحیه RONI تصویر قرار دارند تعبیه می‌شود. سپس با گرفتن تبدیل معکوس DCT از ضرایب تغییر یافته، تصویر نهان‌نگاری شده با اطلاعات بیمار به دست آمد که این تصاویر با معیارهای سنجش الگوریتم‌های نهان‌نگاری، مورد ارزیابی قرار گرفت که مقدار ۰.۹۹۱ برای SR و ۴۸.۵۵۸ برای PSNR به دست آمد.

برای بازخوانی اطلاعات بیمار از تصویر نهان‌نگاری شده نیز تصویر اصلی و تصویر نهان‌نگاری شده، هر دو به بلوک ۸×۸ تقسیم شده و سپس DCT ارسالی استفاده شد. کلید k_1 هم اولین بار برای تعیین هویت کاربر وارد شد. هر آرایه پیکسل تصویر برای هر دو تصاویر مقایسه شد و با توجه به تفاوت پیکسل‌های موجود در تصاویر مطابق فرآیند وارد کردن اطلاعات بیمار به تصویر، همان ضرایب و الگوریتم بازخوانی، داده‌ی باینری استخراج شد و با تبدیل داده‌ی باینری به کاراکتر، و با اعمال کلید k_2 که برای رمزنگاری اطلاعات باینری شده استفاده شده بود، اطلاعات نهان‌نگاری شده بیمار در تصویر ، به دست آمد. طبق بررسی‌های صورت گرفته نتایج به دست آمده برای نسبت شباهت و حداکثر نسبت سیگنال به نویز با روشی که بر روی آن تحقیقات صورت گرفت و این مدل جدید ارائه شده، یکسان به دست آمد. زیرا تغییری در تعبیه اطلاعات درون تصویر صورت نگرفت. بلکه با استفاده از الگوریتم ژنتیک یک مرحله رمزنگاری در اطلاعات باینری شده بیمار قبل از تعبیه در تصویر صورت پذیرفت که باعث بالاتر رفتن مقاومت روش در برابر حملات احتمالی می‌شود بدون این که تغییری در تصویر ایجاد کند. بنابراین حتی اگر کسی به الگوریتم و کلید k_1 دسترسی پیدا کند با یک مرحله دیگر که رمزگشایی این اطلاعات است، مواجه می‌شود. به این ترتیب استفاده از الگوریتم ژنتیک که به عنوان یک روش جدید ارائه شده بود، مقاومت تصاویر پزشکی در برابر حملات را بالا برده است. که برای بررسی آن باید آزمایش‌هایی جداگانه بر روی تصاویر دستکاری شده برای این مدل و روش‌های قبلی صورت گرفته، انجام شود تا با مقایسه نتایج آن‌ها این مطلب اثبات شود.این مقادیر به دست آمده نشان می دهد که انحراف معیار استاندارد پس از تعبیه واترمارک در تصویر، کاهش یافته است. دلیل آن این است که پس از تعبیه واترمارک، مقادیر پیکسل های انتخاب شده افزایش یافته است.

منابع مورد استفاده:

(۱) فرهاد رحیمی، دکتر حسین ربانی، دکتر سعید کرمانی،۱۳۹۰، "نهان‌نگاری دوگانه‌ی اطلاعات محرمانه بیمار در تصاویر پزشکی با استفاده از تبدیل کانتورلت"، مجله دانشکده پزشکی اصفهان- سال۲۹/ شماره۱۷۴/ ویژه نامه (مهندسی پزشکی)

Archive of SID

www.SID.ir

(۲) نادیا رود سرابی، علیرضا بهراد،۲۴-۲۵ بهمن۱۳۸۶-دانشگاه شاهد، "روش جدیدی برای نهان‌نگاری در تصاویر پزشکی با استفاده از شبکه عصبی"، چهاردهمین کنفرانس مهندسی پزشکی ایران

(۳) مینا باقری، حبیب اله دانیالی، محمد صادق هل فروش، ۲۳ و ۲۴ شهریور۱۳۹۰ – دانشگاه فردوسی مشهد، "نهان‌نگاری تهی و نیمه شکننده تصاویر دیجیتال با استفاده از استخراج ویژگی در حوزه ویولت و SVM"، هشتمین کنفرانس بین المللی انجمن رمز ایران

(۴) فاطمه ادریسی، لیلی احسان، احسان اله اکبر، سعید نادر اصفهانی، "بررسی اثر روش انتخاب بلوک و طول رشته گلد در نهان‌نگاری تصویر به روش طیف گسترده"،

(۵) پیمان نفیسی فرد ، ولی درهمی، علی محمد لطیف ،زمستان۹۰،"واترمارکینگ وفقی تصاویر دیجیتال مبتنی بر یادگیری ماشینی"،

(۶) رضا شاه حسینی، سعید همایونی، محمدرضا سراجیان،"طبقه‌بندی تصاویر سنجش از راه دور فراطیفی به کمک ماشین‌های بردار پشتیبان"، گروه مهندسی نقشه برداری، دانشکده فنی، دانشگاه تهران

(۷) رضایی ع، رنجبران س، "آموزش کاربردی الگوریتم‌ژنتیک در نرم‌افزار MATLAB"، انتشارات آذر، تهران،۱۳۸۶.

(۸) جمشیدی، نیما و ابویی مهریزی ، علی و مولایی، رسول، آموزش کاربردی مباحث پیشرفته مهندسی برق با MATLAB تهران،نشر عابد،۱۳۸۸ .

(9) Kumar, S., Raman, B., Thakur, M: Real Coded Genetic Algorithm Based Stereo image Watermarking. IJSDIA 1(1), 23–33,(2009).

(10) Jung, H., Jeon, M: Enhanced SVD Based Watermarking with Genetic Algorithm, vol. 56, pp. 586–593. Springer, Heidelber ,(2009).

(11) Charles L. Karr and L . M . Freeman “ Industrial Applications of genetic Algorithms ”
CRC Press (1999).

(12) L. Der-Chyuan, L. Jiang-Lung and H. Ming- Chiang, "Adaptive digital watermarking using neural network technique", IEEE International Carnahan Conference on, Security Technology, pp. 325-332, (2003).

(13) J. Cong and W. Shihui, "Applications of a Neural Network to Estimate Watermark Embedding Strength", Eighth International Workshop on, Image Analysis for Multimedia Interactive Services, pp. 68-68,(2007).

(14) N. Zhong, J.-M. Kuang and Z.-W. He, "A GA-based Optimal Image Watermarking Technique", Third International Conference on, Intelligent Information Hiding and Multimedia Signal Processing, vol. 1, pp. 291-294, (2007).

(15) Peng, H., Wang, J., Wang, W.: Image watermarking method in multiwavelet domain based on support vector machines. Journal of Systems and Software (2010) (in press)

(16) Wang, X.-Y., Xu, Z.-H., Yang, H.-Y.: A robust image watermarking algorithm using SVR detection. Expert Systems with Applications 36(5) (2009).

(17) Andreas Westfeld , Andreas Pfitzman , “ Attacks On Steganigraphic Systems “ , Department of computer science , IH’99 , LNCS 1768 , pp. 61-76 , (2000).

(18) Matteo Fortini , “Steganography and Watermarking : A Global View”

(19) Ross J.Anderson , Fabien A.Petitcolas , “ On the Limits of Steganography “ ,

(20) I.Djurovi, S.Stankovi and I.Pitas, "Digital watermarking in the fractional Fourier transformation domain", Journal of Network and Compute Applications, 24, P.P. 167-173, (2001).

(21) S.-F. Lin, and C.-F. Chen, “A robust DCT-based watermarking for copyright protection,” IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp. 415-421, Aug(2000).

(22) I.J.Cox,M.L.Miller,and J.A. Bloom, Digital Watermarking, Morgan Kaufmann,(1999).

(23) Lisa M.Marvel , Charles G.Boncelet , Chrles T.Retter, “ Spread Spectrum Image Steganography “ , IEEE Transaction on image processing , vol 8 , No 8 , (1999).

(24) Zain, J.M., Clarke, M.: Security in Telemedicine: Issues in watermarking medical images. In: 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA (2005).

(25) Potdar, V.M., Han, S., Chang, E.: A Survey of Digital Image Watermarking Techniques. In: International Conference on Industrial Informatics INDIN (2005).

(26) Zain, J.M., Clarke, M.: Reversible Watermarking Surviving JPEG Compression. In: EMBS 2005, pp. 3759–3762 (2006).

Archive of SID

www.SID.ir

(27) Planitz, B.M., Maeder, A.J.: A Study of Block-Based Medical Image Watermarking Using a Perceptual Similarity Metric. In: Proceedings in DICTA 2005, p. 70 (2005).
(28) Raul, R.-C., Feregrino, -U.C., de Gershom, J.T.-B.: Data Hiding Scheme for Medical Images. In: Proceedings in: 17th International Conference on Electronics, Communications and Computers (CONIELECOMP 2007), IEEE Computer Society, USA (2007).
(29) Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: Multiple Image Watermarking Applied to Health Information Management. IEEE Transactions on Information Technology in Biomedicine 10(4), 722–732 ,(2006).
(30) Huang, S., Zhang, W.: Digital Watermarking Based on Neural Network and Image Features. In: ICIC 2009, vol. 2, pp. 238–240 (2009).
(31) Cao, X.B., Xu, Y.W., Chen, D., Qiao, H.: Associated evolution of a support vector machine-based classifier for pedestrian detection. Information Sciences 179(8), 1070– 1077 (2009).
(32) Tsai, H.-H., Sun, D.-W.: Color image watermark extraction based on support vector machines. Information Sciences 177(2), 550–569 (2007).
(33) Shao, Y., Chen, W., Liu, C.: Multiwavelet-based Digital Watermarking with Support Vector Machine Technique. In: CCDC 2008 ,(2008).
(34) Saliza Ramly1, Syed Ahmad Aljunid1, and Hanizan Shaker Hussain2 E. Ariwa and E. El-Qawasmeh (Eds.): DEIS 2011, CCIS 194, pp. 372–386, 2011. Springer-Verlag Berlin Heidelberg (2011).
(35) Tsai, H.-H., Sun, D.-W.: Color image watermark extraction based on support vector machines. Information Sciences 177(2), 550–569(2007).
(36) Abdallah, H.A., Hadhoud, M.M., Shaalan, A.A.: A blind spread spectrum wavelet based image watermarking algorithm. In: ICCES 2009, pp. 251–256 (2009).

Archive of SID

www.SID.ir