فصلنامه پژوهش های نوین درعمران، معماری و شهرسازی شماره۳ – دوره ۱- صفحات ۱۳۷-۱۵۱
Journal of New researches in Civil Engineering, Architecture and Urban Planning
ISSN: 3060-608X

شناسایی روش تعیین اصالت کدهای QR مبتنی بر تکنیک های یادگیری ماشین

مونس قفلی [*1]، مرتضی مهرافشاری [2]

۱ -کارشناس ارشد رشته عمران گرایش سازه، موسسه آموزش عالی لیان بوشهر. (کارشناس املاک شهرداری).

۲ -کارشناس ارشد رشته حسابداری، موسسه آموزش عالی خرد بوشهر.

چکیده

هدف این پژوهش شناسایی روش تعیین اصالت کدهای QR مبتنی بر تکنیک های یادگیری ماشین می باشد. در روند اجرای تحقیق، ابتدا به مطالعات کتابخانه ای در زمینه موضوع پرداخته و سپس به بررسی تحقیقات صورت گرفته و روش‌های ارائه شده پیشین خواهیم پرداخت و نقاط قوت و ضعف هر روش را مورد مطالعه قرار خواهیم داد. پس از انجام مطالعات اولیه، به طراحی روش پیشنهادی خواهیم پرداخت. در این مقاله الگوریتم بکار رفته به طور دقیق کدهای QR را با انواع مختلف نویز حذف کرد. ظرفیت ذخیره سازی کدهای QR برای سیستمی از n شبکه) ۴۰۰ (n × که در آن nتعداد شبکه هایی است که به صورت موازی استفاده می شوند. همچنین، بسیار سریعتر از یک شبکه هاپفیلد منفرد با ظرفیت یکسان است، به طوری که اگر شبکه ما دارای ۳۲۴۹ گره و ظرفیت ۴۰۰ n × باشد، یک شبکه هاپفیلد منفرد دارای ۳۲۴۹ n × گره خواهد بود که ظرفیت یک شبکه هاپفیلد به صورت خطی مقیاس می شود. این بدان معناست که الگوریتم ما در این مقاله به دستاوردهای بزرگی در سرعت و نیازهای ذخیره‌سازی نسبت به شبکه‌های معمولی منجر می‌شود و آنها را برای اهداف متنوع‌تری امکان‌پذیر می‌کند. همانطور که در نتایج مشاهده می شود، می توان مقادیر زیادی نویز را با روش حذف نویز ما حذف نمود. الگوریتم ما برای توزیع کدهای QR در چندین شبکه هاپفیلد و انتخاب صحیح، به افزایش ظرفیت ذخیره سازی کدهای QR توسط شبکه ها کمک می کند و بنابراین استفاده از آن در سیستم های بزرگ برای تشخیص کد QR امکان پذیر است.

کلمات کلیدی: اصالت کدهای QR، تکنیک های یادگیری، یادگیری تحت نظارت

فصلنامه پژوهش های نوین درعمران، معماری و شهرسازی شماره۳ – دوره ۱- صفحات ۱۳۷-۱۵۱
Journal of New researches in Civil Engineering, Architecture and Urban Planning
ISSN: 3060-608X

OPEN ACCESS

مقدمه

در دنیای جدید که بشر قادر به انجام هر کاری (همانند بانکداری، خرید، ارتباط و اشتراک گذاری اطلاعات) به صورت آنلاین است، مسأله‌ی دسترسی به چنین خدماتی به صورت کاملاً امن به مهمترین مسأله‌ی روز بدل گشته است. به عبارتی دیگر، با پیچیده شدن و افزایش قدرت ویروس‌ها و بدافزارها، روش‌های امنیتی نیز نیازمند پیشرفت و بهبود عملکردی بوده، تا به کاربران، اجازه‌ی انتقال داده با بیشترین سطح اطمینان را دهد.

خدمات الکترونیکی، کم‌هزینه‌ترین و موثرترین روش برای ارایه‌ی خدمت به مشتریان است. به عنوان مثال، در پرداخت الکترونیکی دیگر نیازی به نوشتن چک یا حمل پول نبوده و تمام چیزی که یک کاربر بدان نیاز دارد، ورود اطلاعات موردنیاز در جست و جو گر وب و فشردن کلید ماوس است. به طور حتم در سال‌های آینده شاهد استفاده‌ی تمامی افراد جامعه از خدمات اینترنتی خواهیم بود. پرداخت الکترونیکی نوعی از پرداخت غیر نقدی به حساب می‌آید که در آن خبری از پول کاغذی نیست. پرداخت الکترونیکی به گونه‌های مختلف از جمله: کارت‌های اعتباری (کردیت کارت و دبیت کارت) و شبکه‌های ACH[1] انجام‌پذیر است. سیستم ACH شامل سپرده‌ی مستقیم، بدهی (وام) مستقیم و چک‌های الکترونیکی(e-checks) می‌باشد. سه نوع ترانکنش برای تمامی متدهای پرداخت الکترونیکی تبیین می‌شود (Cooper., Leavell, ۲۰۱٦):

۱. پرداخت در حین خرید (مشتری به فروشنده)
۲. پرداخت در محدوده‌ی زمانی مشخص
۳. پرداخت خودکار بانک به فروشنده

کدهای QR کدهای ماتریسی یا بارکدهای دو بعدی هستند که در تمامی محدوده‌ی ۳۶۰ درجه قابل خواند توسط دستگاه‌های مربوطه هستند. این کدها توانایی ذخیره‌سازی تا ۴۲۹۶ کاراکتر الفبای انگلیسی (یا ۱۸۱۷ الفبای ژاپنی) را در خود دارد. خصوصیت بارز اینگونه کدها، مقاومت زیاد آن‌ها در برابر خرابی بوده که آن را در صنعت بسیار محبوب ساخته است. Paypal نخستین شرکتی است که با ادغام کدهای QR و پرداخت‌های اینترنتی، خرید آنلاین محصولات را ساده‌تر از گذشته نموده است. به این صورت که کاربر با وارد کردن حساب کاربری در دستگاه تلفن همراه خود و اسکن بارکد محصول موجود در فروشگاه، قادر به پرداخت مبلغ آن خواهد بود. این روش در پرداخت قبوض نیز بسیار کارا و مناسب است.

از طرفی، با توجه به عدم توانایی انسان در خواندن و تشخیص کدهای QR، امکان تشخیص کدهای سالم از کدهای بدخواه توسط او وجود ندارد (Rouillard, ۲۰۰۸). کدهای QR به دو روش جعل می‌شوند: جایگزینی کامل کد با یک کد QR مخرب و یا تغییر بخشی از کد اصلی؛ که در حالت دوم تعیین اصالت کد حتی از طریق تطابق عینی آن با کد اصلی دشوار خواهد بود. حتی در صورت اسکن یک کد QR، قضاوت درباره سلامت آن توسط کاربر عملی دشوار خواهد بود. در چنین شرایطی، آسیب‌پذیری کاربران در استفاده از این کدها همچنان یک چالش اساسی بوده و نیازمند ارائه سیستم‌هایی جهت تعیین سلامت کدهای QR می‌باشیم. براین اساس، در این تحقیق ضمن پرداختن به مشکلات

[1] Automated Clearing House

امنیتی موجود در کدهای QR، یک سیستم امنیتی جهت تشخیص صحت کدهای QR با استفاده از تکنیک‌های یادگیری ماشین ارائه خواهد شد. همانطور که می‌دانیم سه هدف دسترس‌پذیری، یکپارچگی و محرمانگی مهمترین ارکان امنیتی یک سیستم بوده که معماری و طراحی مناسب باید این شرط را برآورده سازد. لذا ارائه یک راهکار تایید صحت کدهای QR، باید با درنظر گرفتن خصوصیات فوق، امنیت کاربران را فراهم نماید. در این تحقیق، ابتدا ویژگی-های کدهای QR براساس خصوصیات محتوایی آنها استخراج شده و آدرس مقصد این کدها مورد تجزیه و تحلیل قرار خواهد گرفت. بدین منظور، از ترکیب تکنیک‌های لیست سیاه و الگوهای مشکوک در ویژگی‌های QR استفاده خواهد شد. پس از استخراج ویژگی‌های کد QR، از تکنیک‌های یادگیری ماشین مانند شبکه عصبی مصنوعی جهت تشخیص صحت و اعتبار کدهای QR استفاده خواهد شد.

مبانی نظری

موضوع «شناسایی و تعیین اصالت کدهای QR مبتنی بر تکنیک‌های یادگیری ماشین» یک حوزه میان‌رشته‌ای است که در مرز میان امنیت داده، پردازش تصویر، یادگیری ماشین و تحلیل کیفیت چاپ قرار می‌گیرد. با افزایش وابستگی زندگی دیجیتال به ابزارهایی مانند پرداخت‌های موبایلی، احراز هویت مبتنی بر تصویر، بلیت‌های آنلاین، بسته‌های لجستیکی و سامانه‌های مبتنی بر هویت دیجیتال، کدهای QR به یک جزء حیاتی از تعاملات روزمره تبدیل شده‌اند (عباسی و مؤمنی، ۱۳۹۹). این کدها حجم زیادی از اطلاعات را در خود ذخیره می‌کنند و قابلیت خوانش سریع توسط دوربین گوشی هوشمند، آن‌ها را به یک ابزار پرکاربرد بدل ساخته است. اما همین گستره استفاده موجب شده است که امنیت و اصالت‌سنجی آن‌ها اهمیت حیاتی پیدا کند. نخست باید به این نکته توجه کرد که کدهای QR در اصل برای ذخیره‌سازی داده طراحی شده‌اند، نه برای تضمین اصالت. در نتیجه هر کاربری قادر است ظرف چند ثانیه یک کد QR جدید تولید کند که از لحاظ شکل ظاهری هیچ تفاوتی با نمونه اصلی ندارد (رحیمی و همکاران، ۱۴۰۰). این مسأله، زمینه‌ساز حملاتی مانند جعل پرداخت، فیشینگ تصویری، هدایت کاربر به لینک‌های مخرب، دستکاری بسته‌های لجستیکی، سوءاستفاده در بلیت‌فروشی و حتی جعل هویت دیجیتال شده است. بنابراین «اصالت‌سنجی» به معنای تشخیص اینکه یک کد **همان نسخه اصلی است یا نسخه‌ای جعلی**، به یک ضرورت جدی امنیتی تبدیل شده است.

در دهه نخست استفاده از QR، روش‌های سنتی مانند امضاهای دیجیتال، کلیدهای رمزگذاری، تطبیق محتوایی و کدهای امنیتی مخفی‌شده در داده مورد استفاده قرار گرفت (رضوانی و همکاران، ۱۳۹۸). اگرچه این روش‌ها در برابر دستکاری دیجیتال مقاوم بودند، اما دو محدودیت داشتند: نخست نیاز به زیرساخت پردازشی و اتصال شبکه، و دوم ناتوانی در تشخیص نمونه‌های جعلی چاپ‌شده. این مسئله بسیار مهم است، زیرا بیشتر جعل‌های عملی در محیط واقعی، با **چاپ مجدد** یا **بازتولید تصویری** انجام می‌شود. مهاجمان غالباً یک QR واقعی را چاپ می‌کنند، تغییرات کوچک در لبه‌ها یا سلول‌ها ایجاد می‌کنند، و نسخه اصلاح‌شده را جایگزین نسخه اصلی در محیط فیزیکی می‌کنند. این نسخه‌ها از نظر محتوایی کاملاً معتبرند و تنها از نظر کیفیت چاپ یا ساختار تصویری دچار تغییر هستند (غفاری، ۱۳۹۹). در نتیجه روش‌های صرفاً رمزنگاری‌شده نمی‌توانند چنین جعل‌هایی را تشخیص دهند.

در پاسخ به این ضعف، حوزه «پردازش تصویر» وارد عمل شد و رویکردهایی مطرح شد که از خصوصیات ظاهری، ساختاری و بافتی کدهای QR برای تعیین اصالت بهره می‌بردند. اما این روش‌ها نیز به استفاده از **ویژگی‌های دستی** متکی بودند؛ ویژگی‌هایی مانند لبه‌ها، شدت پیکسل، الگوی بافت، اعوجاج هندسی و نویز تصویر. هرچند این ویژگی‌ها قادر بودند بخشی از تفاوت میان نسخه‌های اصلی و جعلی را نشان دهند، اما به‌دلیل پیچیدگی‌های زیاد الگوهای چاپگرها، دستگاه‌های مختلف تولید QR و تفاوت‌های محیطی مانند نور، زاویه و کیفیت تصویر، دقت روش‌های دستی محدود بود (شریفی و نادری، ۱۴۰۰). با گسترش یادگیری ماشین و یادگیری عمیق، این حوزه وارد مرحله جدیدی شد. یادگیری ماشین این قابلیت را دارد که بدون نیاز به تعریف ویژگی توسط انسان، هزاران تصویر QR را تحلیل و تفاوت‌های پنهان، ظریف و غیرقابل مشاهده را استخراج کند. این تفاوت‌ها می‌تواند شامل موارد زیر باشد:

- تفاوت میان سلول‌های سفید و سیاه در نمونه چاپ‌شده،
- تغییرات بسیار کوچک در مرز سلول‌ها،
- تفاوت در الگوی پراکندگی پیکسل‌ها،
- نویز ناشی از چاپگر،
- اثر انگشت دستگاه تولیدکننده کد،
- تغییرات ناشی از بازفشرده‌سازی یا کاهش کیفیت،
- تفاوت در ضخامت مرزی نقاط مربعی،
- نشانه‌های ریز ناشی از جعل دیجیتال (حیدری و رهنورد، ۱۴۰۱).

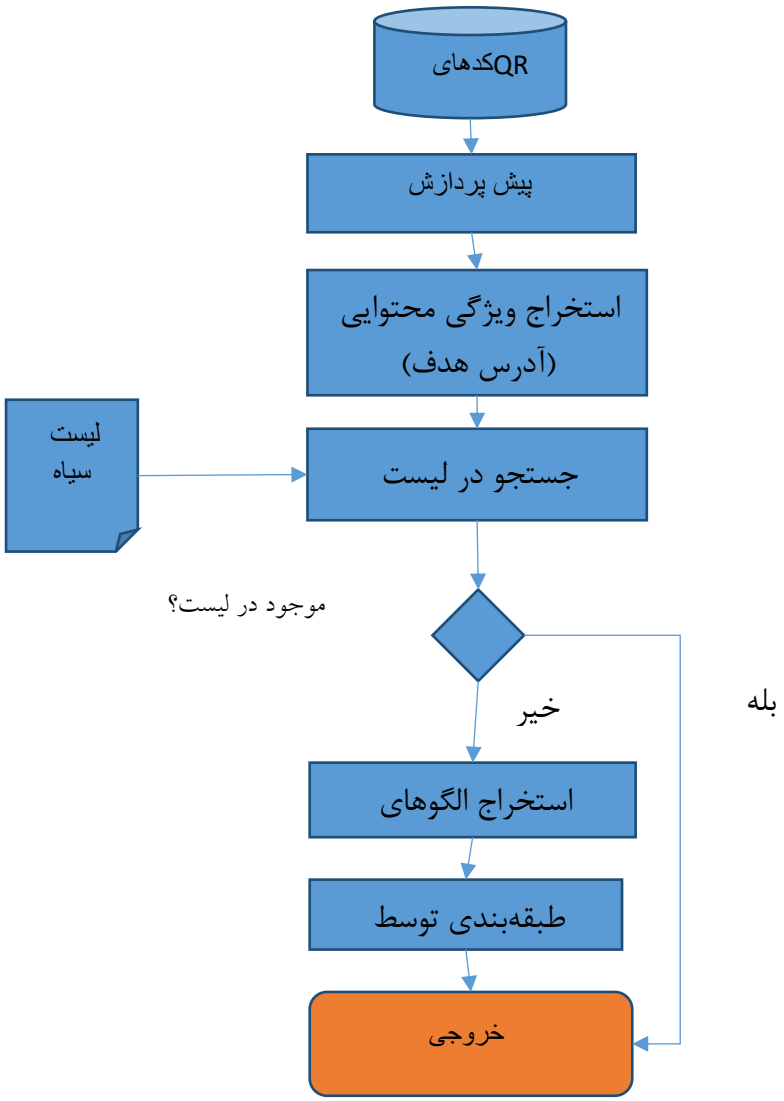
در شبکه‌های عصبی کانولوشنی (CNN)، ویژگی‌ها به‌صورت چندلایه و سلسله‌مراتبی استخراج می‌شوند. به این صورت که لایه‌های اولیه، الگوهای ساده مانند لبه‌ها را تشخیص می‌دهند، لایه‌های میان‌رده، بافت‌ها و الگوهای هندسی را استخراج می‌کنند، و لایه‌های بالاتر الگوهای پیچیده و مرتبط با جعل را تحلیل می‌کنند (کاظمی و احمدی، ۱۴۰۱). این ساختار چندلایه باعث می‌شود مدل قادر باشد تفاوت‌هایی را تشخیص دهد که هیچ روش سنتی یا دستی قادر به دیدن آن نیست. اما یادگیری عمیق تنها یک بخش از معادله اصالت‌سنجی است. بخش دیگر «تحلیل کیفیت چاپ» است. هر چاپگر یا دستگاه خروجی (لیزری، جوهرافشان، حرارتی و...) یک الگوی منحصربه‌فرد از پاشش رنگ، وضوح مرزی و نویز سیستماتیک دارد که مانند اثر انگشت دستگاه قابل شناسایی است (محمدی و فلاح، ۱۴۰۲). به‌همین دلیل پژوهشگران از ترکیب ویژگی‌های چاپ و مدل‌های یادگیری ماشین برای شناسایی منبع تولید QR و تشخیص نمونه‌های جعلی استفاده می‌کنند. تنها با یک تصویر ساده از QR می‌توان تعیین کرد که آیا نسخه مشاهده‌شده با چاپگر ثبت‌شده در پایگاه داده تولید شده یا خیر. این موضوع کاربردهایی مانند تشخیص جعل بلیت، کنترل اصالت بسته‌های پستی و بررسی هویت اسناد چاپی را ممکن ساخته است.

رویکردهای جدیدتر تلفیقی هستند و از چند لایه امنیتی استفاده می‌کنند. برای مثال برخی پژوهشگران از واترمارک‌های نامرئی در لایه تصویری QR استفاده می‌کنند که با چشم دیده نمی‌شود اما در ساختار عددی پیکسل‌ها وجود دارد. سپس مدل یادگیری عمیق علاوه بر تحلیل ساختاری QR، وجود یا عدم وجود این واترمارک را بررسی

می‌کند (صادقی و همکاران، ۱۴۰۳). این روش در برابر حملات چاپ–اسکن، تغییر اندازه، تغییر فرمت، وضوح پایین و حتی بازطراحی QR مقاومت بالایی دارد. در مجموع، مبانی نظری این حوزه نشان می‌دهد که اصالت‌سنجی کدهای QR یک موضوع تک‌بعدی نیست. نمی‌توان فقط از رمزنگاری، یا فقط از پردازش تصویر استفاده کرد. بهترین نتایج زمانی به‌دست می‌آیند که ترکیبی از: یادگیری ماشینی،یادگیری عمیق،تحلیل کیفیت چاپ،پردازش تصویر،ویژگی‌های فیزیکی دستگاه،و حتی رمزنگاری دیجیتال به‌صورت یک سیستم یکپارچه مورد استفاده قرار گیرد (حسینی و همکاران، ۱۴۰۳). هر کدام از این حوزه‌ها نقص‌ها و مزایای خود را دارند، اما ترکیب آن‌ها امکان تشخیص اصالت با دقت بسیار بالا را فراهم می‌کند. این ترکیب به‌ویژه در کاربردهایی مانند پرداخت، هویت دیجیتال، کنترل دسترسی و حمل‌ونقل هوشمند اهمیت دوچندان پیدا می‌کند.

روش کار

در روند اجرای تحقیق، ابتدا به مطالعات کتابخانه‌ای در زمینه موضوع پرداخته و سپس به بررسی تحقیقات صورت گرفته و روش‌های ارائه شده پیشین خواهیم پرداخت و نقاط قوت و ضعف هر روش را مورد مطالعه قرار خواهیم داد. پس از انجام مطالعات اولیه، به طراحی روش پیشنهادی خواهیم پرداخت. فرآیند تشخیص کدهای QR جعلی در روش پیشنهادی بصورت یک دیاگرام در شکل (۱) نمایش داده شده است.



شکل ۱. فرآیند تشخیص اصالت کدهای QR در روش پیشنهادی

مطابق دیاگرام نمایش داده شده در شکل (۱)، روش پیشنهادی با پیش‌پردازش اطلاعات کدهای QR آغاز می‌شود. گام پیش‌پردازش شامل مجموعه‌ای از فرآیندها برای حذف نویز از ورودی‌ها و تبدیل آن به یک فرم استاندارد و قابل پردازش در گام‌های محاسباتی آتی می‌باشد. در گام دوم، ویژگی‌های محتوایی هر کد استخراج خواهد شد. ویژگی‌های محتوایی، به آدرس هدف موجود در هر کد اشاره دارد و با استفاده از تکنیک لیست سیاه، برخی از کدهای مخرب

شناسایی و فیلتر می‌شوند. در صورتی که آدرس هدف یک کد در لیست سیاه موجود نباشد، در گام بعدی به استخراج و طبقه‌بندی الگوهای مشکوک به جعل در کدهای ورودی می‌پردازیم. الگوهای مشکوک به جعل نیز، به مجموعه ویژگی‌هایی اشاره دارد که بصورت مستقیم از الگوی کد QR استخراج شده و از طریق طبقه‌بندی این ویژگی‌ها می‌توان کدهای مشکوک به دستکاری را شناسایی نمود. بدین منظور از یک شبکه عصبی مصنوعی استفاده می‌شود. این مدل یادگیر، یک شبکه مصنوعی پروسپترون چندلایه بوده که براساس نمونه‌های موجود در پایگاه داده آموزش دیده و توانایی طبقه‌بندی الگوهای استخراج شده از نمونه‌های جدید را دارد. پس از ارائه روش پیشنهادی به شبیه سازی و ارزیابی آن با استفاده از نرم‌افزار MATLAB خواهیم پرداخت. پس از پیاده سازی و ارزیابی روش پیشنهادی، نتایج حاصل را با کارهای پیشین مقایسه نموده و در صورت لزوم، به تصحیح و بهینه سازی روش ارائه شده خواهیم پرداخت. در انتها، به تحلیل نتایج پرداخته و نقات قوت و ضعف روش پیشنهادی را مورد بررسی قرار خواهیم داد.

روش گردآوری اطلاعات

روش انجام تحقیق کتابخانه‌ای می‌باشد، داده‌های تحقیق با استفاده از مقالات منتشره درمجلات و کنفرانس‌های علمی معتبر و همچنین بانک‌های اطلاعاتی و شبکه‌های کامپیوتری، پایگاه داده انتشارات معتبر علمی دنیا همچون Springer، Elsevier، IEEE و... گردآوری می‌شود. به منظور گردآوری اطلاعات، از پایگاه‌های علمی معتبر و مجلات منتشر شده و کنفرانس‌های علمی مرتبط با حوزه تحقیق استفاده خواهد شد. همچنین به منظور ارزیابی عملکرد روش پیشنهادی از پایگاه داده CUHK-CQRC استفاده خواهد شد.

روش تجزیه و تحلیل اطلاعات :

تجزیه و تحلیل اطلاعات و بررسی عملکرد روش پیشنهادی با سایر روش‌های مشابه، به کمک فرآیند شبیه‌سازی کامپیوتری و در محیط نرم‌افزاری MATLAB انجام می‌گیرد. به منظور انجام آزمایشات و دستیابی به نتایجی واقع گرایانه، از روش شبیه‌سازی مونت کارلو استفاده خواهد شد. همچنین به منظور مقابله با ماهیت تصادفی داده‌های آزمون، فرآیند شبیه‌سازی را چندین بار تکرار نموده و میانگین نتایج را مورد استفاده قرار خواهیم داد. لازم به ذکر است که ارزیابی عملکرد روش پیشنهادی از طریق معیارهای مانند: دقت، حساسیت، ویژگی و زمان پردازش مورد بررسی قرار خواهد گرفت. معیار حساسیت برای اندازه گیری نسبت کل کدهای جعل شده‌ای که بطور صحیح تشخیص داده شده‌اند بکار می‌رود و بصورت زیر محاسبه می‌شود:

$$Sensitivity = \frac{TP}{TP+FN} \times ۱۰۰$$

که در رابطه فوق، TP کدهای جعل شده‌ای است که بصورت صحیح تشخیص داده شده‌اند و FN کدهای جعل شده‌ای است که بعنوان کدهای صحیح تشخیص داده شده‌اند. معیار ویژگی برای اندازه‌گیری کدهای صحیحی است که بصورت درست طبقه‌بندی شده‌اند بکار می‌رود. این معیار بصورت زیر محاسبه می‌شود:

OPEN ACCESS

$$Specificity = \frac{TN}{TN+FP} \times ۱۰۰$$

در رابطه فوق، TN کدهای صحیحی است که بصورت درست تشخیص داده شده‌اند و FN کدهای صحیحی است که بعنوان کدهای جعل شده تشخیص داده شده‌اند. معیار دقت نیز با استفاده از رابطه زیر محاسبه می‌شود:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$$

تولید کدهای QR

چارچوب پیشنهادی ما بر اساطس یک طرح کد QR پیشرفته است. با این طرح، یک کد QR استاندارد پردازش می‌شود تا در نهایت یک جفت کد QR پیشرفته ($SQR^{۱}$,$SQR^{۲}$) تولید شود که می‌تواند به عنوان دو قطعه از یک QR الکترونیکی دیده شود. کدهای QR پیشرفته محرمانه بودن کوپن ها را تضمین می کنند و دستکاری یا جعل آنها سخت است.

الگوریتم :۱ کدگذاری QR پیشرفته

۱: procedure ENCODING (Sensitive Data *data*)

۲: (*com*, *decom*) ⇐ *Com*(crs, data)

۳: *QR* ⇐ *Encode*(*com*)

۴: ($QR^{۱}$, $QR^{۲}$) ⇐ *Split*(*QR*)

۵: $SQR^{۱}$ ⇐ Stack (QR^{1}, *CQR*)

۶: *SQR*۲ ⇐Stack (QR^{2}, *CQR*)

۷: return ($SQR^{۱}$, $SQR^{۲}$)

۸: end procedure

جریان تولید کدهای QR پیشرفته در شکل ۱ نشان داده شده است. همانطور که الگوریتم ۱ توضیح می دهد، چهار عملکرد اصلی وجود دارد.

Com (*crs*, *data*): انجام فرایند تعهد برروی داده ها

Encode(*com*): تولید QR کد و محتوای خاص com

Split(*QR*): یک جفت الگوی شبه تصادفی را با رویکرد مبتنی بر کدگذاری قطعه برQR. باز می‌گرداند.

Stack (QR^{1},*CQR*): ایجاد یک ترکیب گرافیکی بینQR کد CQR و QR با عنوان CQR

برخی جزییات به رح زیر می باشد:

۱) تعهد: ظرفیت کدهای QR و اندازه تعهدات، داده های حساس .data را در یک کوپن الکترونیکی در نظر بگیرید.

فصلنامه پژوهش های نوین درعمران، معماری و شهرسازی شماره۳ – دوره ۱- صفحات ۱۳۷-۱۵۱
Journal of New researches in Civil Engineering, Architecture and Urban Planning
ISSN: 3060-608X

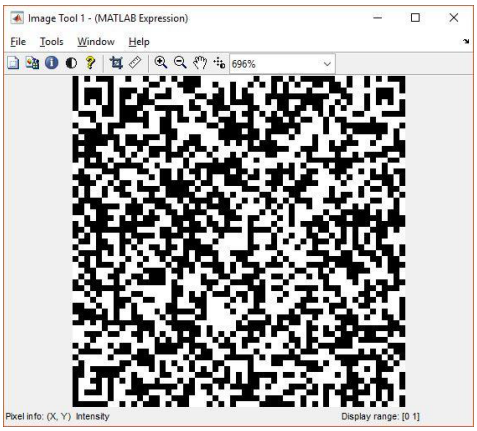
برای اطمینان از محرمانه بودن data. به عنوان Step. ۲، ما از تکنیک تعهد پدرسن برای تولید تعهد $com = g^{data}h^{r}$ $mod\ p$ استفاده می کنیم بطوریکه (p,g,h,r) پارامترهای امنیتی هستند. با چنین طرح تعهد کامل پنهان، حتی اگر M و C حمله تبانی شده ای را انجام دهند، آنها نمی توانند چیزی از data. را از com دریافت کنند.

۲) رویکرد QRFC :

با ایده رمزنگاری بصری، QRFC را رویکرد مبتنی بر کدگذاری قطعه برای کدهای QR را معرفی می‌کنیم. از طریق QRFC ، $\overline{QR}$ را به یک کد QR استاندارد بخش می نماییم، که در مرحله ۳ با com رمزگذاری شده اند، به دو بخش $(\overline{QR2QR1},)$ تقسیم کنیم.

۳) کدهای حاوی QR: از آنجایی که مشتریان به یک راه آسان برای دسترسی به برخی اطلاعات عمومی مانند نام فروشنده، تاریخ انقضای کلید و مبلغ نیاز دارند، ما یک کد QR استاندارد، $\overline{QR}$ ، معرفی می‌کنیم.

CQR همچنین حاوی یک هش از $h(QR^{1})$ و QR^{1} می‌باشد که می تواند برای تأیید. QR^{1} استفاده شود. $h(QR^{1})$ از طریق الگوریتم هش امن (SHA) با کلید مخفی مربوطه (key) تولید می شود. کدهای QR بهبود یافته $\overline{\overline{SQR}^{1}}$ و $\overline{\overline{SQR}^{2}}$ را می‌توان با مرحله ۵ تولید کرد، یعنی قرار دادن QR^{1} و QR^{2} به طور جداگانه در CQR بدون آسیب رساندن به داده‌های موجود در *CQR*. ما شبکه خود را با انواع مختلف نویز از جمله نویز گوسی و نمک و فلفل آزمایش کردیم. برای نویز گاوسی، شبکه با موفقیت کدها را حذف کرده بود و کارایی خود را بر روی یک نوع نسبتاً رایج نویز نشان می داد. کدهای QR با نویز گاوسی variance=۰,۳ توسط برنامه کاملاً حذف شدند، همانطور که در شکل های زیر مشاهده می شود. کد QR حذف شده دقیقاً با کد اصلی مطابقت دارد.



variane=۰,۳ با نویز گوسی qrشکل: کد

کد اصلی qrشکل:

کد با نویز حذف شده qrشکل:

ما همچنین حذف نویز کدهای QR را با نویز نمک و فلفل در شبکه خود آزمایش کردیم. چنین نویزهایی به طور معمول در تصاویر باینری به دلیل نوسانات حرارتی تصادفی در دوربین ها یافت می شود - نویز نمک و فلفل که بر کل کد QR تأثیر می گذارد به طور موثر حذف شد و کد QR اصلی به طور کامل بازیابی شد، همانطور که در شکل های زیر مشاهده می شود.

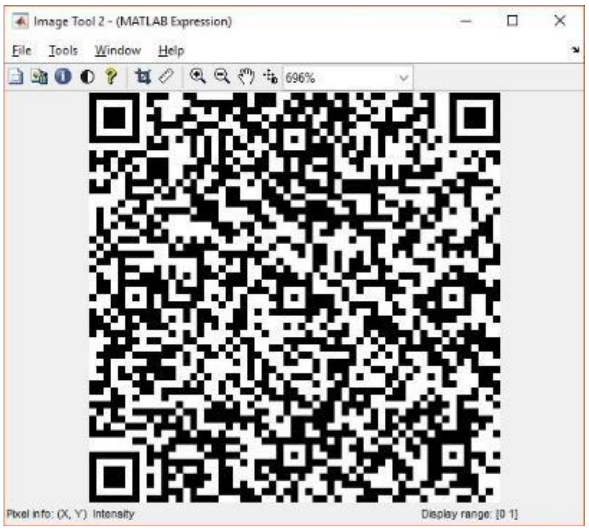
شکل: تصویر کد اصلی qr

شکل: تصویر با نویز نمک و فلفل qr

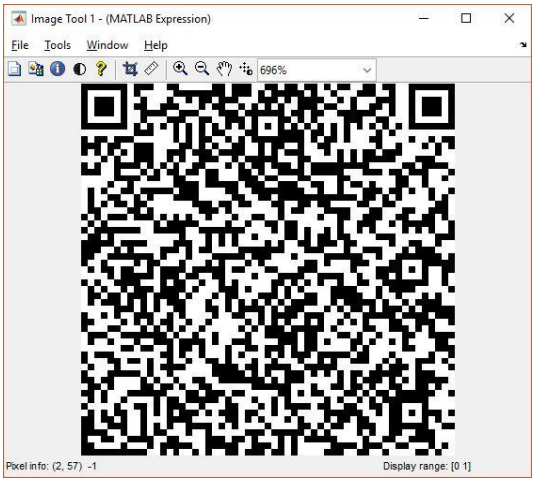
شکل: کد با نویز حذف شده qr

ISSN: 3060-608X

OPEN ACCESS



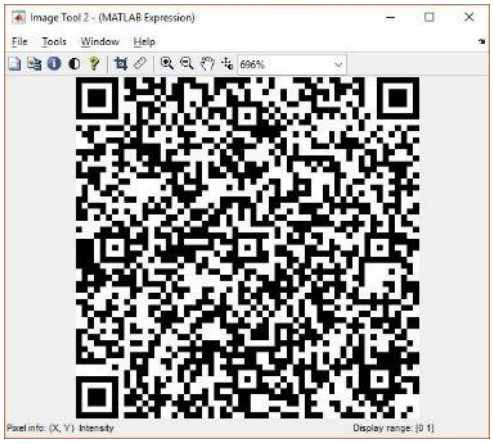
کد اصلیqrشکل: تصویر



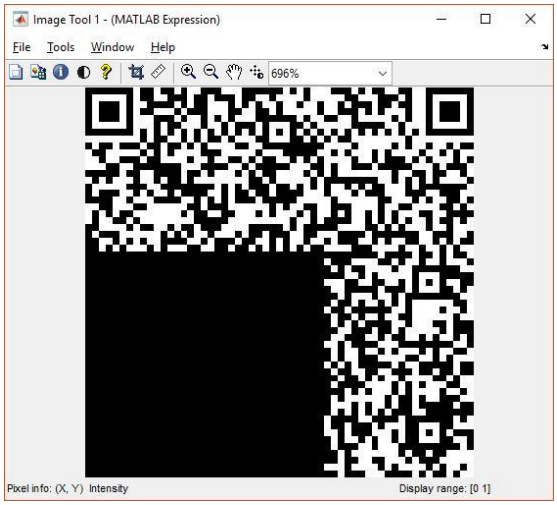
کد در گوشه سمت چپ آن مقدار qrشکل: تصویر
زیادی نویز نمک و فلفل قرار دارد

با نویز حذف شدهqrشکل: تصویر

ما همچنین شبکه خود را بر روی کدهای QR که در آن منطقه بسیار پر سر و صدا یا کاملاً تخریب شده است، آزمایش کردیم. این نوع موقعیت در سناریوهای دنیای واقعی اتفاق می‌افتد (مخصوصاً زمانی که کد QR در فضای باز نگهداری می‌شود و در معرض فرسودگی قرار می‌گیرد) و شبکه ما نیز باید در چنین شرایطی عملکرد خوبی داشته باشد. چنین کدهای QR با گوشه ای که تحت تأثیر مقادیر بالای نویز نمک و فلفل قرار دارند و همچنین شبکه ما کاملاً حذف شده است، همانطور که در شکل های زیر مشاهده می شود.



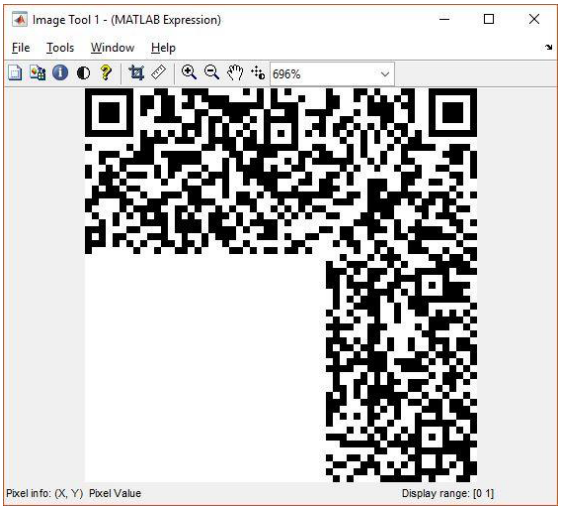
کد اصلیqrشکل: تصویر



کد گوشه سمت چپ سیاه شده استqrشکل: تصویر

با نویز حذف شدهqrشکل: تصویر

کد اصلی qrشکل: تصویر



کد گوشه سمت چپ سفید شده استqrشکل: تصویر

با نویز حذف شدهqrشکل: تصویر

در این پژوهش الگوریتم بکار رفته به طور دقیق کدهای QR را با انواع مختلف نویز حذف کرد. ظرفیت ذخیره سازی کدهای QR برای سیستمی از n شبکه (۴۰۰ × n) که در آن n تعداد شبکه هایی است که به صورت موازی استفاده می شوند. همچنین، بسیار سریعتر از یک شبکه هاپفیلد منفرد با ظرفیت یکسان است، به طوری که اگر شبکه ما دارای ۳۲۴۹ گره و ظرفیت ۴۰۰ × n باشد، یک شبکه هاپفیلد منفرد دارای ۳۲۴۹ × n گره خواهد بود که ظرفیت یک شبکه هاپفیلد به صورت خطی مقیاس می شود. چنین شبکه‌ای با ۳۲۴۹ × n گره بسیار کندتر عمل می نماید، زیرا دارای ماتریس وزنی بسیار بزرگ‌تر از است(۲(۳۲۴۹×n)). در حالی که در این مقاله (۳۲۴۹) می‌باشد. بنلبراین بروز رسانی را بسیار سریعتر می کند. همچنین، الگوریتم ما نسبت به یک شبکه هاپفیلد با همان ظرفیت ذخیره سازی، حافظه کمتری مصرف می کند. یک شبکه منفرد با ظرفیت ذخیره سازی یکسان نیاز به ذخیره سازی مرتبه ۲(۳۲۴۹×n) دارد. الگوریتم ما به ذخیره‌سازی بسیار کمتری نیاز دارد(۲(۳۲٤۹) * n).

این بدان معناست که الگوریتم ما در این پژوهش به دستاوردهای بزرگی در سرعت و نیازهای ذخیره‌سازی نسبت به شبکه‌های معمولی منجر می‌شود و آنها را برای اهداف متنوع‌تری امکان‌پذیر می‌کند. همانطور که در نتایج مشاهده می شود، می توان مقادیر زیادی نویز را با روش حذف نویز ما حذف نمود. الگوریتم ما برای توزیع کدهای QR در چندین شبکه هاپفیلد و انتخاب صحیح، به افزایش ظرفیت ذخیره سازی کدهای QR توسط شبکه ها کمک می کند و بنابراین استفاده از آن در سیستم های بزرگ برای تشخیص کد QR امکان پذیر است. برای انتخاب شبکه ای که حاوی کد QR حذف شده است، از تعداد زیادی حداقل های جعلی و عملکرد انرژی شبکه استفاده می کند. همچنین، روش ما سریع‌تر از ذخیره همه شبکه‌ها در روشی بسیار بزرگ‌تر است، زیرا چندین شبکه کوچکتر داریم که فقط برای چند تکرار (در مورد ما فقط حدود ۱۰۰) اجرا می‌شوند. فقط یکی از آنها (که همچنین یک شبکه کوچک است) تا زمان همگرایی اجرا می شود، بنابراین یک مزیت سرعت بسیار زیاد را ارائه می دهد. همچنین هزینه ذخیره سازی شبکه را کاهش می دهد و آن را در مقایسه با یک شبکه هاپفیلد n برابر کاهش می دهد. از این روش می توان در کاربردهای مختلف شبکه هاپفیلد برای افزایش ظرفیت استفاده کرد.

منابع

- Ahmed, M. M., (۲۰۱۹), Payment Transaction System Using QR Codes, University of Arizona, Internal Publications.
- Chan, P., Halevi, T., Memon, N., (۲۰۱۵), Glass OTP: Secure and Convenient User Authentication on Google Glass. In International Conference on Financial Cryptography and Data Security (pp. ۲۹۸-۳۰۸). □□□□□□□□ □□□□□□ □□□□□□ □□□□□□□□□□□.
- Ityala, S., Sharma, O., Honnavalli, P.B. (۲۰۱۹), Transparent Watermarking QR Code Authentication for Mobile Banking Applications. In International Conference on Inventive Computation Technologies (pp. ۷۳۸-۷٤۸). Springer, Cham.
- Leavell, P., Cooper, D., (۲۰۱٦), The Internet of Things: Strategic considerations for bankers. Journal of Digital Banking, ۱(۱), ۲۲-۳۲.
- Liu, R., Song, J., Huang, Z., Pan, J., (۲۰۱۹), EQRC: An Enhanced QR Code-Based Secure E-coupon Transaction Framework. In ICC ۲۰۱۹-۲۰۱۹ IEEE International Conference on Communications (ICC) (pp. ۱-٦). IEEE.

– Pan, H., Chen, Y. C., Yang, L., Xue, G., You, C. W., Ji, X. (۲۰۱۹), mQRCode: Secure QR Code Using Nonlinearity of Spatial Frequency in Light. In The ۲۵th Annual International Conference on Mobile Computing and Networking (p. ۲۷). ACM.

– Pan, H., Yang, L., Chen, Y. C., Xue, G., You, C. W., Ji, X., Chen, P. Y. (۲۰۱۹), Poster: Secure Visible Light Communication based on Nonlinearity of Spatial Frequency in Light. In The ۲۵th Annual International Conference on Mobile Computing and Networking (p. ۹۳). ACM.

– Pérez-Sanagustín, M., Parra, D., Verdugo, R., García-Galleguillos, G., Nussbaum, M., (۲۰۱٦), Using QR codes to increase user engagement in museum-like spaces. Computers in Human Behavior, ٦۰, ۷۳-۸۵.

– Rouillard, J., (۲۰۰۸), Contextual QR codes. In Computing in the Global Information Technology, ۲۰۰۸. □□□□□□□۰۸. □□□ □□□□□ □□□□□□□□□□□□□□ □□□□□-□□□□□□□□□□□ □□ (□□. ۵۰-۵۵). □□□□.

– Wan, S., Yang, G., Qi, L., Li, L., Yan, X., Lu, Y., (۲۰۱۹), Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code. Mathematical biosciences and engineering: MBE, ۱٦(٦), ٦۳٦۷-٦۳۸۵.

– Wen, X., Chen, Y., Fang, J., (۲۰۱۳), An inter-bank E-payment protocol based on quantum proxy blind signature. Quantum information processing, ۱۲(۱), ۵٤۹-۵۵۸.

– Yang, Z., Cheng, Z., Loy, C. C., Lau, W. C., Li, C. M., Li, G. (۲۰۱٦), Towards robust color recovery for high-capacity color QR codes. In Image Processing (ICIP), ۲۰۱٦ IEEE International Conference on(pp. ۲۸٦٦-۲۸۷۰). IEEE.

– Zhu, X., Hou, Z., Hu, D., Zhang, J. (۲۰۱٦), Secure and Efficient Mobile Payment Using QR Code in an Environment with Dishonest Authority. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. ٤۵۲-٤٦۵). Springer, Cham.