

چکیده

رتینوپاتی دیابتی یکی از عوارض شایع میکروآنژیوپاتی دیابت شیرین محسوب می‌شود. فرد مبتلا به رتینوپاتی دیابتی باید به صورت مداوم و طی بازه‌های زمانی مشخصی کنترل شود تا روند پیشرفت بیماری تحت کنترل در آید. با توجه به محدودیت‌های منابع تجهیزات و انسانی پزشکی از راه دور برای چشم‌پزشکی به خدمت گرفته شده است تا کیفیت خدمات ارائه شده ارتقا یابد. بسترهای مخابراتی انتقال داده به عنوان پلی میان بیمار و کارشناس متخصص هست. ساده‌ترین راهکار ارائه امنیت اطلاعات و حفظ حریم شخصی در بستر مخابراتی رمز کردن اطلاعات هست. از سال ۱۹۹۹ تاکنون الگوریتم‌های رمزنگاری متعددی برای ارائه سطح قابل‌قبولی از امنیت اطلاعات معرفی شده‌اند ولی تاکنون هیچ مطالعه‌ای باهدف انتخاب یک رمزنگار بهینه برای تصاویر پزشکی صورت نگرفته است. در این مطالعه سه الگوریتم برتر رمزنگار بلوکی که معرفی شده‌اند پیاده‌سازی و مورد بررسی قرار گرفته‌اند. مقایسه میان الگوریتم توسط ۷ آزمون حساسیت به نویز، حساسیت به کلید، حساسیت به متن آشکار، کیفیت رمزنگاری، همبستگی متقابل، آنتروپی و سرعت رمزنگاری صورت گرفته است. در نتایج مشاهده شده است الگوریتم رمزنگاری Rijndael به طور کلی در مقایسه بدون اولویت الگوریتم برتر در این ارزیابی می‌باشد. ولی هیچ‌کدام از این الگوریتم‌ها به تنهایی نیازهای مورد نظر برای پزشکی را ارضا نمی‌کنند. به همین جهت حالت‌های کارکرد متفاوت نیز برای الگوریتم Rijndael مورد بررسی قرار گرفته است. حالت‌های کارکردی رمزنگاری OFB و CTR به جهت کاهش حساسیت به نویز بسیار موثر واقع شده‌اند. اما حالت کارکردی CTR به لحاظ امکان پردازش‌های موازی مناسب‌تر ارزیابی شده است. همچنین باید افزود در این مطالعه نسخه ابتدایی یک الگوریتم رمزنگاری مبتنی بر سیستم‌های آشوبگونه معرفی شده است که از لحاظ سرعت ۲۵٪ سریعتر از Rijndael رمزنگاری را انجام می‌دهد و در سایر معیارها قدرت و برتری خود را نشان داده است.

کلیدواژه‌ها

امنیت داده‌های پزشکی، رمزنگاری تصاویر شبکه‌ی چشم، آنالیز رمزنگاری تصاویر، آنالیز آماری الگوریتم‌های رمزنگاری