سیویلیکا – ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:

آنالیز کیفیت رمزنگاری تصاویر پزشکی مبتنی بر الگوریتم راین دال با کلید رمزنگاری یکسان و آشوب گونه

محل انتشار:

مجله انفورماتیک سلامت و زیست پزشکی, دوره 1, شماره 1 (سال: 1393)

تعداد صفحات اصل مقاله: 13

نویسندگان:

محمد رضا نعیم آبادی – کارشناس ارشد مهندسی پزشکی ، گروه مهندسی پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

علیرضا مهری دهنوی – Biomedical Engineering Dept, Isfahan University of Medical sciences, Isfahan, Iran.

حسین ربانی – م رکز تحق ی قات پردازش تصاویر و سیگنال های پزشکی، دانشگاه علوم پزشک ی اصفهان ، اصفهان ، ای ران

خلاصه مقاله:

مقدمه: با توجه به گسترش استفاده از فن آوری های ارتباطی بی سیم در انتقال داده های حیاتی، حفظ حریم خصوصی و امنیت داده ها از اهمیت زیادی برخودار می باشد. در حال حاضر با الگوریتم های متعددی رمزگذاری داده ها انجام می شود . اغلب این الگوریتم ها مبتنی بر رمزنگاری بلوکی می باشند که از یک کلید ثابت از پیش تعیین–شده استفاده می کنند که حداقل ۱۲۸ بیت طول دارد. روش: در این پژوهش، رمزنگاری با الگوریتم راین دال (Rijndael) با کلیدهای ثابت و متغیر صورت گرفته است. در رمزنگاری با کلید متغیر که در این مقاله طراحی شده است از یک بلوک مبتنی بر سیستم آشوب گونه Mackey Glass در واحد موتور تولیدکننده کلید به عنوان جایگزین الگوریتم گسترش کلید در قلب راین دال استفاده شده است و توسط یک بلوک کنترلی، رفتار آن بررسی و اصلاح می شود. نتایج: روش های رمزنگاری عنوان شده، توسط ۶ معیار رمزنگاری، بررسی و ارزیابی شد. ارزیابی ها نشان داده است استفاده از کلیدهای متغیر آشوب گونه با ۴۷/۲ درصد افزایش بار محاسباتی، توانایی الگورتیم راین دال را در پنهان کردن الگو و توزیع هیستوگرام در تصاویر پزشکی به شدت افزایش می دهد. استفاده از کلیدهای متغیر آشوب گونه به طور ذاتی تاثیری بر میزان حساسیت به کلید الگوریتم راین دال نداشته است. نتیجه گیری: استفاده از سیستم آشوب گونه در واحد گسترش کلید برای تصاویر پزشکی که در الگوریتم بهبود یافته راین دال عرضه شده است، امنیت داده های حیاتی و حفظ حریم شخصی را به خوبی فراهم می کند.

کلمات کلیدی:

Encryption quality analysis, Encryption robustness and efficiency analysis, Medical images encryption, Chaotic encryption,
آنالیز کیفیت رمزنگاری, آنالیز قدرت و بهره وری رمزنگاری, رمزنگاری تصاویر پزشکی, رمزنگاری مبتنی بر سیستم های آشوب گونه

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/2036278