عنوان مقاله:
بررسی یک روش رمزنگاری، اصلاح و بهبود آن

محل انتشار:
سومین کنفرانس آموزش و کاربرد ریاضیات (سال: 1398)

تعداد صفحات اصل مقاله: 10

نویسنده:
افشین یاقلی - *کارشناس ارشد ریاضی محض گرایش نظریه کدگذاری، دانشگاه رازی کرمانشاه*

خلاصه مقاله:
در این مقاله یک روش رمزنگاری تصویر مبتنی بر توابع آشوب و تبدیل APA که توسط Ahmad و همکاران ارائه شده است؛ آنالیز وبررسی می شود. نقایص موجود در این روش رمزنگاری موجب می شود که با استفاده از حمله متن آشکار، این روش تحلیل و شکستهشود. در ادامه به اصلاح این روش با استفاده از تابع آشوب هنون و آرنولدکت و جدول جانشینی AES می پردازیم. هردو طرح در نرم افزار Matlab پیاده سازی شده و سپس توسط برخی از آزمونهای رایج به بررسی اعتبار آنها می پردازیم.

کلمات کلیدی:
رمزنگاری تصویر، توابع آشوب لجستیک، هنون، آرنولدکت، تبدیل APA، مربع لاتین کلید دار، جدول جانشینی AES

لینک ثابت مقاله در پایگاه سیویلیکا: