

عنوان مقاله:

یک روش ترکیبی برای رمزنگاری تصویر با استفاده از توابع فوق آشوب و عملگرهای تکاملی

محل انتشار:

هشتمین کنفرانس انجمن رمز ایران (سال: 1390)

تعداد صفحات اصل مقاله: 6

نویسندگان:

سیدعبدالحمید اصفهانی - دانشگاه آزاد اسلامی واحد قاینات

داود بخشش - دانشگاه بجنورد ، دانشکده علوم پایه

خلاصه مقاله:

هر چند که توابع فوق آشوب 1 به دلیل پیچیدگی و بزرگ بودن فضای کلید آنها نسبت به دیگر توابع آشوب ، مقاومت بیشتری درمقابل حملات هکرها دارند اما الگوریتم‌ها یی که تنها از توابع فوق ک یاس برای رمزنگاری تصویر استفاده میکنند از مقاومت کافی در برابر حملات برخوردار نیستند. در این مقاله یک روش جدید جهت رمز کردن تصاویر بر پایه توابع فوق آشوب و عملگر ترکیب ارائه شده است . در این روش ما از قابلیت‌های توابع فوق آشوب که شامل حساسیت به مقادیر اولیه ، رفتار شبه تصادفی و غیر تناوبی بودن تابع می باشد ، بهره می گیریم . همچنین استفاده از عملگر ترکیب در ترکیب مقدار پیکسل ها باعث افزایش قدرت الگوریتم در برابر حمله کننده ها 2 می شود . روش ترکیبی در برابر بس یاری از الگوریتم‌های حمله کننده از قدرت و امنی ت کافی برخوردار است . علاوه بر این به جهت افزایش امنی ت، رمزگذاری تصویر به صورت برداری انجام می شود و ابعاد تصویر نیز به همراه مقادیر پیکسلها رمزگذاری می شود. بیشترین نسبت تفاوت PSNR بین تصویر رمز شده و تصویر اولیه 11 است این عدد نشان می دهد که تصویر رمز شده به اندازه کافی با تصویر اولیه متفاوت است.

کلمات کلیدی:

رمزنگاری تصویر ، تابع فوق آشوب ، الگوریتم تکاملی ، عملگر ترکیب ، الگوریتم حمله

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/125091>

