عنوان مقاله:
الگوریتم رمزنگاری مبتنی بر نگاشت آشوب استاندارد در رمزنگاری کلید متقارن بلوکی

محل انتشار:
سومین کنفرانس سراسری نوآوری های اخیر در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
افسانه کریم الدینی - *کارشناس ارشد*

حمید میروزیری - *دکتر*

زینب خراسانی کمال آباد - *کارشناس ارشد*

خلاصه مقاله:
نگاشت های آشوب امروزه به عنوان یکی از ابزارهای قدرتمند در زمینه ی رمزنگاری مورد مطالعه قرار گرفته اند. حساسیت به مقادیر و شرایط اولیه و نیز حساسیت به پارامترهای کنترلی در نگاشت های آشوب از جمله دلایل اصلی در انتخاب این نگاشت ها به عنوان رکن اصلی الگوریتم های رمزنگاری می باشد. در این مقاله یک الگوریتم رمزنگاری با تکیه بر نگاشت آشوب استاندارد پیشنهاد شده است. الگوریتم پیشنهادی شامل سه بخش (بلوک) مجزا میباشد: 1) بلوک در هم ریختگی، 2) بلوک انتشار، 3) بلوک تبدیل آرنولد، که هریک از این بلوک ها به ترتیب برای بهبود میزان اعوجاج و اثر بهمنی می باشد و بخش سوم به منظور مقابله با ضعف نگاشت استاندارد دو بعدی مورد استفاده قرار گرفته اند. الگوریتم پیشنهادی با نگاشت های آشوب مختلفی از جمله نگاشت تنت و لوجستیک نیز پیاده سازی شده که بررسی نتایج شبیه سازی با استفاده از نرم افزار MATLAB عملکرد مناسب نگاشت آشوب استاندارد بر حسب زمان اجرای الگوریتم، میزان اعوجاج، اثر بهمنی، آزمون بصری و هیستوگرام را نشان می دهد.

کلمات کلیدی:
رمزنگاری بلوکی، نگاشت های آشوب، نگاشت استاندارد، تبدیل آرنولد، رمزنگاری کلید متقارن