عنوان مقاله:
طراحی جعبه جایگزینی بر اساس نقشه آشوب و الگوریتم ژنتیک

محل انتشار:
همایش ملی کاربرد سیستم های هوشمند (محاسبات نرم) در علوم و صنایع (سال: 1392)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمد یعقوبی - *دانشجوی ارشد هوش مصنوعی دانشگاه امام رضا (ع)*

محمدباقر منهاج - *استاد دانشگاه امیرکبیر*

خلاصه مقاله:
جعبه جایگزینی (S-BOX)، یک جزء مهم در الگوریتم های رمز نگاری بلوکی است. در این مقاله، مسئله ساختن جعبه جایگزینی، به مسئله فروشنده دوره گرد و یک روش برای تبدیل طراحی جعبه جایگزینی مبتنی بر آشوب و الگوریتم ژنتیک ارائه شده است. از آنجا که روش پیشنهادی به طور کامل از صفات نقشه آشوب و پردازش تکاملی استفاده می کند، جعبه جایگزینی قویتری به دست آمده است. نتایج حاصل از آزمون عملکرد نشان میدهد که ارائه جعبه جایگزینی دارای خواص رمزنگاری خوبی است، که توجیه می کند الگوریتم پیشنهادی در تولید قویتر جعبه جایگزینی موثر است.

کلمات کلیدی:
آشوب، جعبه جایگزینی، الگوریتم ژنتیک