عنوان مقاله:
الگوریتم رمزنگاری تصویر مبتنی بر گروه جایگشت Sn و توابع آشوب

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 8, شماره 3 (سال: 1399)

تعداد صفحات اصل مقاله: 12

نویسنده:
ابراهیم زارعی زفره - *گروه علوم کامپیوتر، دانشگاه خوانسار، خوانسار ، ایران*

خلاصه مقاله:
در این مقاله، یک الگوریتم رمزنگاری تصویر جدید با استفاده از گروه جایگشت Sn و توابع آشوب ارائه شده است. الگوریتم پیشنهادی شامل سه مرحله می‌باشد: (۱) با اعمال توابع درهم‌ساز بر روی اطلاعات تصویر اصلی و کلید رمز خارجی ۲۵۶ بیتی، یک کلید رمز محرمانه ۲۵۶ بیتی استخراج می‌گردد که با کمک آن شرایط اولیه و پارامترهای مربوط به توابع آشوب تولید می‌شود؛ (۲) در مرحله انتشار، با انجام یک جایگشت سطری و یک جایگشت ستونی مبتنی بر توابع آشوب، موقعیت پیسکل‌ها در تصویر اصلی جابه‌جا می‌شود به‌طوری که همبستگی بین پیکسل‌های مجاور به شدت کاهش می‌یابد؛ (۳) در مرحله اغتشاش، مقدار سطح روشنایی هر پیکسل با انجام جایگشت در سطح بیت با کمک گروه جایگشت S۸ و توابع فوق آشوب تغییر می‌یابد؛ سپس با انجام تبدیل در سطح بیت به وسیله جعبه‌های جایگزینی S۸Sbox و عملگر XOR، امنیت الگوریتم پیشنهادی افزایش می‌یابد. نتایج تجربی و تحلیل‌های امنیتی نشان می‌دهد که ۶۰/۹۹% ، ۳۳%/۴۰ ، آنتروپی بزرگتر ۹۹/۷ و ضرایب همبستگی برای تصویر رمز نزدیک به صفر می‌باشد. همچنین الگوریتم رمزنگاری تصویر پیشنهادی مقاومت بالایی در برابر حملات متداول همانند حملات جستجوی کامل، برش و نویز از خود نشان می‌دهد.

کلمات کلیدی:
رمزنگاری تصویر, گروه جایگشت, توابع آشوب, جعبه جایگزینی, انتشار, اغتشاش