عنوان مقاله:
الگوریتم رمزنگاری تصاویر مبتنی بر مربع های لاتین و جادویی

محل انتشار:
هجدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1400)

تعداد صفحات اصل مقاله: 10

نویسندگان:
ابراهیم زارعی زفره - *گروه علوم کامپیوتر، دانشکده ریاضی و کامپیوتر خوانسار، دانشگاه اصفهان، اصفهان*

معصومه ابدالی - *گروه ریاضی، دانشکده ریاضی و کامپیوتر خوانسار، دانشگاه اصفهان، اصفهان*

خلاصه مقاله:
در این مقاله یک الگوریتم جدید جهت رمزنگاری تصاویر دیجیتال مبتنی بر مربع های لاتین و جادویی با ساختار «پیش پردازش- جایگشت- جانشینی» ارائه می شود. ابتدا با اعمال تابع درهم ساز بر روی اطلاعات تصویر اصلی، کلید محرمانه ۲۵۶ بیتی تولید می شود؛ سپس با استفاده از کلید محرمانه و تابع آشوب لجستیک، مربع لاتین تولید و از آن در مراحل پیش پردازش، جایگشت و جانشینی استفاده می شود. در مرحله پیش پردازش، توزیع آماری پیکسل های تصویر با جاسازی اعداد صحیح تصادفی در تصویر از طریق عمل XOR بین تصویر اصلی و مربع لاتین تغییر می کنند. در مرحله جایگشت، ابتدا با استفاده از مربع لاتین و ترانهاده ی آن، یک مربع جادویی تولید و سپس مکان پیکسل های تصویر با کمک آن تغییر می کند. در مرحله جانشینی با استفاده از مربع لاتین تولید شده، مقدار سطح روشنایی هر پیکسل تغییر می کند و تصویر رمز به دست می آید. نتایج شبیه سازی ها نشان می دهد که UACI>۳۳/۵۶%، NPCR>۹۹/۶۰%، آنتروپی بزرگتر از ۷/۹۹ و ضرایب همبستگی برای تصویر رمز نزدیک به صفر می باشد. همچنین الگوریتم رمزنگاری تصویر پیشنهادی امنیت بالایی در برابر حملات شناخته شده دارد و دارای سرعت بالایی برای کاربردهای بلادرنگ رمزنگاری است.

کلمات کلیدی:
رمزنگاری تصویر، مربع لاتین، مربع جادویی، توابع آشوب، جایگشت، جانشینی