عنوان مقاله:
طراحی الگوریتم سریع جهت رمزکردن تصاویر با استفاده از قضیه باقی مانده چینی و خم بیضوی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 5, شماره 3 (سال: 1396)

تعداد صفحات اصل مقاله: 10

نویسندگان:
غلامرضا کرمعلی - *دانشگاه علوم و فنون شهید ستاری*

عیسی کاوند - *دانشکده تحصیلات تکمیلی دانشگاه علوم و فنون هوایی شهید ستاری*

خلاصه مقاله:
ارسال و دریافت اطلاعات، به صورت محرمانه همواره از اهمیت بالایی برخوردار است. علم رمزنگاری نقش عمده ای در تبادل اطلاعات به صورت امن ایفا می کند. به همین منظور، الگوریتم های رمزنگاری متعددی طراحی و پیاده سازی شده است. از میان الگوریتم های طراحی شده، الگوریتم رمزنگاری خم بیضوی، به دلیل ویژگی های منحصر به فردش، جایگزین مناسبی برای الگوریتم های قدیمی تر از قبیل RSA و دیفی هلمن می باشد. در این مقاله، روش کارآمدی برای رمزنگاری تصویر با استفاده از خم های بیضوی ارایه خواهد شد. این طرح پیشنهادی در مقایسه با روش های فعلی دارای سرعت بالاتری در رمزنگاری و رمزگشایی تصویر است. برای این منظور، از روش گروه-بندی پیکسل های تصویر با استفاده از قضیه باقی مانده چینی، استفاده شد. روش پیشنهادی قابل اعمال بر روی سایر داده ها از قبیل متن، صدا و ویدیو می باشد.

کلمات کلیدی:
پردازش تصویر- رمزنگاری تصویر, رمزگشایی تصوی, رمز نگاری خم بیضوی, قضیه باقی مانده چینی