عنوان مقاله:
الگوریتم ترکیبی مقاوم جهت رمزنگاری کارآمد منابع آگاه برای داده های حجیم چند رسانه ای

محل انتشار:
یازدهمین کنفرانس ملی و اولین کنفرانس بین‌المللی بینایی ماشین و پردازش تصویر ایران (سال: 1398)

تعداد صفحات اصل مقاله: 6

نویسندگان:
کاظم خالقی - *کارشناسی ارشد دانشگاه آزاد اسلامی واحد گرمسار*

علی برومندنیا - *استادیار دانشگاه آزاد اسلامی واحد تهران جنو ب*

خلاصه مقاله:
احساس امنیت یکی از اساسی ترین نیازهای بشر است. با به اشتراک گذاشتن شبکه ها، امنیت تصاویر دیجیتال در فرآیند انتقال، اهمیت ویژه ای پیدا کرده و در نتیجه افراد توجه بیشتری به امنیت و محرمانه بودن اطلاعاتچندرسانه ای دارند. در این میان رمزنگاری تصویر به دلیل برخی از ویژگی های ذاتی همچون حجم بالای داده، همبستگی زیاد میان پیکسل ها و قابلیت فشرده سازی بالا با رمزنگاری متن متفاوت است. اینگونه به نظر می رسد که روش های کلاسیک رمزنگاری متن برای این منظور چندان کارآمد نیستند. در سال های اخیر الگوریتم رمزنگاری مبتنی بر آشوب، راه حل های جدیدی را برای توسعه رمزنگاری ایمن تصاویر پیشنهاد کرده است. هدف اصلی مقاله، حداقل سازی احتمال کشف رمز با ارائه یک الگوریتم رمزنگاری پیشنهادی برای محیط های چندرسانه ای با استفاده از ساختار نگاشت گربه آرنولد و الگوریتم رمز هیل می باشد. برای بررسی طرح پیشنهادی با استفاده از نرم افزار متلب آن را پیاده سازی کرده و با استفاده از آزمون های تحلیل فضای کلید، تحلیل هیستوگرام، تحلیل آنتروپی اطلاعات، تحلیل همبستگی، تحلیل تفاضلی مورد تجزیه و تحلیل قرار دادیم. نتایج بدست آمده از روش پیشنهادی، مقاومت در برابر بیشتر حملات را تایید می نماید.

کلمات کلیدی:
الگوریتم دیفی-هلمن، چندرسانه، داده های حجیم، رمزنگاری، داده های حجیم

لینک ثابت مقاله در پایگاه سیویلیکا: