عنوان مقاله:
تحلیل اتوماتای سلولی برنامه پذیر در پیاده سازی سیستم های رمزنگاری

محل انتشار:
دومین کنفرانس ملی رویکردهای نوین در مهندسی کامپیوتر و برق (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
حمیدرضا یوسفیان - *دانشگاه آزاد اسلامی، واحد نراق، گروه مهندسی کامپیوتر، نراق، ایران*

ساجد داداشی - *دانشگاه آزاد اسلامی، واحد رودسر و املش، گروه مهندسی کامپیوتر، رودسر، ایران*

خلاصه مقاله:
با توسعه روزافزون دنیای ارتباطات و لزوم محرمانگی هر چه بیشتر اطلاعات، به کارگیری سیستم های رمزنگاری امری حیاتی و بدون انکار تلقی می شود. در این میان پیاده سازی این سیستم ها به نحوی کاراتر و سریعتر یکی از چالشهای محققان علوم و فنون IT می باشد. در میان تکنیک های مختلف پیاده سازی سیستم های رمزنگاری، استفاده از ساختارهای اتوماتای سلولی یکی از بهینه ترین روش ها می باشد که تحقیقات زیادی در مورد آن انجام شده و در حال انجام می باشد. ما در این مقاله ابتدا به بیان اتوماتای سلولی پرداخته و سپس با مرور ویژگی ها و روابط ریاضی آن به تشریح اتوماتای سلولی قابل برنامه ریزی می پردازیم. در ادامه نیز با توصیف مباحثی کوتاه در زمینه سیستم های رمزنگاری به تشریح یک سیستم رمزنگاری ترکیبی پیاده سازی شده با PCA خواهیم پرداخت.

کلمات کلیدی:
اتوماتای سلولی، اتوماتای سلولی قابل برنامه ریزی، رمزنگاری کلید متقارن، رمزنگاری رشته ای، رمزنگاری بلاکی