عنوان مقاله:
طراحی روش جدید در تولید کلید رمزنگاری بیومتریک بر اساس تصویر قطعه بندی شده اثر انگشت

محل انتشار:
ماشین بینایی و پردازش تصویر, دوره 10, شماره 2 (سال: 1402)

تعداد صفحات اصل مقاله: 18

نویسندگان:
محمدرضا روزبهانی - *دانشجوی کارشناسی ارشد مهندسی برق، دانشگاه صنعتی امیرکبیر، تهران، ایران*

ساناز سیدین - *گروه مهندسی الکترونیک، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر، تهران، ایران*

بهرام رشیدی - *گروه مهندسی برق، دانشکده فنی و مهندسی،دانشگاه آیت الله بروجردی(ره)، بروجرد، ایران*

خلاصه مقاله:
هدف این مقاله استفاده از ویژگی‌های بیومتریک اثر انگشت برای دستیابی به کلیدهای رمزنگاری تصادفی می باشد. پیچیدگی الگوریتم تولید کلید، تعداد بیت بالا و تصادفی بودن سه فاکتور مهم برای کلیدهای رمزنگاری قوی می‌باشند. در روش پیشنهادی، ابتدا ویژگی‌های بیومتریک یعنی نقاط مینوشیا را با پردازش تصویر اثر انگشت استخراج می کنیم. سپس برای افزایش پیچیدگی روش تولید کلید و امنیت کلید تولیدی، هر تصویر را به ۴۴ قطعه تقسیم می‌کنیم تا با محاسبه فاصله اقلیدوسی و زاویه بین پیکسل‌های مرکزی هر ۴۴ قطعه با کل مینوشیاهای تصویر بتوانیم داده های تصادفی را افزایش دهیم. جهت افزایش بیشتر حالت تصادفی کلید، یک الگوریتم سه-گامه پیشنهاد می کنیم که شامل قرار دادن اعداد مربوط به زاویه و فاصله بصورت زوج و فرد در کنار یکدیگر، دو شکل جابجایی و جایگشت بیت ها و اعمال توزیع یکنواخت روی داده ها برای تولید کلید نهایی می باشد. به علت بالا بودن تعداد بیت کلید، می توان با استخراج زیر کلیدهای ۱۲۸، ۲۵۶ و ۵۱۲ بیتی از ماتریس کلید مذکور در رمزنگاری از آنها استفاده نمود. آنالیزهای آماری انجام شده همچون مجموعه تست های استاندارد NIST، تصادفی بودن و امنیت بالای کلید نهایی ۶۳۷۵۱ بیتی را اثبات می کند، و نشان دهنده عملکرد بهتر روش پیشنهادی در مقایسه با کارهای گذشته می باشد که تنها از فاصله یا زاویه بین نقاط مینوشیا برای تولید کلید رمزنگاری تصادفی با طول بیت یسیار کمتر استفاده کرده اند. الگوریتم پیشنهادی، با توجه به ۱۵ تست NIST، نسبت به کارهای جدید گذشته تا ۲۰% از نظر تصادفی بودن کلید تولید شده بهبود دارد.

کلمات کلیدی:
قطعه بندی تصویر اثر انگشت, کلید رمزنگاری تصادفی, مینوشیا, توزیع یکنواخت, فاصله اقلیدوسی, جایگشت