عنوان مقاله:
ارائه روشی نوین جهت رمزنگاری جویباری ونهان نگاری در داده های صوتی به صورت انتها به انتها

محل انتشار:
چهارمین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی (سال: 1399)

تعداد صفحات اصل مقاله: 10

نویسندگان:
ساراسادات بهبهانیا - *فارغ التحصیل کارشناسی ارشد دانشگاه آزاد اسلامی*

علی برومندنیا - *عضو هیئت علمی دانشگاه آزاد اسلامی واحد تهران جنوب*

خلاصه مقاله:
امروزه با رشد کاربردهای چندرسانه ای، امنیت بحث بسیار مهمی در ارتباطات و ذخیره اطلاعات چندرسانه ای شده است. رمزنگاری به عنوان یک تکنیک مناسب برای امنیت اطلاعات می باشد و رمزگذارهای جویباری یک کلاس مهمی از الگوریتم های رمزگذاری است که بطور منحصر بفرد کارکترهای یک پیغام را در یک زمان با استفاده از یک انتقال رمز در زمان های متفاوت، رمز گذاری می کند. در این پژوهش روشی برای نهان نگاری داده ها بر روی صوت و رمزنگاری جویباری برای ساخت بستری در انتقال بر خط و جلوگیری از تولید کلیدهای عظیم ارایه شده است. در این پژوهش الگوریتم بهینه سازی ژنتیک نقش کلیدی دارد زیرا اطلاعات نهان نگاره به طور مناسب با استفاده از این الگوریتم در فایل اصلی نهان نگاری می شود سپس با کلید رمز کوچک تصادفی با داده ها رمز گشته و از سویی رمزگشایی می گردد، علاوه بر فایل اصلی داده های نهان نگاری شده استخراج می گردد. همچنین در این پژوهش مقادیر PSNR که نشان دهنده نزدیکی داده های قبل نهان نگاری و بعد از استخراج است، محاسبه شد که نتیجه مطلوبی را نشان داد. در بخشی نرخ خطا بیتها با توجه به رمزنگاری و رمزگشایی انجام شد که میزان خطای مناسبی در روش پیشنهادی به ثبت رساند. در مورد مقایسه روش پیشنهادی با روش های می توان گفت که مقادیر SNR، میزان نرخ خطا در بیت و کیفیت فشرده سازی که بر سه جنبه شفافیت، مقاومت و ظرفیت روش ترکیبی ارایه شده دلالت دارد، روش پیشنهادی نتایج مطلوبی از خود نشان داد.

کلمات کلیدی:
داده، صوت، امنیت، رمزنگاری جویباری، رمزگشایی، نهان نگاری، الگوریتم ژنتیک.

لینک ثابت مقاله در پایگاه سیویلیکا: