پایان‌نامه‌ی کارشناسی ارشد: هادی ملکی، ۱۳۹۶

بهبود و آنالیز الگوریتم های پنهان نگاری LSBوDCM در تصاویر دیجیتال و طبقه بندی این تصاویر توسط شبکه عصبی MLP

چکیده :

با توجه به افزایش سرعت در پردازنده‌های جدید و استفاده از این پردازنده‌ها از یک طرف و از طرف دیگر پیشرفت چشم‌گیر در الگوریتم‌های جدید مانند پردازش موازی و رایانش ابری و همچنین توسعه‌ی الگوریتم‌های هوش مصنوعی مانند شبکه‌های عصبی فرایند پنهان نگاری اطلاعات با کاهش احتمال تشخیص بسادگی میسر نخواهد بود. همچنین افزایش پهنای باند و سرعت ارسال اطلاعات در کاربردهای نوین امکان ارسال اطلاعات با حجم بیشتر به آسانی در تکنولوژی‌های جدید فراهم گردیده است.

در پنهان نگاری تصویر، سیگنال پنهان نگاری شده در حوزه مکانی یا یکی از حوزه¬های فرکانسی مثل تبدیل کسینوس گسسته، فوریه، و موجک و ... می-تواند پنهان شود. تکنیک¬های پنهان نگاری درحوزه تبدیل، مقاومت بیشتری در مقابل حملات گوناگون در مقایسه با تکنیک¬های حوزه مکان از خود نشان می¬دهند، چون وقتی از تصویری تبدیل معکوس گرفته می¬شود، تصویر مخفی به طور بی¬قاعد¬ه¬ای در طول تصویر پخش می¬شود، بنابراین خواندن و اصلاح آن برای نفوذگرها بسیار مشکل خواهد شد.

الگوریتم های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر ارائه شده است. به طور کلی روش های پنهان نگاری در تصویر از الگوریتم جاسازی بیت ها و الگوریتم استخراج تشکیل شده اند. برخی روش های رایج در استگانوگرافی فایلهای تصویری عبارتند از :

جایگزینی بیت کمترین ارزش (LSB)، همبستگی بر پایه آستانه، همبستگی بر پایه مقایسه، روش طیف گسترده

مقایسه ضریب باند متوسط، طیف گسترده در دامنه موجک DCT، با توجه به کارهای گذشته ای که در این زمینه انجام شده است، در این تحقیق قصد داریم تا الگوریتم های پنهان نگاری LSBو DCM در تصاویر دیجیتالی را بررسی و توسعه دهیم. برای این منظور از روش های پنهان نگاری که شامل تبدیل موجک گسسته می باشد استفاده خواهیم کرد.و برای طبقه بندی این تصاویر از شبکه عصبی MLP استفاده خواهیم کرد.

چکیده :

با توجه به افزایش سرعت در پردازنده‌های جدید و استفاده از این پردازنده‌ها از یک طرف و از طرف دیگر پیشرفت چشم‌گیر در الگوریتم‌های جدید مانند پردازش موازی و رایانش ابری و همچنین توسعه‌ی الگوریتم‌های هوش مصنوعی مانند شبکه‌های عصبی فرایند پنهان نگاری اطلاعات با کاهش احتمال تشخیص بسادگی میسر نخواهد بود. همچنین افزایش پهنای باند و سرعت ارسال اطلاعات در کاربردهای نوین امکان ارسال اطلاعات با حجم بیشتر به آسانی در تکنولوژی‌های جدید فراهم گردیده است.

در پنهان نگاری تصویر، سیگنال پنهان نگاری شده در حوزه مکانی یا یکی از حوزه¬های فرکانسی مثل

تبدیل کسینوس گسسته، فوریه، و موجک و ... می-تواند پنهان شود. تکنیک¬های پنهان نگاری درحوزه تبدیل، مقاومت بیشتری در مقابل حملات گوناگون در مقایسه با تکنیک¬های حوزه مکان از خود نشان می¬دهند، چون وقتی از تصویری تبدیل معکوس گرفته می¬شود، تصویر مخفی به طور بی¬قاعد¬ه¬ای در طول تصویر پخش می¬شود، بنابراین خواندن و اصلاح آن برای نفوذگرها بسیار مشکل خواهد شد.
الگوریتم های پنهان نگاری متعددی برای ساختارهای مختلف تصاویر ارائه شده است. به طور کلی روش های پنهان نگاری در تصویر از الگوریتم جاسازی بیت ها و الگوریتم استخراج تشکیل شده اند. برخی روش های رایج در استگانوگرافی فایلهای تصویری عبارتند از :
جایگزینی بیت کمترین ارزش (LSB)، همبستگی بر پایه آستانه، همبستگی بر پایه مقایسه، روش طیف گسترده
مقایسه ضریب باند متوسط، طیف گسترده در دامنه موجک DCT، با توجه به کارهای گذشته ای که در این زمینه انجام شده است، در این تحقیق قصد داریم تا الگوریتم های پنهان نگاری LSBو DCM در تصاویر دیجیتالی را بررسی و توسعه دهیم. برای این منظور از روش های پنهان نگاری که شامل تبدیل موجک گسسته می باشد استفاده خواهیم کرد.و برای طبقه بندی این تصاویر از شبکه عصبی MLP استفاده خواهیم کرد.

شماره‌ی پایان‌نامه: ۱۲۷۴۰۱۰۱۹۵۲۰۰۴
تاریخ دفاع: ۱۳۹۶/۱۱/۰۹
رشته‌ی تحصیلی: مهندسی برق - الکترونیک
دانشکده: فنی و مهندسی
استاد راهنما: مهندس علی پاکیزه‌مقدم

M.A. Thesis:

Investigation and improvement of LSB and DCM Steganography algorithms in digital images and classification using MLP neural network

Abstract:

Due to the increasing speed of the new processors and the use of these processors on the one hand, and on the other hand, significant advances in new algorithms such as parallel processing and cloud computing, as well as the development of artificial intelligence algorithms, such as neural networks, information steganography process, with reduced probability of simple diagnosis will not be. Also, increasing the bandwidth and the speed of sending information in new applications. The ability to send more volume information is easily provided in new technologies.

In the image hiding, a signal hidden in a spatial domain or one of the frequency domains, such as the discrete cosine transform, Fourier, and wavelet, can be hidden. Concealment techniques in the area of conversion show a greater resistance to various attacks than those in the area of the field, because when the image is converted inversely, the secret image is unbiased. It will be distributed throughout the image, so it will be very difficult to read and modify it for the attackers Several cryptographic algorithms are provided for different image structures. In general, image cryptographic methods are embedded in bitmap algorithms and extraction algorithms. Some of the common ways in steganography image files are:
Substitution of the least value bit (LSB), threshold correlation, correlation based on comparison, wide spectrum method Comparing Medium Bandwidth, Wide Range in the Dynamic Duct Waveform Domain, In light of past work done in this field, we intend to explore and develop LSB and DCM steganography algorithms in digital images. For this purpose, we will use cryptographic methods that include discrete wavelet transformations, and we will use the MLP neural network to classify these images.