الخلاصة

تزودنا الشبكة العالمية بمدى واسع من الاتصالات كوسيلة لانتشار المعلومات في العالم. تشكل هذه المعلومات وسيلة للافضاء بالافكار بين الناس وتشمل هذه المعلومات النص والصورة والصوت.

مع تطور تقنيات الاتصالات ونمو شبكة المعلومات العالمية اصبح العالم بين يدي اي شخص بمجرد الضغط على بعض الازرار في لوحة المفاتيح. وبما اننا جزء من هذه الشبكة فيجدر بنا ان نأخذ بنظر الاعتبار احتمال ان تكون معلوماتنا مراقبة او تعرضت للتغيير او السرقة . ومن هنا تبرز الحاجة الماسة لاستخدام انظمة معينة لحماية المعلومات من التغيير. وبصورة عامة هنالك تقنيتين يمكن ان تستخدم لحماية المعلومات؛ الاولى تسمى التشفير او الكتابة السرية (*Cryptography*) وهذه الطريقة تقوم بتشفير المعلومات بطريقة ما بحيث تصبح غير مفهومة للجميع عدا الشخص المرسلة اليه المعلومات، اما الطريقة الثانية فتعرف بالاخفاء او الكتابة المخفية (*Steganography*) وفيها يتم اخفاء المعلومات داخل معلومات اخرى (غطاء) مع الانتباه الى عدم حدوث تشويه في الغطاء، وبذلك فان حقيقة وجود معلومات سرية مرسلة تصبح سرا ايضا.

في هذه الاطروحة تم اقتراح نظام اخفاء يقوم باخفاء اربعة صور بحجم (١٢٨ × ١٢٨) ذات مستوى ٢٥٦ مستوى من التدرج الرصاصي داخل صورة بحجم (٥١٢×٥١٢) ذات ٢٥٦ مستوى من التدرج الرصاصي بأستخدام تقنيتين؛ الاولى هي تقنية تحويل المويجة (*Wavelet Transform*) والثانية تقنية تحويل متعدد المويجات (*Multiwavelet Transform*). وفي كلا الطريقتين تم استخدام تقنيتي التشفير بأبدال المواقع(*Transposition Encryption*) والتشفير الانسيابي (*Stream Ciphering*) لزيادة درجة امنية وتعقيد النظام.

اعتماداً على نتائج الحسابات ومن خلال النظر الى الصور، يعتبر النظام المقترح مقبول حيث ان الصور النهائية والتي تحتوي على المعلومات تشبه بشكل كبير الصور الاصلية بحيث يمكن ارسالها دون اثارة اية شكوك حول وجود معلومات سرية، وهذا هو هدف نظام اخفاء المعلومات.

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number of even help to prevent unauthorized direct copying.

Military communication systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver of its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving field can trace their history back to antiquity; and many of them are surprisingly easy to circumvent.

This Thesis speaks of a secret-key steganographic system which embeds four gray-scale secret images of size (128×128) pixels into a cover image of size (512×512) pixels. The techniques used in this project to analyze the cover into its frequency components are wavelet transform using Haar Filter as a basis function and the new approach multiwavelet transform using GHM filter as a basis function. Multiwavelet transform can be considered as a development of the scalar wavelet transform since it gives best results in many applications like compression and denoising. This new approach (multiwavelet transform) offers a combination of orthogonality, symmetry and compact support, which can not be achieved by any scalar wavelet basis.

PDF created with pdfFactory trial version www.pdffactory.com