الخلاصة

لكتابة المغطاة هي علم اخفاء وجود بيانات سرية منقولة عبر قنوات الاتصال من خلال طمر بيانات الرسالة السرية داخل الوسط الناقل كالصورة الرقمية ان اكتشاف الكتابة السرية او تخمين حجم هذه البيانات اواستخراج هذه البيانات اوتدميرها او مسحها نهائي كل هذه العمليات تتبع علم تحليل البيانات المخفية .علم تحليل البيانات المخفية يحظى مؤخرا بقدر كبير من الاهتمام سواء من الجهات الرسمية ذات السلطة القانونية او من الاوساط غير الرسمية كالمؤسسات العلمية والجامعات. عدد كبير من برامج الاخفاء التجارية تستخدم طمر البيانات في البت الادنى من الصورة كخيار لطريقة اخفاء البيانات في الصور الملونة و الرمادية بسبب ما هو شائع من ان التغيير في الوان الصورة الناتج عن التغيير في البت الادنى لها هو تغيير غير محسوس استنادا لما يطرأ عادة على الصور الرقمية من التشويش في هذا البحث تم تقديم طريقة دقيقة لاكتشاف الاخفاء العشوائي في البت الادنى من الصور غير المضغوطة الطريقة المقترحة تبتنى على اساس تحليل سعة اخفاء البيانات في البت الادنى بدون تشويه في الصورة. ان عشوائية البت الادنى تقلل من سعة اخفاء البيانات في البت الادنى من غير تشويه في الصورة بينما تمتلك تأثير مختلف على سعة الاخفاء التي لا تتقيد بموقع بت معين لذا اصبحت سعة الاخفاء بدون تشويه مقياس حساس لدرجة عشوائية البت الادنى (الاخفاء في البت الادنى مثلا) . مفتاح نجاح الطريقة المقترحة يستند الى عملية تشكيل مجموعات ثانوية من وحدات الصورة والتي تتغير بشكل طبيعي مع وجود الاخفاء في البت الادنى وهذا التغيير يمكن ان يقاس بدقة . وتشكل هذه المجاميع الثانوية على اساس حالتها والتي تحدد من خلال استخدام كل من (عملية تبادل مستويات الالوان) و(دالة مميزة) عملية تبادل الالوان تحاكي عملية اضافة قدر ضئيل من التشويش القابل للعكس كما ان الدالة المميزة تقيس تأثير عملية تبادل الالوان على انتظامية المجموعة الخاضعة لعملية التبادل في مستويات الالوان. النظام المقترح تم تنفيذه على حاسبة من نوع بنتيوم 3 ذات معالج سرعته 1.2 GHz واستخدمت بيئة windows 2000 كنظام تشغيل وتم كتابة النظام بلغة Delphi 6 . تم اختبار عدد من النماذج لاثبات دقة النظام المقترح.

PDF created with pdfFactory trial version www.pdffactory.com

ABSTRACT

Steganography is the art of hiding the very presence of communication by embedding secret message into innocuous looking cover documents, such as digital images. Detection of Steganography, estimation of message length, and its extraction belong to the field of Steganalysis.

Steganalysis has recently received a great deal of attention both from law enforcement and the media. Large number of commercial Steganographic programs use the least significant bit (LSB) embedding as the method of choice for message hiding in 24-bit, 8-bit color images, and grayscale images. It is commonly believed that changes to the LSB of colors cannot be detected due to noise that is always present in digital images.

In this research, an accurate method that can detect LSB embedding randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images and estimate a secret message length is proposed. This method originated by analyzing the capacity for lossless (distortion-free) data embedding in the LSBs. Randomizing the LSBs decreases the lossless capacity in the LSB plane, but it has a different influence on the capacity for embedding that isn't constrained to one bit plane. Thus, the lossless capacity has become a sensitive measure for the degree of randomization of the LSB plane. A software system was developed throughout this work based on the proposed method using Delphi 6 programming language. The key to the success of the proposed method is the formation of sub-sets of pixels whose cardinalities change at the presence of LSB embedding, and such changes can be precisely

PDF created with pdfFactory trial version www.pdffactory.com

quantified. The sub-sets of pixels or groups of pixels are obtained according to their status. The status can be obtained using a flipping operation (a permutation of grayscales) and a discrimination function. The flipping simulates an "invertible noise adding", while the discrimination function measures how the flipping influences the smoothness of the flipped group.

The proposed system was executed on a Personal Computer of type Pentium III with CPU Speed of 1.2GHz under Microsoft Windows 2000 as operating system. Various practical examples were tested to prove the accuracy of the proposed method.

PDF created with pdfFactory trial version www.pdffactory.com