الخلاصة:

من المتعارف عليه إن عملية إخفاء نص في صورة يتم باستخدام (ASCII) المقابل لكل حرف في النص المراد إخفاءه كقيمة يتم إخفاءها وكافة الدراسات في هذا المجال تعتمد على هذا المبدأ .

هذه الدراسة تعاملت مع النص على أساس كونه صورة وليس مجموعة من الحروف وبالتالي فان عملية الإخفاء أصبحت تعتمد على إخفاء صورة في صورة ولكي لا تكون العملية خالية من التعقيدات التي تعرقل عمل المهاجم فان صورة النص تم تحويلها الى مجموعة من الأرقام أو القيم لتكن كل قيمتين متجاورتين تمثل الاولى فيها عدد مرات تكرار القيمة الثانية . وتم معاملة هذه القيم على أساس إنها تمثل قيم لونية من خلال خزنها في ملف من نوع BMP . فيتولد لدينا صورة عشوائية ملونة حجمها اكبر من حجم الرسالة السرية . وذلك كمرحلة أولى من مراحل تعقيد العمل .

اعتمدت طريقة إخفاء الصورة في الصورة على إخفاء كامل الصورة السرية في الغطاء (المعلومات الرأسية للملف ، فهرست الألوان ، بيانات الصورة) وذلك بتقسيمها إلى مجموعة من القيم تخفى في مقاطع داخل الغطاء (ملف صورة) ويشار إلى موقع هذه القيم في بداية كل مقطع باستخدام طريقة (LSB) أي تم استخدامها كوسيلة لتشفير موقع البيانات المخفية وليس كأداة للإخفاء كما هو متبع عادة وكذلك تم إخفاء المفاتيح التي ستساعد على عملية فصل البيانات السرية لاحقاً (Public Key ، Secret Key) داخل الغطاء بطريقة تزيد من الصعوبة بكشف مواقعها .

إن التقييم الذي اجري للعمل من خلال دراسة الفرق في مواصفات الصورة الأصلية والصورة ذات المعلومات المخفية اظهر عدم وجود اختلاف كبير حيث إن الفارق الضئيل ممكن أن يعزى إلى وجود ضوضاء أثناء النقل نظراً لقلته كذلك فإن حساب السرية والتشابه اظهر نتائج مشجعة وطيبة جداً .

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

It's known that hiding a text in image is done by using (ASCII) code against each text as a value for hiding and all studies in this field depend on this principle.

This study deals with text as being an image no a group of letters, as a result hiding operation depends on hiding image within image. In order for the operation not to be free from complications, In order to have obstacles in the way of the attacker act, the image of the text is turned to a group of numbers and values to represent each parallel values. The first represents number of second value frequency. This value is treated on a base, which represents color value through store in BMP value. Consequentially one has arbitrary colored image much bigger than the secret letter as a first stage of complexity operation.

Hiding image within image is hiding complete secret image in the cover (image data, files information and colors index) by dividing it to a group of values hidden in sections inside the cover (image file). The position of these values is indicated in the beginning of each section by using a method of (LSB) i.e. as a method to encode hidden data position, not as a tool for hiding. A key that helps to crypt secret text operation is hidden in the cover in a way which makes it is not discovered.

Evaluation performed on the work by studying the differences in original image and efficient hidden data image illustrates no great difference. The little difference is due to noises through transformation because they are too little. The calculation of secrecy and similarity reveals good results.

PDF created with pdfFactory trial version www.pdffactory.com