جامعة الموصل

كلية علوم الحاسوب والرياضيات

استخدام الكبس والتشفير لتوفير إخفاء آمن للصورة

رسالة تقدم بها

يوسف صبحي يوسف حسين

رسالة الدبلوم العالي في

علـــوم الحاسوب

إشراف

د. ياسين حكمت إسماعيل

استاذ مساعد

1442هـ 2021 م

نظراً للتطور الهائل الذي شهدته شبكات الاتصالات والنمو المتزايد لتطبيقات الوسائط المتعددة وكثرة تبادلها عبر تلك الشبكات ظهرت حاجة كبيرة لتوفير طرائق كفوءة لتحقيق تلك المعلومات المتبادلة. استعمل الباحثون في البدء أنظمة التشفير المختلفة لتوفير الحماية للبيانات؛ ولكن رؤية البيانات بصيغتها المشفرة تثير الشك لدى المهاجم أو المتطفل في وجود بيانات مهمة وحساسة قد تم تشفيرها؛ ولهذا يقدم على استخدام أساليب مختلفة من أجل كسر الشفرة ومحاولة معرفة محتواها. هنا ظهرت تقنيات إخفاء المعلومات دالة تعمل على ضم البيانات السرية داخل وسط ناقل وبالتالي لن يلاحظ المهاجم وجود تلك البيانات. في هذا البحث تم استخدام أسلوب جديد يعتمد على دمج مفاهيم الكبس والتشفير والإخفاء لتحقيق مستوى عالٍ من الأمنية للبيانات المتبادلة عبر شبكة الاتصال، وتضمنت الطريقة المقترحة استخدام طريقة الكبس بدون فقدان على الصورة السرية ومن ثم إجراء عملية التشفير بالاعتماد على الدالة الفوضوية التي توفر عشوائية كبيرة. بعد ذلك يتم إخفاء الصورة الناتجة من عملية التشفير باستخدام تقنية الإخفاء في البتات الأقل أهمية (Least)(LSB Significant Bit). لا تحتاج الطريقة المقترحة لتبادل المفاتيح بين جهتين إذ اعتمدت على أسم ملف الصورة لأرسال المفاتيح المستخدمة في عملية التشفير، وبالتالي وفرت الطريقة المقترحة مستوى عالياً من الأمنية، وتم تقييم كفاءة الطريقة المقترحة باستخدام مقياس نسبة الإشارة إلى الضوضاء (PSNR) ومقياس متوسط الخطأ التربيعي (MSE) وكذلك مقياس مؤشر التشابه الهيكلي (SSIM)، لبيان كفاءة عملية التشفير والإخفاء وكذلك استرجاع الصورة المخفية عند الجهة المستلمة، وتبين من هذه المقاييس أن الصورة الاصلية (السرية) عند جهة المرسل هي مطابقة للصورة الناتجة في جهة المستلم وكانت النتائج هي (MSE=0,PSNR=0,SSIM=1).

University of Mosul
College of Computers Sciences And Mathematics

Using Compression and Encryption to Provide Secure Image Steganography

A Thesis Submitted By

Yousif Subhi Yousif Husen

D.Sc./Thesis

Computer Science

Supervised By

Dr. Yaseen Hikmat Ismail
Prof.Assist

2021 A.D 1442 A.H

Due of the tremendous development it has witnessed by communication networks and the growing growth of multimedia applications and their frequent exchange across these networks have shown a great need to provide effective ways to achieve this mutual information. In the beginning, the researchers used different encryption systems to provide protection for the data, but seeing the data in its encrypted form raises the suspicion of the attacker or the intruder that important and sensitive data has been encrypted, so it is presented using different methods in order to break the code and try to know its content. Here, steganography techniques have emerged that work on secret data systems inside a carrier, so the attacker will not notice the existence of that data. In this paper, a new method based on integrating the concepts of compression, encryption and concealment was used to achieve a high level of security for the data exchanged over the network. The proposed method included using the lossless compression method on the secret image and then performing the encryption process based on the chaotic function that provides great randomness. Then, the image generated by the encryption process is Steganography technique using in the Least Significant Bit (LSB).The proposed method does not need to exchange keys between the two sides, as it relied on the image file name to send the keys used in the encryption process, and thus the proposed method provided a high level of security. The efficiency of the proposed method was evaluated using the most important Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index measure (SSIM), to show the efficiency of the encryption and masking process, as well as the retrieval of the hidden image at the receiving party. And it was found from these standards that the original (secret) image at the sender's side is identical to the resulting image on the recipient's side, and the results were (MSE=0, PSNR=0, SSIM=1).