جامعة الموصل

كلية علوم الحاسوب والرياضيات

تنفيذ طرائق جديدة باستخدام التشفير المرئي

منى محمود خضر الخياط

دبلوم عالي

علوم الحاسوب

باشراف

الدكتور ياسين حكمت اسماعيل

مدرس

١٤٣٩هـ **٢٠١٨م**

المستخلص :

تتيح شبكات الحاسوب الحديثة توزيع الوثائق الالكترونية اقتصادياً وبسرعة عالية , ويعود ذلك إلى انخفاض تكلفة المعدات اللازمة لنسخ المعلومات وطباعتها ومعالجتها , وتواكب خاصية توزيع الوثائق الالكترونية واسعة الانتشار التركيز على أَمنية البيانات . ومن الأَساليب المستخدمة في الحفاظ على أَمنية البيانات هو التشفير المرئيّ , الذي يستخدم لتأمين البيانات الصورية مثل معلومات بطاقة الائتمان , والمعلومات الصحية الشخصية والخرائط العسكرية , ومعلومات تحديد الهوية الشخصية , والبيانات التعريفية التجارية .

يسمح لنا التشفير المرئي بتبادل المعلومات بفعالية وكفاءة وأمنية عالية ,إذ يتم توزيع الصورة السرية الى اثنين أو أكثر من الأسهم , ويتم استعادة الصورة الاصلية عن طريق تكديس الأسهم وباستخدام نظام الانسان المرئي من دون مساعدة الكمبيوتر او من دون القيام بعمليات حسابية معقدة .

يهدف هذا البحث الى تقديم طرائق مقترحة جديدة تحاول التغلب على بعض المشاكل التي ظهرت في الدراسات السابقة (التباين , توسيع البكسل , زوايا الدوران ... الخ) , مع الحفاظ على الخاصية الأهم في التشفير المرئيّ وهي قلّة وسهولة العمليات الحسابية المستخدمة في عملية التشفير, وفكّ الشفرة فضلاً عن الأمنية العالية المطلوب توافرها في التشفير.

في الطريقة المقترحة الاولى تم توزيع صفوف الصورة الثنائية الى اعمدة في اسهم , عدد الاسهم وعدد الصفوف المستخدمة في كل مرة تعتمد على المفتاح المستخدم في التشفير والمكون عشوائياً من ارقام وحروف . بينما في الطريقة المقترحة الثانية تم توزيع بكسلات الصورة الثنائية الى اسهم بعد اجراء عملية xor المنطقية على قيمة البت$(n-1)$ للصورة السرية , حيث يمثل n طول المفتاح , عدد الاسهم وعدد البكسلات الموزعة في كل مرة يساوي طول المفتاح .

الطريقة المقترحة الثالثة تمثلت باستخدام صورة ملونة لتشفيرها وصورة اخرى ملونة كمفتاح يحول الى رمادي ويُكرر بحجم الصورة السرية , اجراء عمليات تدوير وتبديل على الطبقات الثلاث ثم استخدام Xor المنطقية بين الطبقات , تم استحصال ٤ اسهم بعد تقسيم الصورة المشفرة الناتجة الى ٤ أسهم.

Mosul University

Collage of Computer Science & Mathematics

Implementation of New Methods Using Visual Cryptography

Muna Mahmood Khether Alkhayat

Higher Diploma Science

Computer science

Supervisor:

Dr. Yasseen Hikmat Ismaiel

Lecture

2018 A.D. **١٤٣٩ A.H.**

Abstract :

Modern computer networks make it possible to distribute documents quickly and economically, This is because of the decreasing cost of the equipment needed to copy, print, process the information. The widespread adoption of electronic distribution of material is accompanied with more emphasis on data security. One of the modern data security methods is Visual Cryptography. Visual Cryptography (VC) is the technique that is used for securing data specially image-based secrets such as credit card information, personal health information, military maps and personally identifiable information and commercial identification data .

Visual Cryptography allow us to share secret effectively and efficiently, the secret image can be distributed in to two or more shares, when shares are superimposed exactly together the original image would be discovered with human visual system (HVS) without out aid of computer or without performing complicated computations.

This research aims to present new proposed methods that try to solve some problems that have emerged in previous studies (variance, pixel expansion, angles of rotation... etc.), While preserving the most important feature of visual encryption is the few and simplicity of calculations used in the process of encryption and decryption. In addition to the high security required for encryption.

In the first proposed method, the rows of the binary image were distributed to columns in the shares, the number of shares and the number of rows used each time dependent on the length of the key used in the cryptography and randomly composed of numbers and letters. While in the second proposed method, the binary image pixels were distributed to shares after applying the logical Xor operation on the bit value $(n-1)$ of the secret image , where n represents the key length, the number of shares and the number of pixels distributed each time equal to the length of the key.

The third suggested method was to use a color image to encode it and another color image as a key , converting key to gray and repeat the key size to

equal the image size , rotate and switch operations on the three layers and then use logical Xor between the layers and key , 4 shares were obtained after dividing the resulting coded image to 4 shares .