مجلـــــة السعيد للعلـــــوم الإنســـانيـــة والتطبيقية
Al - Saeed Journal of Humanities and Applied Sciences
journal@alsaeeduni.net
Vol (5), No(3), September, 2022 المجلد(5)، العدد(3)، 2022م
ISSN: 2616 – 6305 (Print) ISSN: 2790-7554 (Online)

تشفير وإخفاء البيانات داخل الصور اعتماداً على واحد Bit

الباحث/ أديب اسماعيل حزام سنان
مساعد مدرس
Senanty2010@gmail.com

إشراف
أ.د/ محمد عبد اللة الهاجري
استاذ مشارك
hajry@ou.edu.sa

نشر ملخص رسالة ماجستير في نظم المعلومات منحت من الأكاديمية العربية للعلوم المالية والمصرفية قسم نظم المعلومات فرع صنعاء

تاريخ تسليم البحث 2022/8/5م تاريخ قبوله للنشر2022/9/12م

https://alsaeeduni.net/colleges/research-and-strategic/2017-03-10-08-03-59

تشفير وإخفاء البيانات داخل الصور اعتماداً على واحد Bit

الباحث/ أديب اسماعيل حزام سنان
مساعد مدرس

إشراف
أ.د/ محمد عبد اللة الهاجري
استاذ مشارك

ملخص البحث:

يسمي هذا العصر بعصر الاتصالات وثورة تقنية المعلومات ومن أهم الأشياء التي يحسب لها الكثير من الحسابات هي حماية هذه المعلومات وتوفير شبكة اتصال أمنة لنقل المعلومات، وفي وقت أصبحت المعلومات سلعة تباع وتشترى، فكلما زادت أهمية المعلومات كلما ارتفع ثمنها. فكانت الحاجة تتزايد لإيجاد وسيلة لتوفر الحماية لهذه المعلومات.

فعلم التشفير أو إخفاء المعلومات لم يكن وليد الحاضر، بل لقد استخدم منذ قرون عدة، وكان يطلق علية بالتشفير أو الإخفاء، أي أنهُ لم يكن هناك فرق بينهما وكأنه مفهوم واحد، أما اليوم فقد تطور هذا العلم وتوسع حتى أنه صنف وُقسم ووضع له طرق ووسائل، فقد أصبح التشفير مجال بحد ذاته وكذلك الإخفاء وأصبحت تطبيقاته واسعة في مجالات التجارة الإلكترونية والطب والمجال العسكري وغيرها من العلوم.

الكلمات المفتاحية: علم الاخفاء–علم التشفير–طرق الاظهار للنص– طرق فك التشفير– تقنية واحد بيت.

Encrypt and hide data inside an image depending on one bit

Research\ Adeeb Esmail Senan
Teacher Assistant

Supervisor
Dr. Mohammed Abdullah Alhagery
Associate Professor

Abstract:

This era is called the era of communications and the revolution of information technology. One of the most important things for which many accounts are counted is the protection of this information and the provision of a secure communication network for the transmission of information. At a time when information has become a commodity to be bought and sold, the more important the information, the higher its price. There was an increasing need to find a way to provide protection for this information.

The science of cryptography or hiding information was not a product of the present. Rather, it has been used for several centuries, and it was called encryption or concealment, meaning that there was no difference between them as if it were one concept, but today this science has developed and expanded until it was classified and divided and put ways and means for it. Cryptography has become a field in itself, as well as concealment, and its applications have become extensive in the fields of e-commerce, medicine, the military field and other sciences.

Key words: Cryptography Science-Stenography Science-Methods of showing-Methods of Decryption- One bit Technique

مشكلة البحث:

نظراً للتطور السريع في قطاع الاتصالات الإلكترونية وما تبعه من تطور في المعدات جعل العالم كقرية صغيرة وأصبح الاعتماد بشكل رئيسي على الإنترنت في تبادل المعلومات وأصبح البريد الإلكتروني من أهم الوسائل وأسرعها لتبادل الرسائل وأقلها كلفة ولكن عندما يقوم المرسل بإرسال رسالة يتم خزنها في حافظة الحاسوب وتذهب الرسالة إلى محطة طرفية عبارة عن الخادم الذي يقدم خدمة البريد الإلكتروني حتى يقوم الشخص المعني باستلام الرسالة حيث أن الرسالة لا تستغرق سوى ثواني للوصول إلى هذه الفوائد الكثيرة قد يكون لها بعض الثمن هو السرية أو خصوصية الرسالة حيث أنه يمكن أن تتعرض الرسالة لبعض المخاطر الأمنية سواء عند الإرسال أو عندما تكون الرسالة مخزنة داخل السير فر (Server) الذي يقدم خدمة البريد الإلكتروني وقد يكون ذلك غير مقبول للرسائل الحساسة التي تحتوي على نوع من السرية بحيث يراد للمخولين فقط بقراءتها. ومن هنا يأتي السؤال هل يمكننا حماية الرسائل المهمة من أن يتم الاطلاع عليها؟ ومن جهة أخرى قد يقول البعض أنه لا يحتاج إلى إرسال المعلومات المهمة أو السرية لأي جهة بل يريد الاحتفاظ بها في جهاز وبرغم من أنه يمكن أن يحتاط بوضع الجهاز في غرفة آمنة ويمكن أن يضع كلمة مرور للجهاز أو يقوم باستخدام التقنيات المتوفرة من محررات نصوص كال_ MS Word مثلاً ويقوم بحماية الملف بواسطة كلمة مرور وبالتالي هو يعرض نفسه للمخاطر حيث يوحي للآخرين أن هناك شيء مهم يريد إخفائه وقد لا تصمد هذه الاحتياطيات أو تدوم فنحن نعلم أن هناك برامج لكسر كلمة السر سواء لبرنامج ال_ MS Word مثل برنامج Advanced Office XP Password Recovery أو أي من البرامج الشهيرة التي تحمي ملفاتها بواسطة كلمات السر لهذا تتولد الحاجة لنظام يقوم بتحويل الملف أو الرسالة النصية لكلام غير مفهوم لا يثير الاهتمام ثم إخفاءه داخل حامل رقمي ويقوم بتعزيز أمنية النظام.

ومن المشكلات أيضًا التنافس بين المنظمات المختلفة للسيطرة على هذا المضمار مما جعل العديد من النظم تقع فريسة لمحللي الشفرات والإخفاء وبأساليب مختلفة وبأسعار تصل إلى عشرات الملايين من الدولارات من أجل كسر شفرة نظام واحد.

ومن هنا تستدعي الحاجة لوجود نظام (Stego)، معقد وقوي بحيث يمكن أن يتخطى العديد من المحاولات لكسره.

ومن المشكلات أيضًا وجود العديد من البرامج الخدمية التي تقوم بتشفير البيانات من قبل شركات عملاقة الكثير منها أمريكية وفي الحقيقة فإن القانون الأمريكي يحظر تصدير برنامج بقوة تشفير تزيد عن Bit 40 ولكن لما يتم تصدير هذه البرامج ويمكن استخراج

المعلومات من الصورة إذا شك في أنها تخفي نص بمعرفة أن النص مرمز تزيد من تأكيد بأن النص ذا أهميه كبيرة ولذلك لأن النص مشفر ومخفي.

وفي الحقيقة فإن هذه البرامج تخضع لسيطرة المخابرات بهدف السيطرة على المعلومات وتجري بعض الأمور خلف الكواليس كتعديل البرنامج بحيث يحوي بعض المعلومات في الرسالة المشفرة التي تساعد على فكها أو تكون الخوارزمية معدلة لغرض فكها من قبل هذه الجهات وحتى في الدول الأخرى فإن الوضع لن يكون أفضل وبالتالي فإن برامج التشفير المستوردة تعاني من نقصان في الموثوقية لذلك تم دمج خوارزميات الإخفاء مع خوارزميات التشفير لزيادة في الأمنية.

أهداف البحث:

يهدف هذا البحث إلى إدخال بيانات داخل صورة بعد تشفيرها ومن خلال هذا الهدف العام ممكن أن يفصل الأهداف الفرعية التالية:

- دمج (6) من الخوارزميات في التشفير والإخفاء لزيادة في الأمنية في إرسال رسائل سرية
- عمل برنامج لحماية للمعلومات بدمج وسيلة الإخفاء ووسيلة التشفير.
- إضافة (كلمة السر) لعملية الإخفاء والإظهار والتشفير لصعوبة من استخراج البيانات في الصورة.
- الزيادة من القدرة على عدم استخراج النص من الصورة وذلك بوضع نص غير مفهوم في الصور بعد تشفيره وترميزها في الصورة.
- يعتبر هذا البحث نقطة للوصول إلى الاستفادة القصوى من هذه العلوم في مجال الأعمال والتجارة الالكترونية والبنوك والطب وغيرها من المجالات.
- تطوير طرق وأدوات تكون أكثر كفاءة وموثوقية لدي المستخدم.

فرضيه البحث:

وتتمثل فرضية البحث بالإجابة عن السؤال التالي:

ما هي الطريقة المثلي لاستفادة من تقنية علم الإخفاء في الحاسبات الحديثة في تسيير أنظمة سرية في إرسال البيانات من المرسل إلى المستقبل في الحامل الرقمي ضمن الصور؟ وما مقدار المساحة المستغلة في الصور؟ وذلك من خلال استنتاجات البحث.

الادوات المستخدمة في البحث

- تم تصميم النظام ثم برمجته باستخدام لغة Visual Basic.net، وذلك لما تتمتع بها هذه اللغة من المميزات مثل:
- إمكانيات التعامل مع أنواع البيانات المختلفة حتى على مستوى Bit، وهو ما يهمنا في عمل هذا النظام.

- توجد به Classes للتعامل مع Bits بشكل مباشر مثل Bit Array وBit Converter وBitmap.
- تتعامل هذه اللغة بشكل أساسي مع البرمجة الهدفية (OOP).
- التعامل مع الذاكرة بشكل أفضل مما كانت عليه في الإصدارات السابقة.
- سهولة إعادة تعريف الشفرة بشكل قوي ومتين بمجرد تنشيط الكائن من أي مكان في البرنامج.
- إمكانية تصميم واجهة رسومية تسهل على المستخدم التعامل مع هذه اللغة بشكل أفضل.
- اتساع عدد المبرمجين الذين يتقنون العمل هذه اللغة مما جعل المنصة الأولى لتطوير التطبيقات تحت بيئة نظام التشغيل ويندوز، حيث أنه يمكن الاستفادة من البرامج التي تم عملها سابقاً وتطويرها.
- كما أنها تتيح للمبرمج عمل الأدوات ActiveX ومكتبات DLL تمكن المبرمج من عمل أدوات أو مكتبات تعمل على لغات أخرى كال++C VISUAL وغيرها.
- الحفاظ على سرية Code الذي تم برمجته بداخل الأداة أو المكتبة أو التصنيفات مع إمكانية استخدامها.
- توفير المساحة المستخدمة في الذاكرة بحيث أنه لو لديك عدة برامج تستخدم نفس Code فإن كل Code سيأخذ مساحة بالذاكرة أما إذا تم عمل أداة أو مكتبة أو عمل الصنف لهذا Code فإن المساحة التي تخصص له في الذاكرة واحدة بحيث أنه يمكن أن تستفيد منه عدة تطبيقات في نفس الوق

نظرية الإخفاء

فكرة الإخفاء جاءت وبشكل واسع استنباطنا من مشاكل التصنت على الرسائل بين المرسل والمستقبل عندما كان Alic وBob في طرفين ويتمنوا التواصل بين هما بواسطة رسائل سرية كل التواصل بين هما عبر طرف ثالث ولأن Wendy الذي يقوم بعملية التفتيش والفحص للرسائل وهذا يسبب لهم متاعب وبصوره دقيقة يوضح نموذج الإخفاء.

1-إن Alic يأمل أن يرسل رسالة سرية إلى Bob

2-يضع إخفاء للرسالة داخل شي محجوب

3-ترسل الرسالة عبر قناة عامة

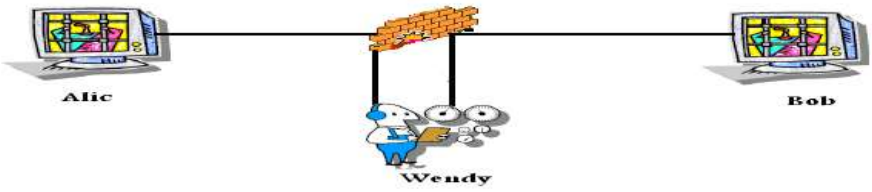
4-Wendy يفحص كل الرسائل المتبادلة بين الطرفين

5-يكون الفحص سالب وموجب

6-يتعمد Wendy التغير في الرسالة

7-هذه النظرية لا يستطيع Wendy أن يشعر بان الرسالة مختزلة

إذا الهدف من نظريه السرية المكتمل في الاتصال الغير قابلة للكشف وأيضا الموثوقية وهناك تطبيقات عديدة في علم الإخفاء الرقمي للصورة التشفير والبطاقة المستقبلية وسريه الاتصال [5].



الشكل (1:1): نظرية الإخفاء

محللي الإخفاء:

هو فن ومهارة كشف وتحديد حالات الرسائل إذا ما اخفوا فيها رسائل مشفرة أو مخفية وإذا أمكن استعاده معلومات الرسائل المخفية من أي حامل رقمي أو من أي قنوات اتصال للمعلومات المخفية وبسبب اختلافات في خصائص الناقل الرقمي التي يمكن إن تنتج من خاصية التجريد أو أي خصائص غير متوقعة كما أنه يقوم بعملية التحقق والملاحظة للعلاقات بين مكونات حجب الرسالة وخصائصها وأدوات برنامج الإخفاء، إذ أن الهدف من وجود رسالة مخفية هو أن تهبط من اكتشافها من قبل المتطفلين وللهجمات والتحليل في علم الإخفاء للمعلومات قد يأخذ عدد من الإطارات مثل الكشف التلخيص والتغير والهدم في المعلومات المخفية وذلك بعد إظهارها كنص مرئي وهذا يدفعنا إلى أن تستخدم برامج وأدوات حتى تزودنا بوسائل وطرق أكثر أمنا في إيصال الرسائل من المرسل إلى المستقبل بدون إن يكتشفها أو يلاحظها أحد لأننا اليوم في عصر التقنيات وتكنولوجيا المعلومات

لغة الإخفاء:

وهي طريقة جيدة وسريعة للكتابة (STENOGRAPHY) لأنها تستخدم رموز مبهمة ومختصرة للغات وكانت تستخدم من قبل الملك والحاشية وكلمة (STENOGRAPHERS) تعني بلغه اليونانية الكتابة السريعة وكانت تكتب بواسطة رموز تعرض رمز الصوت أو مجموعه من الرموز أو تعرض رمز لكلمة أو مجموعه من الكلمات وتعرض أحيانًا رمز لمظهر من الأشكال وعمومًا فأن الإخفاء يتضمن أنوع عديدة من أنظمة اختزال الكتابة.

طريقه watermarking:

(watermarking)، وإن كان في تطبيقات أخرى يمكننا أن نستفيد منها بشي قريب، في أفكار مستقبلية لهذه التقنية لاستخدمها بصور المنتجات بحيث تحتوي الصورة على معلومات المنتج واستخدام برنامج معين يستطيع قرأه المعلومات، أو ممكن أن تكون في

كاميرات تستطيع أن تقرأ المعلومات وتحولها إلى أفكار مستقبلية فقط ويدعا بعلم آل_ (Steganography)، أكثر من (watermarking)، على الرغم من أن أل_ (watermarking)، تأخذ أحيانًا بعض إحدى أهم خاصيات آل_(Steganography)، ألا وهي إخفاء المعلومات بحيث لا تكون ظاهره للمستخدم، لكن الخبراء يختلفوا عن بعضهم بالهدف، فأن (Steganography)، هدفها الأساسي هو إخفاء المعلومات بالشكل الذي لا يظهر للمستخدم، وتظهر بشكل رسالة عاديه بعكس آل_(Cryptography)، أما (watermarking)، هدفها حفظ معلومات خاصة بحماية الملكية الفكرية للمنتجات بشكل عام (صوت، صورة أو...) ضمن هذه المنتجات، ولا يهم إن كانت طريقة الحفظ هذه ظاهرة للعيان أم لا.

مصطلحات البحث:

مصطلحات التشفير والإخفاء (Cryptographic and steganography)

سوف نذكر بعض المصطلحات التي سوف نستخدمها عند الحديث عن التشفير وهذه المصطلحات هي:

1- مصطلح التشفير(Cryptography) عبارة عن طريقة يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية، الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة (أي استعادة المعلومات الأصلية).

2- النص الأصلي أو الصريح (Plaintext) وهو عبارة عن النص أو البيانات التي يراد تشفيرها أو هي البيانات الأصلية التي لم يتم تشفيرها أو هي البيانات التي تم فك تشفيرها واستعادة محتوياتها الأصلية قبل التشفير.

3- النص المشفر (Ciphertext) وهو عبارة عن النص أو البيانات التي تم تشفيرها.

4- التشفير(Encryption) هو عملية تحويل النص أو البيانات إلى شكل غير مفهوم بغرض إخفاء هذه البيانات أو هو عملية تحويل من (Plaintext) إلى (Ciphertext)

5- فك التشفير(Decryption) هو عملية تحويل النصوص أو البيانات التي تم تشفيرها إلى صورتها الأصلية قبل التشفير أو هو عملية التحويل من (Ciphertext) إلى (Plaintext).

6- المفتاح (Key) وهو عبارة عن كلمة السر المستخدمة في خوارزمية التشفير أو فك التشفير ويعتبر وهو من أهم الأشياء التي يجب إخفائها حيث أنه يعتبر من الأشياء السرية التي لا يعرفها إلا المخول لهم فك الشفرة.

7- محللي الشفرات (Cryptanalysts) وهم الأشخاص الذين يحاولون فك الشفرة أو كسرها دون حصولهم على مفتاح التشفير.

8- تحليل الشفرة (Cryptanalysis)

تعرف عملية تحليل الشفرة بأنها محاولة معرفة النص الصريح من النص المشفر دون الحصول على المفتاح من خلال دراسة ظواهر مختلفة على النص المشفر [11].

9- مصطلح الإخفاء Steganography هو علم الإخفاء وله عدد من الطرق والأدوات

10- مصطلح Lsb وهي طريقه تستخدم في إخفاء وإظهار البيانات.

الخلفية النظرية للإخفاء:

الغرض من عرض خلفيه نظريه شامله لكل القضايا الأكثر أهمية لأنشطه البحث والمتعلقة بالإخفاء والطرق الأخرى وكذلك تعمل على تحليل الأبحاث المختلفة، وأيضا تعمل على مدي التكامل في الإخفاء وأنواع الحامل الرقمي التي يمكن تحسينها أكثر في الحاضر في مجالات الاتصال المختلفة.

تاريخ الإخفاء: هذه الطريقة أو التقنية ليست جديدة ولكنها من العلوم القديمة لدي الإغريق في الماضي في ألازمنه القديمة كان الناس يستخدمون طرق عديدة في إخفاء الرسائل الوشم أو إخفاء الحبر ذلك لسرية والابتعاد عن المتطفلين:

- كما ظهر فن التشفير في مصر قبل 4000 سنة.
- كانت تستخدم الملكة ماريا التشفير والإخفاء للبيانات. كما استخدم الفنان جاسبر في صفحات النوتة الموسيقية ليضع رسائل بداخله.

ظهرت اليوم تقنيات الإخفاء والتشفير باستخدام الكمبيوتر وقنوات الاتصالات الرقمية

علم الإخفاء: وهو احدى العلوم المهمة والمسح للدراسة الحالية تشمل على عدة أقسام، القسم الأول يحوي على أنواع الإخفاء، والقسم الثاني يتحدث على التقنية التي تستخدم في الإخفاء أما القسم الثالث، يتحدث على برامج الإخفاء القسم الرابع يركز على أنواع الحامل الرقمي.

أنواع الإخفاء: _توجد ثلاثة أنواع تستخدم برتوكولات برامج الإخفاء وهي التالي:

Pure Steganography.
Secret Key Steganography
Public Key Steganography

طريقة Pure Steganography:

تعتبر طريقة من طرق الإخفاء بحيث لا تتطلب التشفير في الرسائل، مثل إخفاء مفتاح التشفير وهذه الطريقة في الإخفاء أقل أمناً وسريه من حيث سرعة الكشف التي بواسطتها يتم التواصل بشكل سري بين المرسل والمستقبل ويمكن أن تعتمد على فرضية أنه لا توجد جهات أخرى تتطلع على الرسائل عندما يكون النظام مفتوح مثل الانترنت.

المفتاح السري في الإخفاء:

يعرف كنظام تشفير الذي يطلب التغير في المفتاح السري السابق للاتصال والمفتاح السري للإخفاء بحيث يعمل على حجب الرسائل وإخفاءه، والرسالة السرية بداخلة باستخدام مفتاح سري والجهات التي تعرف المفتاح السري تستطيع أن تغير وتعالج الرسائل السرية عكس النظرية الأولي عندما تكون قنوات الاتصال جاهزة وغير مرنه، والمفتاح السري للإخفاء يجعله أكثر مقبولية وآمناً في الاتصالات ومن فوائد المفتاح السري في الإخفاء انه إذا عرف من قبل جهات أخرى فانه يمكن تغير المفتاح السري للرسالة في أي وقت وفي أي مكان.

المفتاح العام في الإخفاء:

يأخذ مفهومه من المفتاح العام للتشفير والمفتاح السري للإخفاء وكذلك يعرف كبرنامج للإخفاء والذي يستخدم المفتاح العام والمفتاح الخاص ليؤمن اتصالات بين الجهات التي تريد التواصل فيما بينهم بشكل سري، والمرسل سوف يستخدم المفتاح العام والخاص الذي يمتلك علاقة رياضية مع المفتاح العام الذي يمكنه حل شفرة الرسالة السرية والمفتاح العام يزودنا بطريقه قويه وأكثر أمنا لتنفيذ برامج الإخفاء وذلك لاستخدامه بطرق أكثر قوة وأمنا في تكنولوجيا الأبحاث في التشفير ولديه مستويات متعددة الأمن من الجهات الغير مرغوب فيها ويجب أولاً استخدام برامج الإخفاء التي تقوم على خوارزميات ال_ **crack** المستخدمة من قبل المفتاح العام قبل إن يتم التعرف على الرسالة السرية.

تقنيات الإخفاء القديمة

يجب أن نوضح خلفيه نظريه قصيرة على التقنيات القديمة قبل أن نخوض في التقنيات الحديثة التي تستخدم تقنيات الإخفاء مع بعض التفاصيل لكل تقنيه:

1- **Old Steganographic techniques**
2- **Hide messages in wax tablets**
3- **Hide messages on messenger's body**
4- **Hide messages using Microdots**

إخفاء الرسائل باستخدام الشمع: كان شعب اليونان قديما يكتبوا الرسائل على الألواح ويتم بعد ذلك وضع الشمع على الرسائل فتحجب الرسائل بحيث تكون غير مرنيه للعيان ويتم استخلاص هذا الشمع من كهوف النحل (**bee wax**) التي تستخدم في بناء كهوف العسل ولذلك فهذه المادة عند صهرها على اللوح بحيث تكون الرسائل تحت هذه المادة بدون أن يلاحظ أي احد إنه هناك توجد رسائل مخفيه.

إخفاء الرسائل باستخدام الوشم: قديما كان في اليونان الفيلسوف هيرودوت يحكي أنها كانت ترسل الرسائل السرية في الحروب بواسطة الوشم في الرأس المحلوق للعبد عندما كانت تخوض حرب مع الفرس فتوضع رسالة سريه على راس العبد عن طريق وشمه بطريقه الوشم بعد ذلك ينتظر حتى ينمو شعره فتحجب الرسالة فلا أحد يلاحظ أو يشك أن هناك رسائل مخفيه، وعند الوصول إلى الهدف يقوم بحلق شعره حتى تقرأ الرسائل الموشمة وتحليلها.

إخفاء الرسائل باستخدام microdot :

تم استخدامها في الحرب العالمية الثانية من قبل ألمانيا وجهات أخرى مثل وكالات التجسس الذين كانوا يستخدمون (**microdot**)، من وإلى أماكن مختلقه بحيث يتم تقطيع الرسائل إلى أجزاء صغيره جدا بحيث تكون حجم الجملة أو الكلمة مطبوعة من قبل الطباع على شكل نقاط صغيره (**DOT**)، وربما إلى خطوط من 10–12 في كل بوصه ولا يستطيع التعرف عليها من قبل أي جهات ما لم تحصل على جميع أجزاء الرسالة وتحليل الشفرة وكانت تخفي الرسائل داخل الطوابع البريدية

التقنيات الجديدة عن برامج الإخفاء

- **Chaffing and winnowing**
- **Invisible ink**
- **Null ciphers**

طريقة Chaffing and winnowing :

هي غربله وتقشير الحبوب بواسطة آلات الضرب تستخدم هذه العبارة مجازيا في تقنية التشفير (عزل وغربلة)، لتحقيق أهدافها بشكل سري جداً بدون استخدام تشفير، وعند إرسال البيانات بواسطة القناة الغير سرية في هذه التقنية بحيث يرسل المرسل رسالة مختلفة، وكل رسالة غير مشفرة تكون محققة بواسطة شفرة الرسالة وتحقق الذي في هذه المفتاح واحدة فقط من هذي الرسائل محققة والأخرى مزيفة بحيث أن المتطفل على الرسائل لن يكون بمقداره الوصول إلى محتوى هذه الرسالة.

طريقة Invisible ink:

وهي مادة التي يمكن الكتابة عليها وهي غير مرئية في الواقع وتختفي بسرعة والمادة تخزن بشكل تسلسلي باستخدام حبر الإخفاء من قبل وكالات التجسس ولبساطة في هذا الحبر لأنه يستخدم عصير الليمون والحليب ومن هذا النوع يحتاج الحبر حرارة للتثبيت وأي حمض أخر سوف يكون مفيد للكتابة داخل الورقة مثل قلم التعبئة وخشبة الآسنان بحيث يتم وضعه في الحبر والختم يتم وضعه داخل الحبر حتى يجف وتظهر محتوي الرسالة المطلوب

طريقة Null ciphers:

قديمًا كان يتم التشفير بحيث يكون النص الأصلي قبل التشفير مخلوط مع كمية كبيرة من المادة غير المشفرة بحيث تعتبر اليوم كصيغة بسيطة لعملية إخفاء الشفرة الغير مهمة وممكن تستخدم شفرة النص كجزء من عملية أكثر تعقيدا مثل أحوال الطقس في الليل وكذلك زيادة نسبة الثلج المفاجئ والضباب الغير المتوقع في المدن بحيث أن نكون حذرين جداً وينذرنا باستخدام كفرات الثلج الخاصة في الأنفاق والخطوط السريعة الغير معروف وكذلك تستخدمه الشرطة في الطوارئ بحيث تحذر الناس في انزلاق الثلج في يوم معين ويتم اخذ هذه الرسالة بشكل تتابعي حتى يتم تسليم الرسالة الحقيقية المنبه بالخطر وهذه العملية تقوم بإرسال شفرات متقطعة إلى عدة أجزاء وعند تجميع هذه الشفرات المجزئة نستنتج بأنها رسالة حقيقية ذو أهمية كبيرة وهذا النوع مفيد للأحوال الجوية وفي المجال العسكري أيضاً.

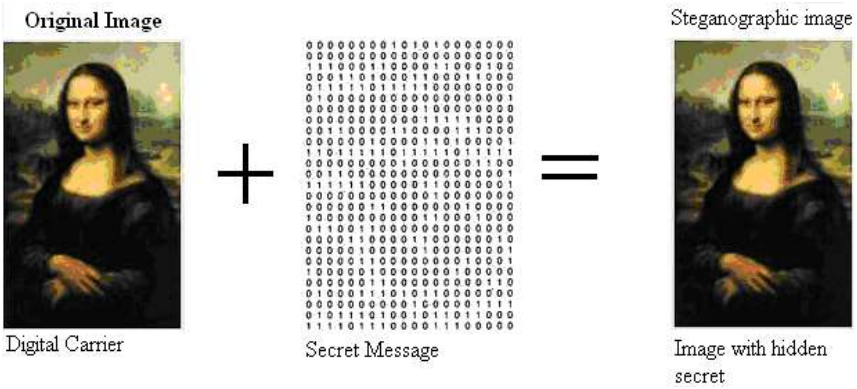
تحليل أمنيه النظام:

تعتمد معظم النظم في تصميم أمنيتها على وجود كلمة المرور (Password)، بحيث لا تسمح بالدخول إليها دون معرفة كلمة المرور أو فتح ملف الإخفاء أو فك شفرة ملف أو تشفير كما في نظامنا وبما أن النظام الذي نقوم بتصميمه يعتبر من هذه النظم فقد روعي عند تصميمه الكثير من الجوانب الأمنية حيث تم الحرص على عدم استخدام أي ملفات مؤقتة أثناء إظهار الرسائل السرية أو لتشفير أو فك التشفير كما أنه عند التشفير يتم إدخال كلمة السر مرتين بغرض التأكد من صحة كلمة السر عند التشفير كما أنه تم مراعاة حالة الأحرف حيث أن النظام حساس لحالة الأحرف عند إدخالها ما يسمى بال (Case Sensitive)، وبالتالي يوفر المزيد من الأمنية عند إدخال كلمة المرور.

ترميز المعلومات داخل الصورة:

القوه في المشروع تظهر في مضاعفة الحماية التي تبدأ في التشفير والترميز والإخفاء وذلك بدس رسالة سريه بعد تشفيرها وترميزها وإخفاءها داخل الصورة (Digital image)، والتي سوف نتطرق إلى تفاصيل كل العمليات والخصائص الرئيسية للصورة الرقمية

والكمبيوتر يعرض الصور عن طريق عدد من المصفوفات المختلفة وتكون على شكل نقاط أوpixels وهذأه النقاط أو pixels تعرض البيانات التي تشاهده العين المجردة ويبين الشكل (1:3) ترميز المعلومات داخل الصورة [3].

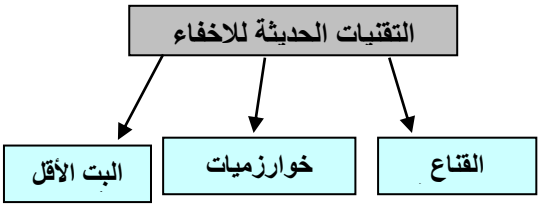


الشكل (1:3): ترميز المعلومات داخل الصورة

معظم الطرق الشائعة في الإخفاء تستخدم طرق قديمة مثل التبديل عدد كبير من pixel بحيث تكون الصورة فيها قليل من التشويش عكس طريقه lsb والتي تقوم بعمليات إخفاء الرسالة بعد تشفيرها داخل الصورة باختيار عدد من pixel وتبديلها مع عدد من Bits ومن مميزاتها إنها طريقة سهله في توظيف الرسائل وتحميلها داخل الحامل الرقمي حيث تقوم بتقسيم كل Byte إلى Bit8 وتعمل عمليات الترميز للصورة الأصلية ونحتاج إلى مكونات التالية:

1- الصورة الأصلية
2- الحمل الرقمي
3- التشفير الرسائل السرية
4- عمليات الترميز
5- الصورة بداخلها الرسائل المخفية

التقنيات الحديثة للإخفاء :



الشكل (2:3): التقنيات الحديثة للإخفاء

طريقه LSB: هو أخر Bit في اليمين ويدعي (LSD) وهو Bit الأقل أهميه بسبب أنه يغير القيم وتأثر على عدد من قيم أخري مثل 11111111=255 بحيث تقوم LSD بتغير واحد Bit بحيث تصبح القيمة 11111110=254 فمعظم أدوات الإخفاء تستخدم LSD لكل Pixel يساوي 8 Bit وكل رقم ثنائي يستبدل مع واحد Bit لإخفاء الرسالة والبيانات الثنائية للرسالة السرية تكون مدخلات في LSD لكل pixel في الصورة.

طريق القناع: تأتي بمعني القناع وتعني التغطية وحجب الأشياء إشارة بواسطة إشارة أخري وهي التصفية واستخدام هذه الطريقة لإخفاء المعلومات بواسطة علامة في الصور في إخفاء المعلومات بطريقه مشابه في إخفاء المعلومات للصفحة الأصلية watermarking التي تم النسخ منها، وبعض الأحيان يتم استخدام طريقه أل_ watermarking الرقمية في استخدام 24 bit ولمعان في الصور مما يزيد في مقدار الإضاءة للصورة مما يعرضها للكشف السريع وإما القناع فالوضوح فيها قليل مما يعطي فرصة قليلة للكشف من قبل المتطفلين فالقناع يضيف حشو في إخفاء المعلومات ثم نستخدم التصفية لإظهار الصورة وهذه الطريقة تعطي حماية تجاه بعض من أنواع معالجات الصور مثل (cropping and routing)

خوارزميات التحويل:

هذه التقنية تستخدم الدوال الرياضية وخوارزميات الضغط لإخفاء المعلومات وحجب الصور بواسطة التغير في المعامل الرياضي النسبي أو تحويل درجة المعامل للصورة (cosign)، والفكرة هو إخفاء البيانات باستخدام Bit الأقل أهمية (LSD) في ملفjpeg مع معالجة من (DCT)، (Direct cosign transformation) تستخدم هذه الخوارزمية لضغط الصور من نوع JPEG كما تقوم خوارزمية النقل Bit لكل قطاع بشكل متتابع في الصورة Pixel 8*8 كما نستطيع أن يعالج الصورة بواسطة Fourier transformation, (wavelet)

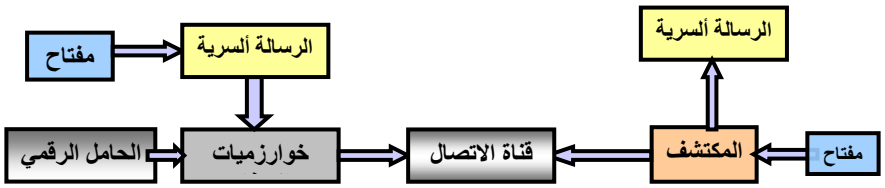
خوارزميات كشف البيانات:

خوارزميات تستخدم من قبل محللي الإخفاء عند الشك بملفات معينه جاءت من قبل المرسل إلى المستقبل فيعترض طريقه المتطفلين وبعض الوكالات المخولة بذلك مثل شركة (Microsoft)، داخل الشبكة العنكبوتية ويتكون الشكل (3:3) من الأجزاء التالية:

1- الحامل الرقمي
2- المفتاح
3- الرسالة السرية
4- خوارزميات الإخفاء
5- قناة الاتصال
6- المكتشف

قبل البدء بعمل نظام إخفاء قوي يجب أن نجيب على عدد من التساؤلات، ما هي العلاقة بين الحامل والرسائل، من يفتح الرسائل، كم عدد الذين يستقبلونها هناك، هل المفتاح معروف للكل؟ وهناك خطوات لعمل نظام كشف وهي كالتالي:

1- ما نوع المفتاح المستخدم؟
2- ما نوع الحامل الرقمي المستخدم؟
3- ماهي الخوارزميات المستخدمة؟
4- قناة الاتصال بين المستخدم والمرسل؟
5- المكتشف هو محلل الإخفاء والتشفير؟
6- الرسائل السرية؟



الشكل (3:3): خوارزميات كشف البيانات

خوارزميات الإخفاء الرئيسية:

توضح هذه الخوارزميات كيف يتم عمليات الإخفاء من جهة المرسل والإظهار تعتبر عملية عكسية عند المستقبل تعتمد أساساً على خوارزميات ودوال رياضية ويوضح الشكل(4:3) خوارزميات الإخفاء الرئيسية

1-وطائف الإخفاء fE.

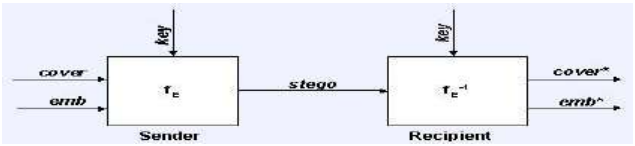
2-وطائف الإظهار fE.

3-حجب البيانات داخل الحامل الرقمي cover.

4-الرسالة المخفية emb.

5-المفاتيح التماثلية key.

6-جمع الرسائل داخل الحامل يعطي الإخفاء stego.

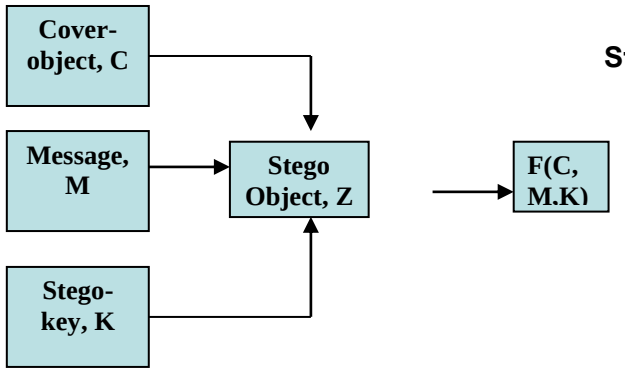


الشكل (4:3): خوارزميات الإخفاء الرئيسية

مكونات Steganography:

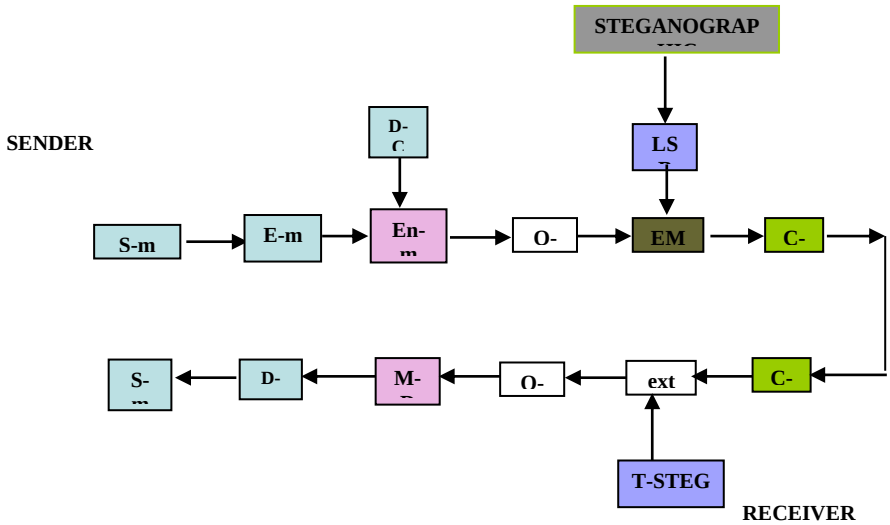
من خلال الشكل يتضح لنا المكونات الأساسية لبناء نظام إخفاء تتكون من الوعاء أو الحامل والرسالة السرية والمفاتيح المستخدمة تعتبر مدخلات أساسية للنظام تنتج عنها نظام إخفاء يسمى stego-object

I. **Cover- Object**
II. **Steg-key**
III. **Steg-Application**
IV. **Stego-Object**



الشكل (5:3): مكونات Steganography

دورة حياه النظام



الشكل (6:3): دورة حياه النظام

توضيح رموز خوارزمية النظام:

1- (S-M) الرسالة السرية.

2- (E-M) عمليات تشفير الرسائل السرية.

3- (EN-M) عمليات ENCODER للرسائل المشفرة.

4- (D-C) نوع الحامل الرقمي المستخدم Digital carrier.

5- (O-G) الصورة الأصلية قبل عمليات الإخفاء.

6- (EMB) خوارزميات الإخفاء.

7- (C-G) الصورة بعد عمليات الإخفاء.

8- (EXT) خوارزميات الإظهار للصورة.

9- (DC-M) عمليات DECODER للرسالة المشفرة.

10- (D-M) عمليات فك التشفير للرسائل.

11- (T-SEG) استخدام أدوات الإخفاء.

12- (K-S) المفتاح التماثلي.

- يوضح (s-m)، الرسالة السرية التي يقوم المرسل بتحرير الرسالة بمحرر النصوص MS-Notepad أو أي محرر آخر مثل MS-word ويتم حفظها قبل أن تتم عليها عمليات التشفير والإخفاء وإرسالها إلى الهدف

- (D–C) Digital carrier الحامل الرقمي هو الوعاء الذي يستخدم لحمل الملفات كحامل رقمي وتم اختيار الصور الرقمية عن غيرها من أنواع أخري مثل الصوت أو الفيديو بسبب استخدامها بشكل واسع على الشبكة وأيضاً المقدرة على الضغط وحجمه الصغير لا تسبب لها مشاكل في الشبكة ولها أنواع عديدة مثل bmp, gif.
- (K–S) KEY–SYMMETRIC نوع المفتاح المستخدم في عمليات تشفير وفك التشفير والإخفاء والإظهار وهو مفتاح تماثلي يستخدمه المرسل والمستقبل.
- (G–O) ORIGINAL–IMAGE الصورة الأصلية وهي الصورة التي لم يحدث لها أي معالجه آو تغير في محتوياتها.
- (C–G) COVER–IMAGE هي الصور التي تم لها عملية معالجه وتغير في محتواه مثل عملية إخفاء البيانات داخلها بتبديل pixel الصورة مع Bit الرسالة السرية.
- (T–SEG)، اختصار Tools– Steganography استخدام أدوات في علم الإخفاء لعمليات مقارنة في نتائج البحث.

طريقة تشفير البيانات النصية:

(E–M) اختصار Encryption– Message طرق التشفير كثيرة وواسعة لكن سنعمل على طريقة واحده وهي خوارزمية (DES)، التي تستخدم (64 Bit)، أي تقوم بتشفير كلمة مكونة من ثمانية حروف فقط وتستخدم كلمة سر بطول (50 Bit)، ومن كلمة السر سوف نستخرج (key–16)، وذلك لان (64Bit)، سوف تمرر على مراحل الخوارزمية (16 دورة)، قبل أن تخرج لنا في شكلها النهائي بصورة كلمة مشفرة، وفي كل دورة سوف تشفر (64 Bit)، بمفتاح مختلف وذلك لتعزيز الحماية وسوف نوضح هذه المراحل بشكل أفضل مع شرح كيفية إعادة إلى المرحلة الأولى قبل التشفير (فك تشفير) وقبل البدء في تحليل مراحل الخوارزمية (DES)، سوف نقوم أولاً بشرح كيفية توليد المفاتيح لأن هذه المفاتيح يجب إنشائها قبل البدء بتشفير النص.

تحليل نظام تشفير النصوص: وهو يستخدم لتشفير النصوص المكتوبة أو المفتوحة بواسطة محرر النصوص المستخدم لكتابة النصوص حيث نقوم بإضافة 64 Bit عشوائية والغرض منها توليد نص مشفر مختلف كل مرة حتى لو تم التشفير بنفس المفتاح، ونضيف 32 Bit مع ال_64 Bit المستخدمة لتغيير النص المشفر والغرض من هذه الBit 32 هو التعرف على كلمة السر عند فك التشفير هل كلمة السر صحيحة أم لا ثم نقوم بدمجها في بداية النص المضغوط المراد تشفيره ومن ثم نقوم بتشفير البيانات بواسطة الطريقة القياسية لتشفير البيانات DES وبعد ذلك نقوم بترميزها بواسطة طريقة (Base64)، لنتغلب على مشكلة

الترميز في أنظمة التشغيل المختلفة وبالتالي تكون عملية التشفير قد تمت وعند فك التشفير نقوم بعكس خطوات التشفير بالإضافة لتوليد نص مشفر مختلف عند تشفير نفس النص مع نفس كلمة السر في كل مرة وعند فك أي نص مشفر فإن النص الناتج هو النص الأصلي رغم اختلاف النص المشفر وتشابه المفتاح وبإضافة عملية ثمانية Byte عشوائية قبل التشفير وعملية الترميز بعد التشفير فإن ذلك يعطي النظام مناعة قوية ضد الاختراق.

نتائج البحث: في هذه الدراسة سوف نوضح النتائج التي حصلنا عليها بعد عمليات التجربة على عدد من أنواع الحامل الرقمي المختلفة للصور في الامتداد والمختلفة في الحجم وأيضًا حجم البيانات التي سوف نقوم بخفاء ها داخل الحامل الرقمي والتي سوف نحول نجيب على عدد من القضايا منها ما مقدار أكبر حجم من البيانات التي سوف يتم خزنها داخل الصور ومع ذلك نقرر ما مقدار ال_Pixel في الصورة والمساحة التي يتم إخفاءه في كل Pixel نلاحظ بين الصورة الأصلية والصورة (Stego)،عندما تري بالعين المجرد بنظام البشري للإنسان لا نري أي فرق بينهما نسبة للتأثيرات اللون.

الشكل (1:6) : صورة أصلية

الشكل (2:6) : صورة داخلها البيانات

تأثير المتجهات في عمليات الإخفاء:

يوضح الجدول (1:6)، كم عدد من الأحرف التي يمكن إخفاءها داخل الصورة مع أحجام

مختلفه هذه الجداول توضح لنا مقدار البيانات التي نستطيع أن نخفيها اعتمادا على حجم الصور وعلى دقه كل Pixel في الصورة وعمق اللون بناء على الاستنتاجات.

جدول (1:6): تأثير المتجهات في عمليات الإخفاء

اسم الصورة	البعد (Pixel)	حجم الصورة (KB)	نوع الصورة	عدد أحرف الرسالة للخفاء	حجم الصورة بعد (KB)	نوع الصورة بعد	طول كلمة السر (حرف)
Yemen	812X612	207	24bit JPEG	61862	1454	24bit BMP	10
River	600X450	70.8		33559	791		
Palace	450X600	64.1		33551	792		
Neal	250X341	32.8		10494	250		
Eagle	250X341	27.3		10494	250		

تأثير دقة pixel في عمليات الإخفاء:

يوضح الجدول (2:6)، تأثير مجموع حاصل كل Pixel في الصور والتي تملك أنواع مختلفه عندما نحول صوره من نوع (JPEG)، إلى صوره من نوع (BMP)، والرسالة السرية مخفيه بداخلها.

جدول (2:6): تأثير دقة Pixel في عمليات الإخفاء

اسم الصورة	البعد (Pixel)	حجم الصورة (KB)	نوع الصورة	عدد أحرف الرسالة للخفاء	حجم الصورة بعد (KB)	نوع الصورة بعد	طول كلمة السر (حرف)
Yemen	812X612	1454	24bit BMP	61862	1454	24bit BMP	10
River	600X450	791		33549	791		
Palace	450X600	792		33549	792		
Neal	250X341	250		10494	250		
Eagle	250X341	250		10494	250		

تأثير حجم الصورة في عمليات الإخفاء:

نلاحظ بين الصورة الأصلية والصورة (Stego)، عندما تري بالعين المجرد بنظام البشري للإنسان لا نري أي فرق بينهما بنسبه للتأثيرات اللون.

يوضح الجدول (3:6) تأثير مجموع حاصل كل Pixel في الصور والتي تملك أنواع مختلفه عندما نحول صوره من نوع (JPEG)، إلى صوره من نوع (BMP)، والرسالة السرية مخفيه بداخلها مع العلاقة في حجم ونوع الصور.

جدول (3:6): تأثير حجم الصورة في عمليات الإخفاء

اسم الصورة	حجم الصورة (KB)	البعد (Pixel)	نوع الصورة	عدد حروف الرسالة للخفاء	حجم الرسالة بعد (KB)	طول كلمه السر (حرف)
Yemen	207	24bit JPEG	812X612	61862	1454	10
River	70.4		600X450	33549	791	
Palace	60.1		450X600	33549	792	
Neal	32.8		250X341	10494	250	
Eagle	27.3		250X341	10494	250	

يوضح الجدول(4:6) تأثير حجم الصور من نوع BMP وحجم الصور لخفاء رسائل سريه فيها.

جدول (4:6): تأثير المتجهات في عمليات الإخفاء

اسم الصورة	حجم الصورة (KB)	البعد (Pixel)	نوع الصورة	عدد حروف الرسالة للخفاء	حجم الرسالة بعد (KB)	طول كلمه السر (حرف)
Yemen	1454	812X612	24bit BMP	61862	1454	10
River	791	600X450		33549	791	
Palace	792	450X600		33549	792	
Neal	250	250X341		10494	250	
Eagle	250	250X341		10494	250	

متطلبات التشغيل: أن اقل المتطلبات التي يمكن أن يعمل عليها نظامنا هي النحو التالي:

الكيان المادي: ويقصد به مكونات الحاسوب حيث يتطلب النظام وجود هذه المواصفات كحد أدنى:

1- معالج (Microprocessor)، السرعة 200 MHz.

2- ذاكرة مؤقتة (RAM)، الحجمMegabyte 64.

3- قرص صلب (Hard Disk)، السعة 2Gigabyte.

4- طابعة لطباعة المستندات.

5- الكيان البر مجي

يتطلب نظامنا وجود نظام تشغيل Windows 7 نسخة عربية أو أي إصدار أحدث مع العلم أنه اذا لم تتوفر مثل هذه المواصفات يمكن توفير مواصفات أعلى منها حسب الإمكانيات.

القائمة الرئيسية: عند الضغط على أمر القائمة الرئيسية الواجهات في الشكل (1:5) التالي والذي يحتوي على عدد من الأوامر التالية:

1-إخفاء

2-إظهار

3-مقارنه

4-تعليمات

5-إغلاق

الشكل (1:5):القائمة الرئيسية

واجهة الإخفاء:

هذه الواجهة الأساسية للإخفاء وتحتوي على الخيارات الآتية:

1-ادخل كلمه السر والتي لا تقل عن 8 حروف.

2-الضغط على أمر تحميل الصورة في قائمه الصور.

3-الضغط على فتح النص للرسالة السرية أو كتابه مباشره في text.

4-الضغط على آمر تشفير النص للرسالة السرية.

5-الضغط على أمر Encoder للنص المشفر.

6-الضغط على أمر إخفاء للنص بعد العمليات التي أجرت عليه.

7-حفظ الصورة بعد عمليات إلا خفاء عليها.

الشكل (2:5): واجهة الإخفاء

واجهة الإظهار:

هذه الواجهة الأساسية للإظهار وتحتوي على الخيارات آلاتية:

على عدد من الأوامر الموضحة في الشكل (3:5)

1-ادخل كلمه السر المكونة من 8 حروف.

2-الضغط على أمر إظهار للرسالة السرية.

3-الضغط على أمر Decoder للنص المشفر للرسالة المشفرة.

4-الضغط على أمر فك التشفير للنص المشفر.

5-حفظ الرسالة السرية.

6-الضغط على آمر خروج.

الشكل (3:5): واجهة الإظهار

واجهة المقارنة:

واجهة مقارنة من القائمة الرئيسية وعند الضغط على أمر مقارنه بين الصور الموضح في الشكل (4:5) والذي يحتوي على التالي:

1- القائمة الرئيسية.
2- الضغط على أمر الصورة الأصلية.
3- الضغط على أمر الصورة التي بداخله الرسالة السرية.
4- إغلاق.

الشكل (4:5): واجهة المقارنة

المراجع:

[1] R.J. Anderson, and F.A.P. Peticolas, "On the Limits of Steganography," *IEEE J. Selected Areas Comm.*, vol. 16, no. 4, May 1998
http://isse.gmu.edu/~njohnson/stegdoc/stegdoc.html
[2] F. Petitcolas, R. Anderson, and M. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no.7, pp.1062-1078, July 1999.
[3] (Applications of Data Hiding in Digital Images Tutorial for The ISSPA'99, Brisbane, Australia August 22-25, 1999
[4] R. J. Anderson and F. A. P. Petitcolas, Information Hiding: An annotated bibliography, available on the web at http://www.petitcolas.net/fabien/steganography/bibliography/ version 1.25, 13 Aug 1999.
[5] Andersen, R., "Stretching the Limits of Steganography," Cambridge University, May 30, 1990.
[6] Kate Gregory, "Special Edition Using Visual C++ 6", Copyright, Macmillan Computer Publishing.
[7] MSDN Library Visual Studio 6.0, Microsoft Corporation,1999
[8] University of Auckland - Peter Gutmann للكاتب Encryption and Security Tutorial-كتاب

[9] (Bruce Schneier) (كتاب Applied Cryptography للكاتب)
[10] Security and privacy Issues by Neil Johnson, http://www.jjtc.com/Security
[11] network and communication.Bhrozan, July 2005.
[12] *An Image hiding technique using block truncation coding. Piyu Tsai, Yu Chen Hu and Chin Chen Chang. July 2002*.

المصادر الإلكترونية:

[13] http://www.hazemskeek.com/Scientifc_Assay/physics/physicsassay.htm
[14] http://www.yashabab.net/modules/news/article.php?storyid
[15] http://www.softshape.com
[16] http://www.itep.co.ae/itportal/arabic/Content/EducationalCenter/InternetConcepts/encryption.asp