

اقترح خطوة مسبقة للإخفاء باستخدام الصور المشفرة
باستبدال مواقع عناصر الصورة
م. وداد عبد خضر م. م. علي ربيع هاشم م. م. الهام فاضل عقيل

المستخلص:

هناك العديد من طرق إخفاء وتشفير النصوص والرسائل باستخدام الصور (التي تعتبر غطاء)، ويهدف البحث الحالي إلى إعداد خطوة (مرحلة) تسبق الإخفاء/ التشفير (بغض النظر عن طريقة الإخفاء/ التشفير المستخدمة)، وهذه الخطوة تعمل على زيادة التعقيد على من يهدف (المهاجم) إلى فتح الشفرة أو محاولة ذلك، بالتالي الحفاظ على سرية المعلومات المرسله. يتم أولاً إخفاء/ تشفير المعلومات في صور ما، ثم العمل على تغيير اختيار مجموعة من عناصر الصورة (البسكل) بعناية ونقلها ليتم استبدالها بعدد مساوي من لها من عناصر الصورة بحيث نحافظ على الشكل العام للصورة عند النظر إليها بالعين المجردة. بمعنى آخر؛ على مستلم الرسالة والمخول له بالاطلاع على المعلومات المخفية إرجاع عناصر الصورة إلى أماكنها الأصلية من ثم استخدام الطريقة "المفتاح" المخصصة له لفك تشفير الرسالة.

Abstract:

There are many methods to hide and encrypt text messaging with pictures (which is a cover), and aims at the current search to the preparation step (stage) prior to hidden/ encryption (regardless of the method of hidden/ encoder used), and this step is working to increase the complexity of aims (the attacker) to open the code or try it, thus preserving the confidentiality of information transmitted.

Is first hide/ encrypt the information in the images of what, and then work to change the selection of a set of picture elements (pixels) and carefully transfer to be replaced by an equal number of its picture elements so that we maintain the overall shape of the image when viewed with the naked eye. In other words; no message and is authorized to have access to hidden information elements is returned to their places

of origin of the way and then use the "key" assigned to him to decrypt the message.

(1) الجانب النظري:

١-١ مقدمة عامة:-

لا يعد علم الإخفاء من العلوم المستحدثة، فلقد كان أول ظهور لهذا العلم في العصر الإغريقي، حيث قام أحد رجالات العصر بالتواصل مع احد أقربائه في اليونان، عن طريق حلق شعر رؤوس عبيده ثم وشم الرسائل على رؤوسهم بعد ذلك يقوم بانتظار نمو شعر رأسهم ثم إرسالهم إلى الشخص الذي يهدف إلى التواصل معه. ثم جاء بعده العديد من الأشخاص الذين استخدموا الناس والحيوانات والخشب المغطى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية. واستمر تطور هذا العلم، حتى توصل العالم إلى اختراع الحبر الخفي إبان الحرب العالمية الثانية، والذي ساهم كثيراً في التواصل بين أطراف الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الأسرار. وقد تطور علم الإخفاء في الوقت الحالي كثيراً، فأصبح يستخدم المعلومات الرقمية والحاسبات كوسيلة لنقل البيانات. [١]

لإخفاء المعلومات أهمية كبيرة وذلك لأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عاملاً مساعداً على إخفاء حماية وأمناً على المعلومات. يستخدم هذا الفن في عدد من المجالات إلا أن المجال الذي يبرز فيه هذا الفن هو التجارة الإلكترونية التي تزداد تطبيقاتها، والاهتمام بها يوماً بعد آخر. من تطبيقات هذا العلم، العلامات المائية (Watermarks) والتي تستخدم في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة. وبالرغم من أن المشتري أو مستخدم هذه البرامج قد يعلم بوجود مثل هذه العلامات، إلا أن اكتشاف أماكنها داخل البرنامج من الصعوبة بمكان. وعلى افتراض أن المستخدم قد تعرف على مكان وجود هذه العلامة، فسيظهر أمامه تحدٍ آخر، وهو معرفة البرنامج المستخدم في الإخفاء وكلمة السر ومفتاح التشفير، وكلا من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً [٢]. ويأتي أصل مصطلح علم إخفاء المعلومات (Steganography) من الكلمتين الإغريقيتين: stegos والتي تعني السقف أو الغطاء و graphia والتي تعني الكتابة. ويعرف علم إخفاء المعلومات على أنه إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى، لهدف محدد. والبيانات المستخدمة في الإخفاء قد تكون عبارة عن ملفات الوسائط المتعددة (multimedia) كالنصوص، الصور، وملفات الصوت أو الفيديو وغيرها. وقد تكون أيضاً عبارة عن ملفات تنفيذية للبرامج (executable file). وفي عملية الإخفاء نحتاج إلى توفر عنصرين مهمين لإتمام هذه العملية، الأول هو الرسالة التي نهدف إلى إخفائها والثاني هو الوعاء أو الغطاء (cover) المستخدم لإخفاء هذه الرسالة. [٣]

٢-١ الفرق بين علم التشفير وعلم الإخفاء:

علم التشفير وعلم الإخفاء هما طريقتان لحماية المعلومات من عرضها والعبث بها من قبل الأشخاص الغير مرغوبين، لكن كلا من الطريقتين لو استخدمت لوحدها، قد لا تعتبر وسيلة حماية كافية وكاملة. بالنسبة لإخفاء المعلومات مثلاً، حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما، فإن الهدف من عملية الإخفاء يصبح بلا قيمة! لذا فإنه ولزيادة حماية المعلومات المخفاة يجب علينا استخدام كلا من تقنيات حماية المعلومات، التشفير والإخفاء. [٤]

لاكتشاف أهم فرق بين علم التشفير وعلم الإخفاء نكتفي بعرض تعريف لكليهما. فعلم التشفير هو العلم الذي يهدف إلى دراسة طرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل. بينما علم الإخفاء هو العلم الذي يهدف إلى إخفاء وجود الرسالة. إذن الفرق الأساسي هو أن التشفير يغير من هيئة محتوى الرسالة بحيث لا يستطيع أحد قراءتها سوى الأطراف المعنية بها، لكنه لا يخفي وجودها. أما علم الإخفاء فيخفي محتوى الرسالة في المقام الأول. [١]

وهذا يختلف عن فن الإخفاء حيث أن التشفير يغير من هيئة محتوى الرسالة لكنه لا يخفي وجودها. أما إخفاء الكتابة فيخفي وجود الرسالة من الأساس. يمكن تقسيم أساليب فن التشفير إلى [٥]:

- أساليب تحويل الكتابة: وتبنى إما على مبدأ الإبدال، أي يتم تحويل كل عنصر من الرسالة إلى عنصر آخر.

ومبدأ النقل، وفيه يتم إعادة ترتيب حروف الرسالة.

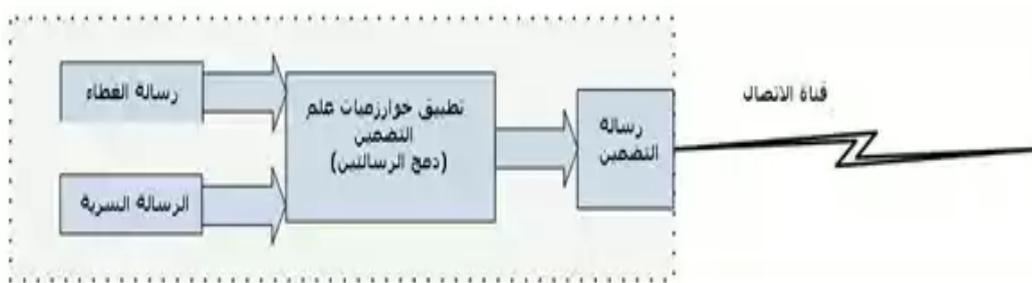
- أساليب معالجة الكتابة: حيث يتم تقسيم الرسالة إلى قطع، وإدخالها على عملية تعالج هذه القطع باستخدام خوارزميات رياضية.

٣-١ أساليب الإخفاء:

يتم إخفاء الرسالة عن طريق إدخالها ضمن الغطاء والذي غالباً ما يكون ملف نصي أو صورة أو ملفات صوت أو فيديو ثم إرسالها إلى الأطراف المعنية. تتمحور فكرة الإخفاء في إدخال الرسالة داخل الغطاء لتكوين الهدف المخفي. ويمكن تمثله المعادلة الآتية والشكل رقم (١):

[٥، ٦]

الهدف المخفي = الرسالة المراد إخفاءها + الغطاء + مفتاح الإخفاء



شكل (١): طريقة إخفاء المعلومات

الشكل (١): مخطط يوضح فكرة الإخفاء في إدخال الرسالة داخل الغطاء لتكوين الهدف المخفي

في ما يلي شرح مبسط لأنواع من علم الإخفاء.

١- **الإخفاء النصي**: وذلك عن طريق إخفاء الرسالة المراد إرسالها باستخدام النصوص. وتتم هذه الطريقة إما بطريقة نصية، مثلاً: يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفية. أو بطريقة نحوية أو لفظية. ويعتبر هذا النوع من الإخفاء من أصعب أنواع الإخفاء، ومن أمثلة هذا الإخفاء هي:

- طريقة استخدام الحرف الأول من كل كلمة: مثال Bring us your invoice by Monday والتي قد تعني: BUY IBM
- طريقة استخدام نموذج (Tamplet).
- طريقة تغيير أماكن التنقيط.
- طريقة استخدام المد (إطالة الكلمات باستخدام -).
- طريقة استخدام التشكيل.
- طريقة استخدام **Unicode Texts**. وتعد هذه طريقة من أجدد الطرق المستخدمة في الإخفاء.

٢- **الإخفاء الصوري**: وذلك عن طريق إخفاء الرسالة المراد إرسالها تحت ملف صوري، ويعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء. ويتم تطبيق هذه النوع من الإخفاء باستخدام أحد الطرق الآتية:

- الإخفاء باستخدام التحويل الزاوي المتقطع (Discrete Cosine Transform).
- الإخفاء باستخدام التحويل الموجي.
- الإخفاء باستخدام الإدخال في البت الأقل أهمية. وتعد طريقة الإدخال في البت الأقل أهمية من أكثر الطرق شيوعاً.

٣- الإخفاء الفيديوي: يعتبر الإخفاء باستخدام ملفات الفيديو جزءاً مشتقاً من الإخفاء باستخدام الصور، وذلك لأن ملفات الفيديو عبارة عن صور مجمعة، لأجل هذا تقنيات الإخفاء بالصور يمكن استخدامها في هذه الطريقة. ومن أشهر الطرق المستخدمة في هذا النوع:

- طريقة الإخفاء باستخدام التحويل الزاوي المتقطع. وتقوم هذه الطريقة بإخفاء جزء من المعلومات في جزء معين من الصور التي يتكون منها الفيديو، وتمتاز هذه الطريقة بأنها غالباً لا يتم اكتشاف البيانات المخفاة بالفيديو باستخدام العين البشرية. لكن يجب ملاحظة أنه كلما ازداد حجم البيانات المخفاة كلما كان كشفها أسهل في جميع الطرق المستخدمة للإخفاء.

٤- الإخفاء الصوتي: ويتم في هذه الطريقة إخفاء الرسالة المراد إرسالها داخل إشارة صوتية ممكن أن تكون في مجال الزمن أو مجال الطيف. ويتم بإحدى الطرق الآتية:

- تغطية الإدراك: وتعد من أكبر الطرق المستخدمة من ناحية سعة الإدخال (٤٥٠,٠٠٠ بت في الثانية) لكنها من أضعف الطرق في الإخفاء، حيث تعد من أكثر الطرق عرضة للاكتشاف.
- ترميز البت المنخفض: وتمتاز هذه الطريقة بسعة إدخال عالية (٤١,٠٠٠ بت في الثانية) لكنها عرضة للاكتشاف من قبل المهاجمين. وفي هذه الطريقة يتم إبدال أكثر بت غير مهم (Least Significant Bit) من كل إشارة صوتية، وتقنية هذه الطريقة مشابهة جداً لتقنية إبدال أكثر بت غير مهم في الإخفاء الصوتي.
- الطيف الممتد: ويتم في هذه الطريقة إدخال الرسالة داخل الترددات العالية. وتعتبر أكثر طريقة من ناحية الإخفاء لكن سعة الإدخال فيها منخفضة جداً (٤ بت في الثانية)، بالرغم من سعتها المنخفضة إلا أنها من أقوى الطرق حماية للمعلومات المخفاة حيث أن الأذن البشرية لا تستطيع تمييز الاختلاف بالصوت بخلاف الطريقتين السابقتين والتي يمكن للأذن البشرية تمييز التشويش في الصوت الناتج عن عملية الإخفاء.

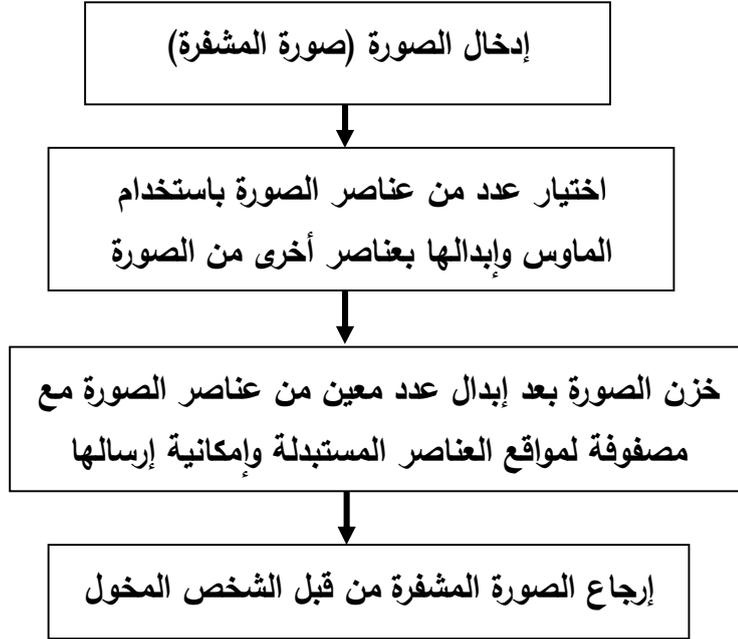
٤-١ الصورة الرقمية:

في الحاسوب، تمثل الصورة كمصفوفة ذات بعدين $(n \times m)$ تضم بداخلها (عناصر) يسمى كل عنصر منها بالبسكل (Pixel) والذي بدوره يملك موقع (Position) في المصفوفة وقيم تمثل كثافة الألوان الثلاثة (Red, Green, Blue)، حيث قيمة لكل من ألوان الثلاثة تصف نقطة على الشاشة، لذا يمكن أن تنشأ مجموعة محدودة من الألوان تغطي الطيف المرئي الكامل من خلال تغيير كثافة قيم (RGB). ويمكن تمثيل الصورة بمصفوفة رقمية وكالاتي:

$$f(x,y) = \begin{pmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{pmatrix}$$

٢- الجانب العملي:**١-٢ الخوارزمية المقترحة:-**

الشكل (٢) يوضح خوارزمية العمل الحالي والتي تتضمن تغيير مواقع معينة من عناصر الصورة (المشفرة بغض النظر عن الطريقة المستخدمة بالتشفير) واستبدالها بمواقع عناصر أخرى والتي يتم اختيار بعناية بحث لا تؤثر على معالم الرئيسية للصورة.



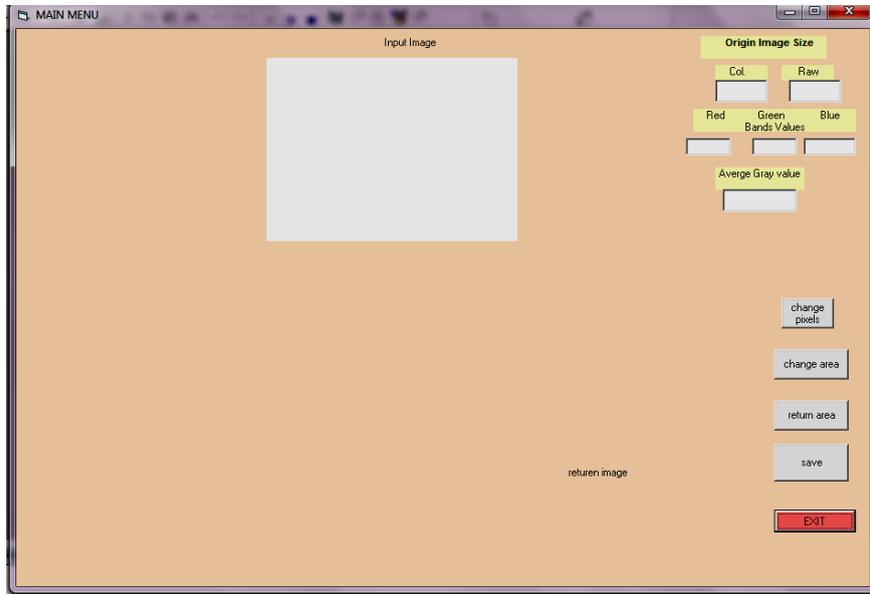
الشكل (٢): مخطط يوضح خوارزمية البحث الحالي

٢-٢ فكرة الدراسة الحالية:-

تعمل فكرة البحث الحالي تغيير (استبدال) مواقع معينة من عناصر الصورة (المشفرة) بمواقع أخرى من عناصر نفس الصورة والتي لا تؤثر على الشكل العام للصورة خاصا للناظر لها، بحيث يتم استبدال العناصر بأخرى تكاد تكون شبيهة لها بالعين المجردة، عن طريق استخدام برنامج VB بالنقر على التوالي على العنصرين المراد استبدال مواقعها ووضعهما في مصفوفة تخزين في نفس البرنامج لغرض إرجاع الصورة إلى شكلها الأصلي متى ما ارد الأشخاص المخولين بفتح الشفرة أو الرسالة المخفية.

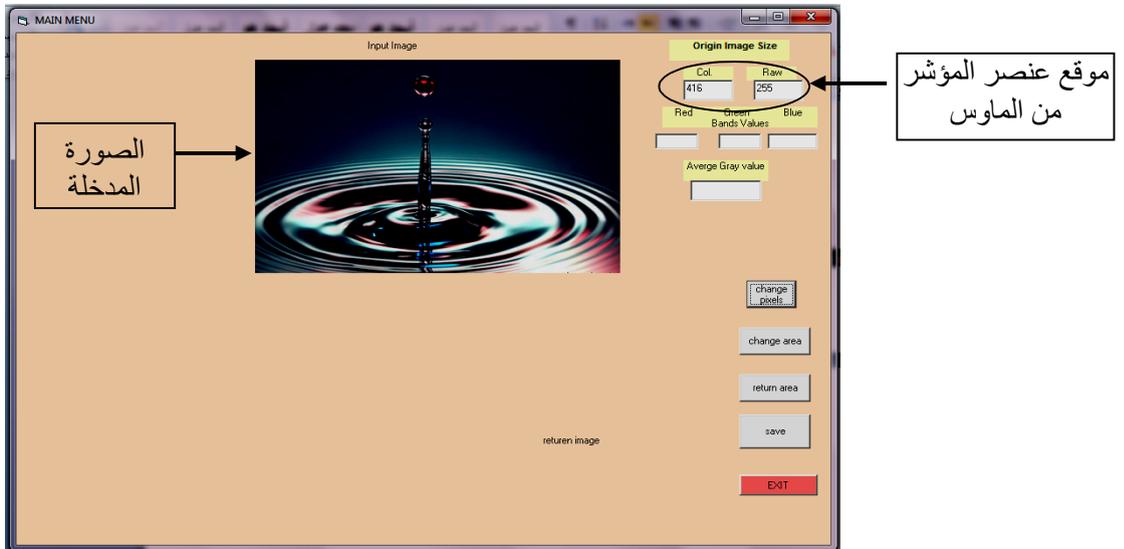
٣-٢ واجهة البرنامج:

الشكل (٣) يوضح واجهة البرنامج بلغة VB المستخدمة في الدراسة الحالية وكالاتي:



الشكل (٣) واجهة البرنامج بلغة VB المستخدمة في الدراسة الحالية

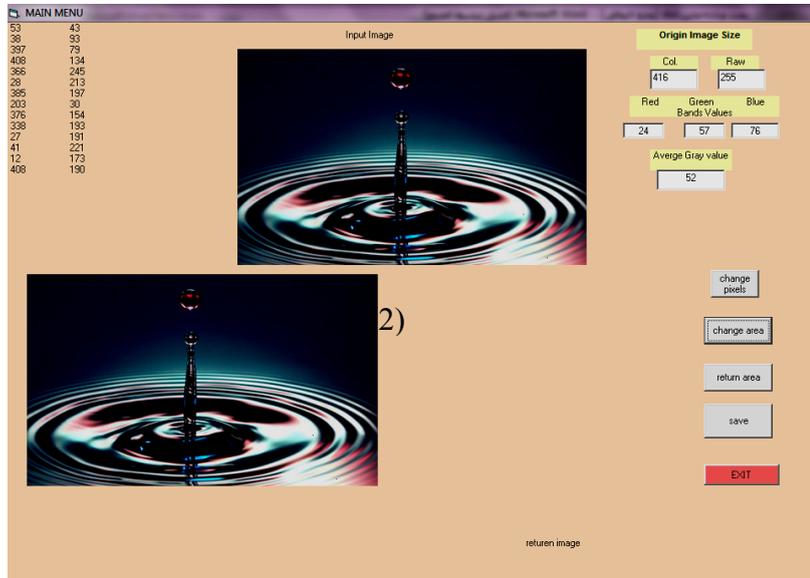
١- استدعاء الصورة المشفرة باستخدام برنامج VB.



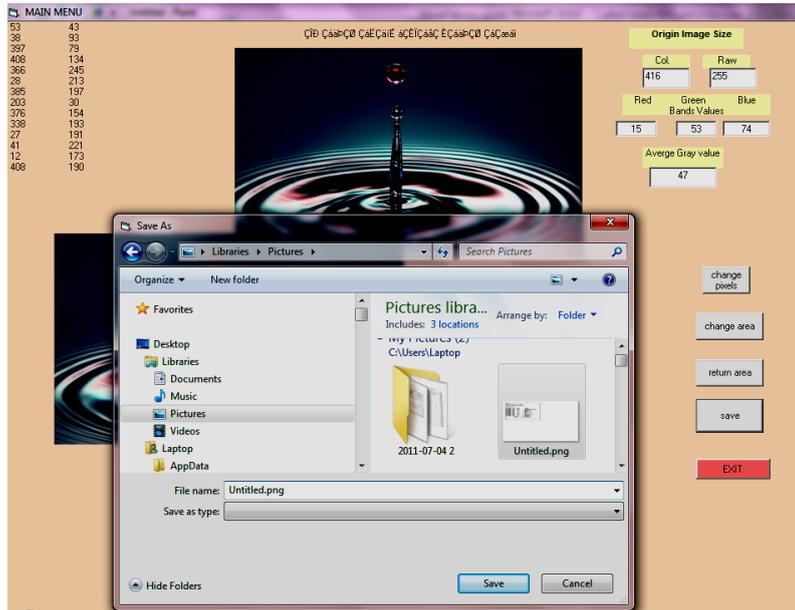
٢- النقر فوق عنصر ما (بكسل) المراد نقله والنقر فوق العنصر المراد استبدال مكانه. وتعاد نفس العملية لعدد من عناصر الصورة (على ان يراعى ان الاستبدال يتم بحيث عدم تشوية الصورة) وخرن مواقع صر المستبدلة بمصفوفة لإمكانية استرجاعها عند الحاجة.



٣- إظهار الصورة بعد استبدال مواقع مجموعة من العناصر (رقم ٢).



٤- خزن الصورة من الإيعاز save أو استرجاع الصورة الأصلية من الإيعاز return.



٣) الاستنتاجات:

- ١- يعمل البرنامج الحالي على زيادة التعقيد على المهاجم للصورة المشفرة.
- ٢- عدم ملاحظة التغيير في مواقع عناصر الصور.
- ٣- يعد سهل التطبيق وعدم الاحتياج للوقت في تنفيذ مرحلة مسبقة لزيادة الأمان في فك الشفرة للرسائل المتضمنة في الصور.
- ٤- سهولة استرجاع الصورة الأصلية دون أي تغيير.

المراجع:

- ١- فن الإخفاء Steganography، منشورات مركز التميز لأمن المعلومات، الكاتب: يوسف دردير، المراجع، يوسف الرويلي، ماجد الربيعان.
- 2- Huaqing Wang, Shuozhong Wang Communications of the ACM " Cyber warfare: steganography vs. steganalysis " <http://www.acmqueue.com>
- 3- Neil F. Johnson, Zoran Duric, Sushil Jajodia, Center for Secure Information Systems George Mason University "Information

Hiding Steganography and Watermarking -Attacks and Countermeasures"

4- Gary C. Kessler Associate Professor Computer and Digital Forensics Program Champlain College Burlington "An Overview of Steganography for the Computer Forensics Examiner"

5- Curran, K. and Bailey, K. "An Evaluation of Image Based Steganography Methods". Int. J. of Digital Evidence, Fall 2003.

6- <http://en.wikipedia.org>