جامعة بوليتكنيك فلسطين

كلية العلوم الإدارية ونظم المعلومات

دائرة تكنولوجيا المعلومات

إخفاء معلومات داخل صورة

(Steganography)

فريق البحث

رهام سمير عادي ساميه سليمان كتلو فاديه وليد أبو شامة

المشرف

المهندس محمد نادر الفلاح

قدم هذا البحث لإنهاء متطلبات التخرج في تخصص تكنولوجيا المعلومات

2009

ملخص المشروع

يهدف المشروع إلى الحفاظ على سرية المعلومات التي تم إخفائها داخل الصور,وعدم اكتشافها واختراقها من قبل أي شخص غير المقصود, لذلك تم الإخفاء بتطبيق عدد من الطرق, لتتناسب كل طريقة مع ما سيتم إخفائه سواء كانت الرسالة المراد إخفائها نصية أو صورة داخل الصور من نوع Bitmap, ولزيادة الحماية على الرسالة التي تم إخفائها فانه تم استخدام ملف المفتاح الذي يعمل على حماية الرسالة المخفية فلا يتم استخراج الرسالة إلا بوجوده.

فهرس المحتويات

الفصل الأول

الفصل الثاني

الفصل الثالث

الفصل الرابع

الفصل الخامس

الفصل السادس

الفصل السابع

قائمة الجداول

فهرس الأشكال

الفصل الأول

المقدمة

1.1 المقدمة

1.2 أهداف المشروع

1.3 أهمية المشروع

1.4 مشكلة الدراسة

1.5 تاريخ علم الإخفاء

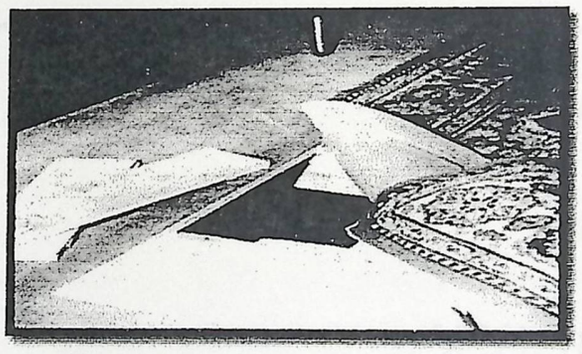
1.6 النتائج المتوقعة

1.7 فريق العمل

1.1 المقدمة :

تعددت وسائل الاتصالات بين الناس، كالهاتف والفاكس وشبكات الحاسبات وأجهـزة الراديـو وأجهزة تخاطب أخرى. وبالرغم من ذلك يبقى الهاجس هو الحفاظ على خصوصية المعلومات المتبادلة، فكل وسيلة من وسائل الإتصال يجب أن تُؤمّن الحد الأدنى من سرية المعلومات المتبادلـة، والطـرف الذي تُرسل له الرسالة يجب أن يكون الوحيد الذي يستطيع أن يقرأ أو يسمع هـذه الرسـالة ويفـسرها ويفهمها كما هو مطلوب.

ظهرت فكرة إخفاء المعلومات منذ القدم بمفهومها البسيط، حيث كان قديماً يتم إخفاء المعلومات المهمة تحت السجاد وغيرها وذلك للحفاظ على سريتها، وذلك دلالة على وجود فكرة إخفاء المعلومـات منذ الزمن القديم جداً.



الشكل (1.1) صورة توضح طريقة الإخفاء في القدم

من هنا جاءت أهمية إخفاء المعلومات, وظهر ما يعرف بعلم الإخفاء في القرن الخامس عـشر قبل الميلاد، فاستُخدم علم إخفاء المعلومات بشكل موسع في فترات زمنية معينة وخصوصاً قبل تطور نظام التشفير. وسَجّل تاريخ علم إخفاء المعلومات في العديد من الحضارات البـشرية المبكـرة حيـث استخدمت كل حضارات العالم نموذج ما في تقنية إخفاء الرسائل .

في هذا المشروع تم اعتماد فكرة إخفاء المعلومات داخل صورة وهو ما يسمى ب Steganography حيث يعود أصل الكلمة إلى اللغة الإغريقية وهي مركبة من كلمتين Stego تعني إخفاء أو تغطية، Graphy تعني الكتابة، فيكون معنى الستيغانوغرافي الكتابة المغلفة أو المغطاة.

ويتكون المشروع من واجهتين إحداهما للمرسل والآخر للمستقبل، حيث يقوم الطرفين باتفاق مسبق على صورة معينة ثم يحدد المرسل الرسالة (نص, صورة) المراد إخفائها، وبناء على الطريقة التي يتم اختيارها يتم دمج الرسالة داخل الصورة.

أما المستقبل فيختار الصورة المدمج بداخلها الرسالة, وعن طريق البرنامج يتم استخراج الرسالة المخفية داخل الصورة.

تعتمد آلية دمج الرسالة داخل الصورة على التعديل على الBits المكونة منها الصورة مع مراعاة عدم التغيير بشكل كبير حتى لا يؤثر على ملامح ولون الصورة بشكل ملحوظ، فتكون عُرضة للإكتشاف من الطرف غير المقصود .

1.2 أهداف المشروع :

تتلخص أهداف المشروع بالنقاط التالية :

1. القدرة على إخفاء نص داخل صورة.
2. القدرة على إخفاء صورة داخل صورة.
3. عدم تغيير حجم ومواصفات الصورة الحاملة للرسالة.
4. عدم تغيير ألوان وملامح الصورة (ظاهرياً).
5. القدرة على فك الإخفاء من قبل المستقبل حيث تصل الرسالة المخفية إلى المستقبل فيقوم بفك الرسالة للحصول على الرسالة المخفية المطلوبة.

1.3 أهمية المشروع :

تتمثل أهمية المشروع في إخفاء معلومة مهمة في أوساط مختلفة ظاهرة للعيان، بحيث لا يمكن رؤية المعلومات المخفية إلا من قبل الشخص المقصود, ويأتي مصدر قوة إخفاء المعلومات من عدم إمكانية اكتشاف المعلومات المخفية من قبل الخصم.

1.4 مشكلة الدراسة:

تكمن المشكلة في إرسال رسالة من طرف لآخر دون قدرة أي طرف غير مقصود من الوصول إلى هذه الرسالة, ومن التحديات في عملية الإخفاء عدم القدرة على إخفاء معلومات كثيرة لأنه كلما زاد حجم الرسالة المراد إخفائها تكون امكانية التأثير على ملامح وألوان الصورة بشكل أكبر مما يؤدي الى اكتشاف وجود رسالة مخفية.

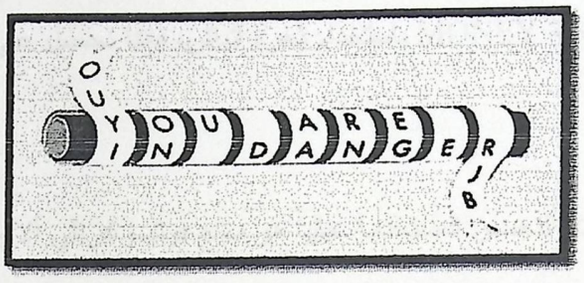
1.5 تاريخ علم الإخفاء:

علم إخفاء المعلومات علم قديم جداً بقدم الإنسان، وحديث ومتطور بتطور علوم الحاسب وتقنية المعلومات، فقد بدأت عملية إخفاء المعلومات في عهد الإغريق (في حدود 700 سنة) قبل الميلاد، وذلك بكتابة الرسائل السرية على الأحجار أو الجلود وإخفائها في بطون الحيوانات، ومن ثم إرسالها إلى الجهة المقصودة بعد اتفاق مسبق بين الطرفين.

أما الحضارات الصينية القديمة فقد اعتادت أن تكتب الرسائل باستخدام القز الرفيع وبعد ذلك تُلف لتُشكّل كرات صغيرة وتُغطى بالشمع.

كما استخدم الإيطاليون في القرن الخامس عشر الألمنيوم والخل للكتابة على قشور البيض، ولاحقاً أصبح البيض يُغلى مما يجعل القشرة الخارجية إسفنجية بحيث ينفذ الحبر إلى زلال البيض المقسّى و تظهر الرسالة عن طريق إزالة القشور.

وبعد ذلك جاءت طريقة جديدة للإخفاء باستخدام الأسطوانة الخشبية ذات القطر المحـــدد بـــين الطرفين، إذ يقوم المرسل بلف شريط من الورق على الأسطوانة الخشبية ويكتب الرسالة التـــي يريـــد إخفاؤها بشكل طولي، وعندما يقوم المستقبل باستلامها يقوم بلفها على أسطوانة بنفس القطر للحـــصول على نص الرسالة المطلوب، وإذا تم وضع الشريط من قبل طرف غير مقصود على أســـطوانة بقطـــر مختلف فلا تظهر الرسالة بنفس الترتيب وبذلك لا يتم فهم الرسالة المخفية كما هو موضح:



الشكل (1.2) طريقة إخفاء المعلومات بواسطة أسطوانة[1]

ومع تقدم الزمن تطورت عمليات إخفاء المعلومات داخل نص كتابي، وتتم هذه العملية بطـــرق مختلفة ومن الأمثلة عليها:

- قراءة الحرف الثاني من كل كلمة في النص بحيث يكون الناتج هو عبارة عن الرسالة المخفية.

فمثلاً عند إخفاء النص التالي: " Pershing Sails from Nyr June I" يتم دمجه داخل نص آخر كما يلي:

"Apparently, neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affect pretext for embargo on by products, ejecting suets and vegetable oils." [2]

---

[1] Steganography and History of Cryptography

[2] أمن المعلومات

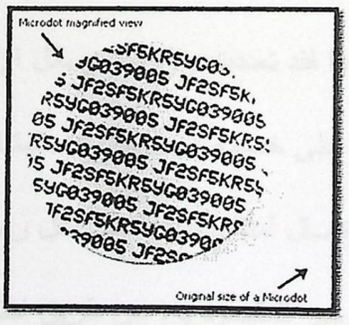
- وبعد ذلك تم استخدام شفرة جديدة تسمى شفرة أتباش، وتعتبر من أبسط أنواع الشفرات، وتلخص طريقتها بأن نجعل الحرف الأول في اللغة هو الحرف الأخير، والحرف الثاني هو الحرف قبل الأخير، وهكذا...، كما هو موضح كالتالي:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

فمثلاً إذا أردنا أن نشفر كلمة MONEY باستخدام شفرة أتباش، فإننا نحصل على النص المشفر التالي .NLMVB

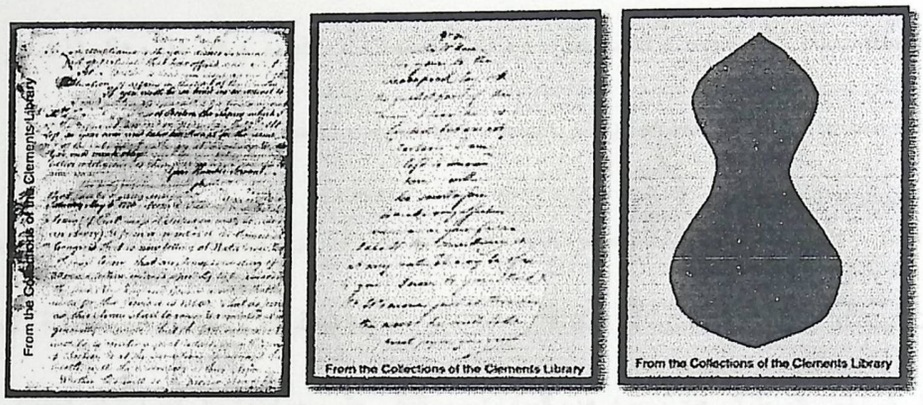
ومن إحدى تقنيات التجسس المستخدمة حالياً هو منتج فوتوغرافي ألا وهو مايكرودوت، والمايكرودوت عبارة عن نص أو صورة تتقلص إلى حجم صغير جداً بحيث لا تكاد تُرى بالعين المجردة, حيث أنّ تلك الصورة أو ذاك النص يُصغّر حرفياً إلى نقطة بحيث تصبح غير ملحوظة للمراقب أو للخصم عندما تُنقل عبر مسار غير أمني، وتُقرأ من قبل المستقبل باستخدام الميكروسكوب, وقد تطورت المايكرودوت حيث أصبحنا نجدها في المركبات، إذ أصبح مصنعوا السيارات يلصقون أرقام صغيرة على القطع باستخدام المايكرودوت, لمنع سرقتها.



الشكل (1.3) طريقة المايكرودوت لإخفاء المعلومات

أما في العصور الوسطى فقد أصبح فن الإخفاء شيئاً معروفاً، فاستُخدمت الكتابة السريّة من قبل الكنيسة الكاثوليكيّة في صراعاتها المتعددة عبر التاريخ ومن قبل الحكومات أيضاً في تلك الفترة. كما واستُخدم علم فن الإخفاء بشكل متلازم مع التشفير للحصول على إخفاء أفضل للمعلومات.

وفي عام 1500 للميلاد اكتشف جيمس جاي الحبر السري واستُخدم من قبل العالمان الأمريكيان صموئيل ودل وروبرت تاونسند، حيث اعتمدوا على أرقام الصفحات والأسطر في كتب معينة مستخدمين الحبر غير المرئي لكتابة رسائلهم عند هذه الصفحات والأسطر، كما استخدم في تقنيات أخرى مختلفة، كما هو موضح بالصور التالية:



الشكل (1.4) طريقة الحبر السري لإخفاء المعلومات [3]

وفي عصر الحاسبات عصرنا هذا فقد تعددت وازدادت وسائل الإتصالات بين الناس، مما زاد الحاجة لوجود طرق جديدة وآمنة للحفاظ على خصوصية المعلومات المتبادلة، فلم تتوصل التكنولوجيا المعاصرة حتى الآن من اختراع وسيلة إتصال آمنة بالقدر الكافي لنقل رسائل فائقة السرية دون الخوف من وقوع هذه الرسائل بين يدي الطرف غير المقصود به، عن طريق اختراق هذا الطرف لوسيلة

---

[3] Steganography and History of Cryptography

الإتصال والإطلاع على الرسالة، فقد تعددت طرق إخفاء المعلومات داخل الصور أو الفيديو، ومن أكثر الطرق شيوعاً لإخفاء المعلومات داخل الصورة ما يلي :

- طريقة الستيغانوغرافي (Steganography).
- طريقة الكريبتوغرافي (Cryptography).

Steganography 1.5.1

الستيغانوغرفي هو إخفاء رسالة ما داخل رسالة أخرى بهدف إخفاء وجود الرسالة الأولى لهدف محدد، والبيانات المستخدمة كظرف أو وعاء للإخفاء يمكن أن تكون عبارة عن ملفات الوسائط المتعددة (الملتيميديا) كالصور، والنصوص، وملفات الصوت أو الفيديو وغيرها، وهكذا في عملية الإخفاء هذه نحتاج إلى ملفين أحدهما يسمى الغطاء (cover)، والآخر هو المادة المراد إخفاؤها.

تهدف هذه التقنية إلى إخفاء معلومات داخل معلومات أخرى، بطريقة لا تؤدي إلى التأثير على المعلومات بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف الحقيقة، والغرض من عملية الإخفاء هذه أن لا يعلم المهاجم المحتمل عن وجود هذه البيانات، وبالتالي يتم حمايتها من القراءة أو التغيير عليها أو التدمير عن طريق هذا المهاجم.

❖ طرق إخفاء البيانات باستخدام طريقة ال Steganography

1. Least Significant Bit(LSB)

طريقة ال Bit الأقل أهمية، ويكون عمل هذه الطريقة بتبديل ال Bit الأقل أهمية في الملف وهذه المناطق من الملف تُستبدل بالمعلومات المراد إخفائها، أما من الخارج فلا يتم التعديل على الملف بشكل ملحوظ وهذا يعطي الأمان للشخص بإخفاء المعلومات في الملف مع التأكد أنه لا يمكن لأي إنسان آخر أن يكتشف وجود تغير في الملف.

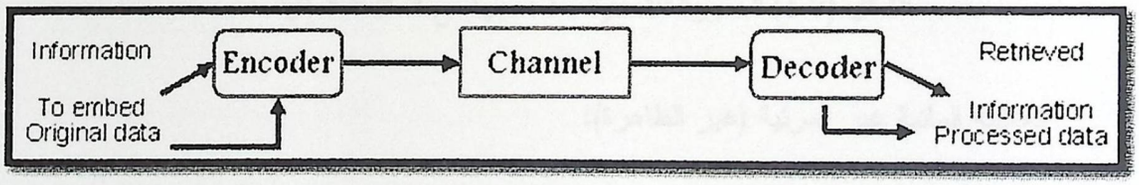
وتكون هذه الطريقة أكثر كفاءة عند استخدامها في ملفات الصور التي تمتلك درجة وضوح عالية وتستعمل العديد من الألوان المختلفة، كما أنها تكون مجدية بالملفات السمعية التي لها العديد من الأصوات المختلفة.

كما وتتميز طريقة ال Bit الأقل أهمية أنها لا تزيد حجم الملف حتى لا يتم ملاحظة أي تغير في الملف، ولكنها تعتمد على حجم المعلومات التي ستخفى داخل الملف.

2. العلامات المائية (Watermarks):

تعتبر العلامات الرقمية المائية من أهم التطبيقات التقنية وأكثرها استخداماً، وهي عبارة عن رسالة مخفية داخل صورة رقمية أو ملف صوتي أو ملف فيديو رقمي، ويتم تخزين هذه الرسالة (العلامة) داخل محتويات الملف ذاته فلا تحتاج لمساحة عالية لأن هذه الرسالة غالباً تكون صغيرة.

وبشكل عام فإنّ أي علامة مائية تحتوي على ثلاثة أجزاء رئيسية كما هي موضحة في الشكل التالي :



الشكل (1.5) آلية دمج العلامة المائية

❖ أنواع العلامة المائية:

1. العلامة المائية المرئية (الظاهرة):

تعتبر العلامة المائية المرئية (الظاهرة) أكثر قوة من العلامة غير المرئية لأنها ليست جزء من الصورة الأصلية ومن الصعب حذفها, فهي تظهر بشكل واضح إما أن تكون ملونة أو غير ملونة لتغطي مساحة واسعة من الصورة لحمايتها من الحذف دون التأثير على ملامح الصورة الأصلية .

ومن الأمثلة عليها شعار المحطات الفضائية، ويمكن استخدامها كدعاية للحفاظ على رابط قـــوي بين مالك الصورة والصورة، فهي تحافظ على حقوق الملكية وحقوق النسخ.

الشكل (1.6) الصورة الأصلية والعلامة المائية قبل الدمج

الشكل (1.7) الصورة الأصلية بعد دمجها مع العلامة المائية

2. العلامة المائية غير المرئية (غير الظاهرة):

هي النوع الثاني من العلامة المائية والهدف منها هو حماية الملكيـــة, ســـواء كـــان للـــشركة المصنعة أم للزبائن, حيث لا يمكن ملاحظتها لكن يمكن فكها عن طريق خوارزميات حـــسابية, وهـــي تحتوي على معلومات مخفية, فعند فك العلامة المائية يتطلب ذلك وجود كلمة مـــرور (Watermark key) .

أنواع ال Attacks للعلامة المائية:

1. Jitter Attack:

في هذا النوع يقوم المهاجم بعمل نفس العلامة المائية هدفها استبدال الbit التي تحدد العلامة المائية بواسطة "jitter".

2. Additive Noise:

في هذا النوع يقوم المهاجم بإضافة تشويش على الصورة, حتى يقوم بإيقاف Watermark detection Process, لأن كل pixel في الصورة لها حد معين من التشويش حتى تبقى غير مرئية.

3. Linear Filtering:

أما في هذا النوع عندما يريد المهاجم حذف العلامة المائية أو تدمير أي معلومات عن المالك, فإنه يقوم بتنقي العلامة المائية من الصورة ويعيد تخزين الصورة الأصلية, ممكن أن يؤدي هذا إلى تدمير المعلومات المخفية وذلك حسب درجة التعقيد لها.

3.البصمات الإلكترونية (Fingerprints):

البصمة الإلكترونية هي عبارة عن رقم سري أو سلسلة من الأحرف يتم اشتقاقها وفقاً لخوارزميات معينة تدعى اقتران (Hash Function)، إذ تطبق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة تمثل ملفاً كاملاً أو رسالة (سلسلة صغيرة)، والبيانات الناتجة من هذه البصمة الإلكترونية للرسالة تسمى (سلسلة كبيرة)، ويتم بعد ذلك إخفاؤها ضمن الوسائط الرقمية التي يمكن أن يوزع نسخ منها لعدد كبير من الزبائن، حيث يتمكن المالك أو المنتج للوسائط الرقمية من تحديد الزبون الذي انتهك حقوق النشر، عن طريق نسخ وإعادة توزيع هذه الوسائط وذلك عن طريق تضمين رقم سري أو سلسلة أحرف مختلفة من نسخة إلى أخرى.

تتكون البصمة الإلكترونية للرسالة من بيانات لها طول ثابت عادة يتراوح بين (128 bit- 160 bit)، حيث يؤخذ من الرسالة المحولة ذات الطول المتغير، ومن خلال هذه البصمة يتم تمييز

الرسالة الأصلية والتعرف عليها بدقة وإذا حصل أي تغيير في الرسالة مهما كان بسيطاً ولو كان في (bit) واحد سيفضي إلى بصمة مختلفة تماماً.

ومن غير الممكن اشتقاق البصمة الإلكترونية ذاتها من رسالتين مختلفتين، حيث تتميز البصمات الالكترونية عن بعضها بحسب المفاتيح الخاصة (Private Key) التي أنشأتها، ولا يمكن فك شفرتها إلا باستخدام المفتاح العام (Public Key) العائد إليها.

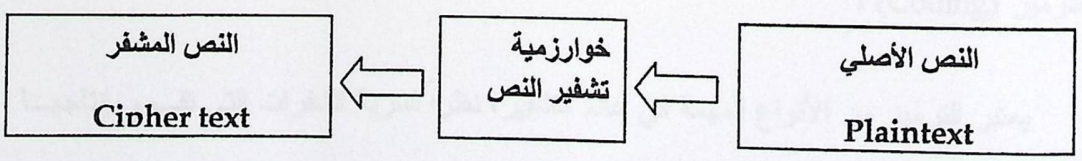
ظهرت الحاجة إلى البصمة الالكترونية للرسالة لأن طريقة التشفير بالرغم من قدرتها على منع الإطلاع على محتويات الرسالة، إلا أنه لا يمنع المخربين من العبث بها بمعنى أن التشفير لا يضمن سلامة الرسالة .

Cryptography 1.5.2

إن استخدام التشفير أو ما يطلق عليه (بالتعمية) قديماً لإخفاء المعلومات والمراسلات منذ الحضارة الفرعونية والدولة الرومانية.

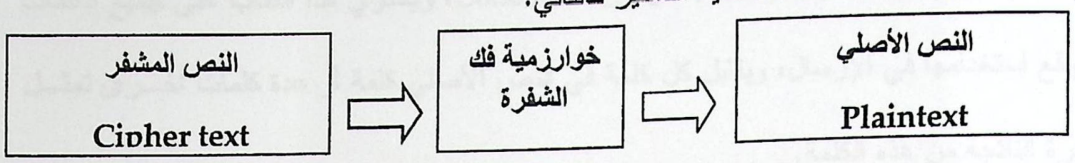
وقد شاع في أيامنا استخدام مصطلح التشفير دلالة على إخفاء المعلومات، وقد جاءت كلمة التشفير أصلاً من اللغة العربية ولكن بمعنى آخر لكلمة "الصفر"، حيث كان مفهوم الصفر جديداً وغريباً لدرجة أنهم أخذوه بنفس الإسم فأسموه cipher للدلالة على الأشياء المهمة والغامضة.

ومن هنا نتوصل أن التشفير هو تحويل المعلومات المهمة والسرية إلى نص لا يمكن فهمه من قبل الأطراف غير المقصودين.



الشكل (1.8) التشفير

ويتم فك التشفير بطريقة معاكسة لعملية التشفير كالتالي:



الشكل (1.9) فك التشفير

وكتطبيق بسيط يوضح هذا المفهوم، فمثلاً لتشفير كلمة Arab نجعل كل حرف يساوي الحرف الذي يليه، كالتالي:

A=B

R=S

A=B

B=C

وعندما يستلمها المستقبل يقوم بعكس التشفير، حيث يجعل كل حرف يساوي الحرف السابق له، وبـذلك يكون قد حصل على النص الأصلي.

تستخدم الكريبتوغرافي في معظم الحالات التي تكون فيها كمية المعلومات المطلوب حمايتهـا كبيرة، ولكن في هذه الطريقة يعلم المهاجم بوجود هذه البيانات، وقد يستطيع الوصول إليهـا، لكنـه لا يستطيع قراءتها إلا بعد كسر الشفرة، لكنه قادر على إزالتها أو العبث فيها وتغييرها إذا شك فيها مثلاً.

❖ بعض طرق التشفير (Cryptography)

1. الترميز (Coding) :

يعتبر الترميز من الأنواع المهمة في عالم التشفير، نظراً لسرية الشفرات التي تقـوم بإنتاجهـا هذه العملية وبالرغم من ذلك فهي تعتبر كبداية من أنواع التشفير، وبالتالي فهي لم تستخدم بشكل كبيـر وذلك لما تتطلبه من إنتاج لغة سرية، والإحتفاظ بها عند الأشخاص بأن تتم عملية الإرسال بينهم والنوع

الأشهر في الترميز ما يطلق عليه بكتاب الرموز Codebook، ويحتوي هذا الكتاب على جميع الكلمات المتوقع استخدامها في الإرسال، ويقابل كل كلمة في النص الأصلي كلمة أو عدة كلمات أخـــرى تمثـــل الشفرة الناتجة من هذه الكلمة.

وعند التشفير بهذه الطريقة كل ما علينا هو البحث في كتاب الرموز واستخراج الكلمة المقابلـــة للكلمة المراد تشفيرها، وهكذا نحصل على الكلمة الجديدة المشفرة بهذه الطريقة.

Codeword	Word
...	...
Computer	Dawn
...	...
Explode	Enemy
...	...
Lion	At
...	...
Run	Attack

الشكل(1.10) كتاب الرموز[4]

ولفك تشفير كلمة ما في Codeword ، كل ما علينا هو معرفة ما يقابلها في Word ، وبالتالي نحصل على الكلمة المطلوبة.

وتكمن سيئة كتاب الرموز أن كل كلمة يقابلها كلمة مشفرة، حيث كون من الممكن فك تشفيرها حتى لو أنها ليست واضحة ولكن قد يُستفاد منها بطريقة ما، لذلك استُخدم بـــدلاً منهـــا أرقـــام Code Number .

---

[4] Classical cryptography

ولأن كتاب الرموز حجمه كبير جداً حيث يحتوي على جميع الكلمات المتوقع استخدامها في عملية الإرسال، وفي بعض الأحيان تكون جميع الكلمات معروفة فيه، لذلك يكون مرتب بالترتيب الهجائي وبالتالي كل حرف يقابله رقم معين وهكذا...، وكتاب الترميز هذا يسمى (One Part-Code).

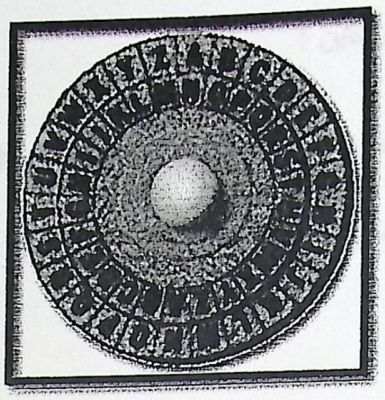
لكن كما هو ملاحظ يمكن لمهاجم الشفرة كسر هذه الرموز لأنه يعرف أن الحرف A دائماً أقل من الحرف Z وبقليل من المحاولات يتم كسرها، لذلك يتم اللجوء إلى (Two Part-Code) أي أن هنا يوجد كتاب للتشفير، وكتاب آخر مرتب بطريقة أخرى لفك التشفير وهكذا لا يمكن تخمين ما ينتجه الكتاب الأول.

وعلى الرغم من سرية هذه الطريقة لحد ما، إلا أنها غير مجدية تماماً وذلك نظراً لصعوبة الإحتفاظ لهذا الكتاب عند الطرفين، وفي حال تم استخدام (Two Part-Code)، سنحتاج إلى كتابين عند كل طرف حتى يستطيعوا إرسال واستقبال الرسائل فيما بينهم، مع الأخذ بعين الإعتبار الصعوبة في إرسال الكتاب إلى الطرف الآخر والتأكد أنه لا يوجد أي أحد يملك نسخة منه، بالإضافة إلى صيانته من إضافة كلمات جديدة عليه والتعديل عليه وإرسالها إلى الطرف الآخر.

2. شفرة قيصر Caesar :

وهي من أحد أشهر أنواع التشفير الكلاسيكي، حيث تتميز ببساطتها ولكن يعيبها سهولة كسر الشفرة الناتجة ببساطة، حيث أننا نقوم بتبديل كل حرف بثالث حرف بعده، (وهو دائماً يكون 3 في شفرة قيصر) مع النص الأصلي، ويكون هو الحرف الأول في النص المشفر، وهكذا يكون الحال بالنسبة لباقي الحروف.

وفي حال كان الحرف هو الحرف الأخير في الأبجدية نقوم بالرجوع إلى بداية الحروف (حيث تكون على شكل دائرة)، كما هو موضح بالشكل التالي:



الشكل (1.11) شفرة قيصر الدائرية[5]

والشكل التالي يوضح عملية ترتيب الحروف وما يقابلها مشفرة:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

الشكل (1.12) شفرة قيصر[6]

مثال : لتشفير النص التالي FIRE MISSILE

لأن وضع الحروف المشفرة على نفس ترتيب الحروف في النص الأصلي يسهل من عملية تخمين الكلمة، فإننا نضع النص المشفر على شكل block ، أو مجموعات كل منها يتكون من 5 حروف كما جرت العادة.

والآن بعد وضع النص المشفر على شكل مجموعات كل منها يتكون من خمسة حروف فيكون الناتج كالآتي: ILUHPLVVLO H

وهكذا أصبح النص أكثر تعقيداً لكاسر الشفرة ، ولكن تبقى خوارزمية قيصر ضعيفة جداً.

---

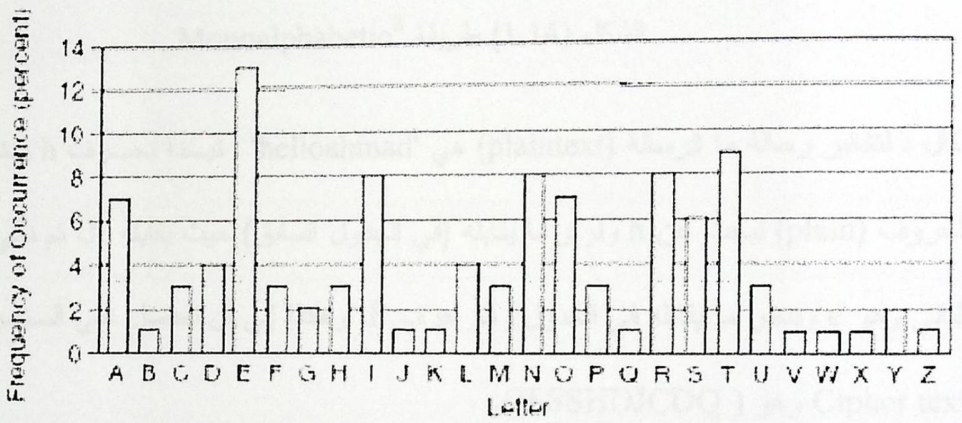
[5] كتاب أمن المعلومات

[6] كتاب أمن المعلومات

ويمكن فك تشفير شفرة قيصر بطريقتين :

- بطريقة عكسية لطريقة التشفير وهو طرح ثلاثة أحرف من كل حرف في النص المشفر وبالتالي نحصل على النص الأصلي.
- التحليل الإحصائي :

يتم استخدام طريقه التحليل الإحصائي لكسر شفرة قيصر، حيث نقوم بالنظر في النص المشفر ونلاحظ الحرف الأكثر تكراراً في النص، إذ أن الحرف الأكثر تكراراً في اللغة الإنجليزية هو حرف E (كما يبين الرسم البياني القادم)، بعدها قد يكون هذا الحرف في النص المشفر هو الأكثر تكراراً.



الشكل (1.13) معدل تكرارات الحروف في اللغة الانجليزية[7]

3. طريقة Monoalphabetic :

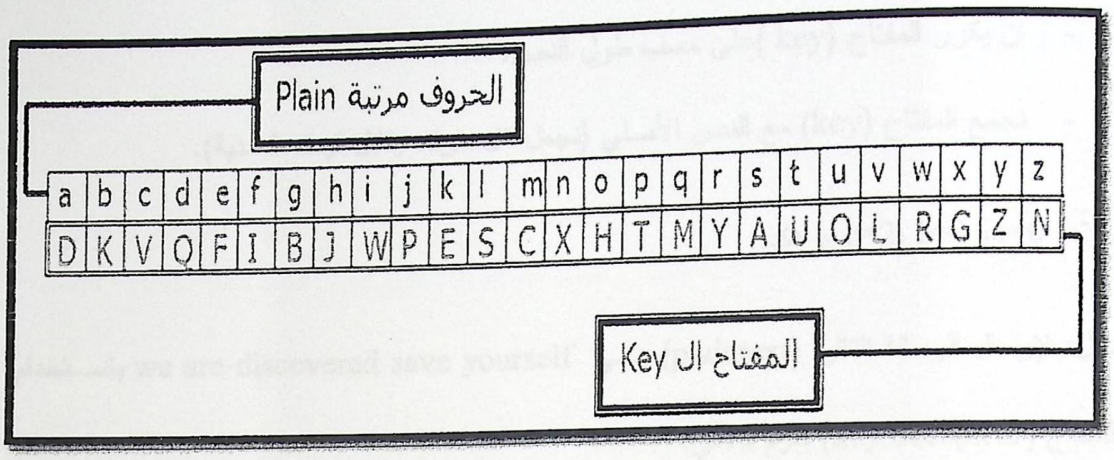
تعتمد فكرة هذه الطريقة أن يكون لدينا مفتاح key ونقوم بتبديل النص الأصلي بالمفتاح Key، وهي أفضل من طريقة Caesar لأن المفتاح متغير يتم إختياره بشكل عشوائي وليس له قاعدة، ويتم توزيع الحروف بشكل متباعد.

---

7 كتاب أمن المعلومات

شرح الطريقة:

لدينا الأحرف من (a-z) كما هو موضح بالشكل التالي:



الشكل (1.14) طريقة Monoalphabetic[8]

مثال : لتشفير رسالة ما الرسالة (plaintext) هي "helloahmad" , نبدأ بحرف h وننظر إلى الحروف (plain) نبحث عن h ونرى ما يقابله (في الجدول السابق) حيث يقابله J، ثم نأتي إلى الحرف التالي وهو e وننظر ما يقابله في الجدول وهو حرف F، وهكذا إلى أن نحصل على النص المشفر Cipher text وهو (JFSSHDJCDQ).

كسر شفرات Monoalphabetic :

طريقة التحليل الإحصائي هي الطريقة الشائعة لمثل هذه الطرق (حيث تستبدل هذه الطرق كل حرف في الشفرة الأصلية بحرف ما اعتماداً على إزاحة معينة – مفتاح ما– أو جملة للتشفير)، ولفك تشفير هذه الطريقة يجب أن يكون هناك نص كافي للبدء في مرحلة العد, أي أن النص إذا كان يتكون من 10 حروف أو اقل فإنه يصعب جداً كسره بهذه الطريقة.

---

8 كتاب أمن المعلومات

4. طريقة Vigenere :

في هذه الطريقة نقوم بوضع مفتاح (key) للنص على أن يطبق الشروط التالية:

- أن يكرر المفتاح (key)على حسب طول النص.
- نجمع المفتاح (key) مع النص الأصلي (نجعل كل حرف يقابل قيمته العددية).

مثلاً: a=0، b=1، c=2، وهكذا.

مثال: لإرسال الرسالة التالية (plaintext) هـــي we are discovered save yourself باســـتخدام المفتاح (key deceptive) نقوم بالآتي:

Key: deceptivedeceptivedeceptive

Plaintext: wearediscoveredsaveyourself

d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J

الشكل (1.15) طريقة Vigenere[9]

- نجمع المفتاح (key) على طول النص الأصلي.
- نجمع كل حرف من النص الأصلي مع الحرف الذي يوازيه من حروف المفتاح (key) حيـــث d+w تساوي 22+3 = 25 وهو حرف Z أي أن حرف Z=d+w، وكـــذلك e+e تـــساوي 4+4 = 8 وهو حرف I.

---

[9] كتاب أمن المعلومات

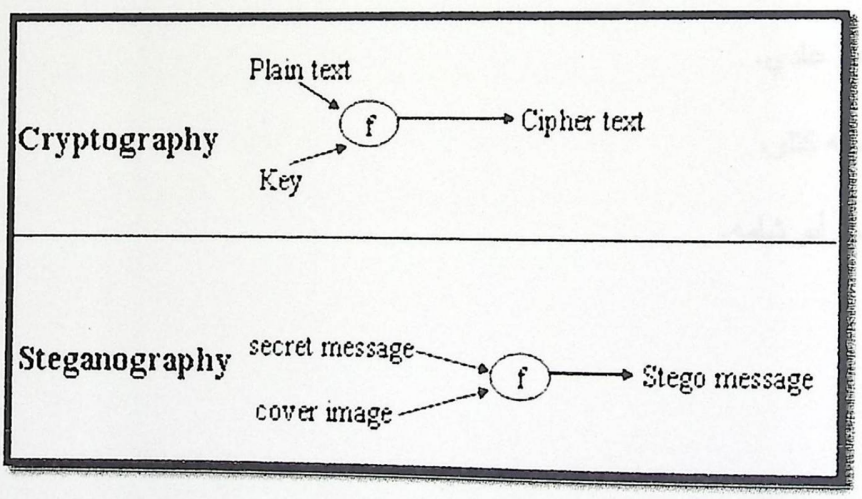
وبعد تشفيرها يصبح النص ZICVTWQNGRZGVTWAVZHCQYGLMGJ

كسر شفرة Vigenere:

النص الأصلي = النص المشفر – الحرف الموازي له من المفتاح (key).

الفرق بين ال Steganography و ال Cryptography :

هناك فرق كبير بين إخفاء المعلومات وتشفيرها، ففي الإخفاء تكون المعلومات مخفية, بحيث المستخدم العادي لن يكون على معرفة وعلم بوجود تلك المعلومات وحتى يستطيع معرفة وجود الرسالة يجب معرفة الوسط المخفي فيه أولاً، أما في التشفير فإن المستخدم يكون على علم بأن هناك معلومة مخفية ولكنها مشفرة غير مفهومة ومن الممكن اعتراض هذه المعلومة وتفسيرها. ولذا فإن أنسب طريقة لبناء نظام حماية قوي، هو الإعتماد على التقنيتين لجعل عملية اختراق النظام أكثر تعقيداً.



الشكل (1.16) المقارنة بين التشفير والإخفاء[10]

[10] [JOH 1998]

1.6 النتائج المتوقعة:

يفترض بعد اكتمال هذا المشروع وجود :

- واجهة خاصة للمرسل بحيث يقوم المرسل بتحديد الصورة المراد الإخفاء بداخلها، ومن ثم تحديد الرسالة المراد إخفائها , ثم يتم دمج الرسالة داخل الصورة بالإعتماد على الطريقة التي تم إختيارها وفي النهاية بإمكانه معاينة الصورة لمشاهدة النتيجة.
- واجهة أخرى للمستقبل بحيث يحدد المستقبل الصورة المدمج بداخلها الرسالة, فمن خلال البرنامج يتم استخراج الرسالة المدمجة.

1.7 فريق العمل:

يتكون فريق العمل من ثلاث طالبات:

- رهام عادي.
- ساميه كتلو.
- فاديه أبو شامه.

الفصل الثاني

2.1 المقدمة

2.2 شرح طرق في الإخفاء

2.1 المقدمة:

يوجد العديد من الأبحاث عن إخفاء المعلومات داخل الصور, وهناك عدة طـرق اسـتُخدمت للإخفـاء, وسيتم في هذا الفصل توضيح بعضها.

2.2 شرح طرق الإخفاء:

يتم تمثيل الصورة على شكل قيم مرتبة داخل مصفوفة وكل قيمة تمثل Pixel المكـون مـن 3Byte, حيث يمثل كل Byte قيمة لون من ألوان RGB (Red, Green, Blue) كما يلي:

Pixel ⇨ 11111000 11001001 00000011

أزرق(3) أخضر(201) أحمر(248)

يتم تحديد تدرجات RGB حسب نـوع الـصورة المـستخدمة فمـثلا" فـي الـصورة مـن نـوع 8bit_bitmap فإن كل لون له 2^8=256 تـدرج, أمـا فـي حالـة اسـتخدام الـصور مـن نـوع 24bit_bitmap فإن كل لون له 2^{24} = 16777216 تدرج.

وبناء على ذلك فإنه يتم استخدام الصور من نوع 24bit_bitmap في هذه الطرق لأن جودة الإخفـاء في هذه الصور أفضل من غيرها, وبسبب حجمها الكبير فإنها توفر مساحة أكبر للإخفاء, ولكن عمليـة النقل والتحميل (Transfer, Upload) تكون بطيئة, مما تثير الانتبـاه مـن قبـل ال "Attacker" بسبب حجمها غير العادي, لذلك نحتاج إلى آلية ضغط (Compression) لتقليل حجم الصورة ولكـن من الممكن أن تؤثر على الرسالة المخفية. [11].

---

[11] [JOH 1998]

2.2.1 شرح الطريقة الأولى ((Least Significant Bit (LSB 8 Bit):

في هذه الطريقة يتم تحويل الرسالة إلى النظام ASCII ثم إلى النظام ال Binary ليتم قـراءة الByte من المفتاح وقراءة الByte من الرسالة المراد إخفائها وعمل XOR بينهما بحيث تكون النتيجة رسالة مشفرة يتم إضافتها على آخر Bit من كل Pixel وفي هذه الطريقة لا يلاحظ تأثير على ملامح الصورة لأنه يتم التعديل على درجة واحدة من لون Pixel .

فمثلاً لإخفاء الرسالة(abcdef) باستخدام المفتاح(9657852) :

abc= 01100001 01100010 01100011

def=01100100 011001101 01100110

9657852=10010011 01011101 11111100

Result abc XOR 9657852=01100001 01100010 01100011

XOR

10010011 01011101 11111100

11111110 00111111 10011111

لأن الرسالة أطول من المفتاح نحتاج إلى تكرار المفتاح:

Result def XOR 9657852= 01100100 011001101 01100110

XOR

10010011 01011101 11111100

11110111 00111000 10011010

Encrypted message=11111110 00111111 10011111 11110111 00111000

10011010

توضيح كيفية الإضافة على آخر Bit من كل Pixel:

فمثلاً لإخفاء حرف " I " حيث يمثل في (Ascii =73), (Binary 01001001)

نحتاج إلى 8 Pixel من الصورة وهي فرضاً كالتالي:

Pixel (1) ⟶	11000101 10011010 00001010
Pixel (2) ⟶	11000101 10011010 00001010
Pixel (3) ⟶	11000101 10011010 00001010
Pixel (4) ⟶	11000101 10011010 00001010
Pixel (5) ⟶	11000101 10011010 00001010
Pixel (6) ⟶	11000101 10011010 00001010
Pixel (7) ⟶	11000101 10011010 00001010
Pixel (8) ⟶	11000101 10011010 00001010

ويتم إخفاء حرف I(01001001) كما يلي:

- يتم تخزين أول Bit وهو "1" في الموقع (7.0)، فيصبح ال Pixel الثامن في الصورة الأصلية:

11000101 10011010 00001011

- يتم تخزين ثاني Bit وهو "0" في الموقع (6,0)، فيصبح الPixel السابع في الصورة الأصلية:

11000101 10011010 00001010

- يتم تخزين ال Bit الثالث وهو "0" في الموقع (5,0)، فيصبح ال Pixel السادس في الصورة الأصلية :

11000101 10011010 00001010

- يتم تخزين ال Bit الرابع وهو "1" في الموقع (4,0)، فيصبح الPixel الخامس في الصورة الأصلية:

11000101 10011010 00001011

- يتم تخزين ال Bit الخامس وهو "0" في الموقع (3,0)، فيصبح الPixel الرابع في الصورة الأصلية:

11000101 10011010 00001010

- ثم يتم تخزين ال Bit السادس وهو "0" في الموقع (2,0)، فيصبح ال Pixel الثالث في الصورة الأصلية:

11000101 10011010 00001010

- يتم تخزين ال Bit السابع وهو "1" في الموقع (1,0)، فيصبح ال Pixel الثاني في الصورة الأصلية:

11000101 10011010 00001011

- يتم تخزين ال Bit الثامن وهو "0" في الموقع (0,0)، فيصبح ال Pixel الأول في الصورة الأصلية:

11000101 10011010 00001010

وعند الإنهاء من إخفاء الرسالة كاملة يتم إنشاء صورة من نوع Bitmap تحتوي على الرسالة المخفية.

عملية الاسترجاع:

لاسترجاع الرسالة التي تم إخفائها في الصورة، سيتم ذلك بخطوات عكسية للعملية التي تم إخفاء الرسالة بها.

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (0,0) :

11000101 10011010 00001010

فنأخذ آخر Bit وهو"0".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (1,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "1".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (2,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "0".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (3,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "0".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (4,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "1".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (5,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "0".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (6,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "0".

- يتم استرجاع ما تم تخزينه في ال Pixel الموجود في الموقع (7,0) :

11000101 10011010 0000101

فنأخذ آخر Bit وهو "1".

وبعد الإنهاء من استرجاع الرسالة (01001001) يتم التحويل إلى (Ascii =73)

حيث يقابل 73 حرف "I".

✓ مزايا استخدام الطريقة:

1. لا تؤثر على حجم الصورة بعد إخفاء الرسالة بداخلها.
2. لا تؤثر على ألوان وملامح الصورة.

✓ سيئات استخدام الطريقة:

1. حجم الرسالة المراد إخفائها محدود، وبالتالي من الصعب إخفاء رسالة طويلة.
2. يتم استخدام آلية الضغط من نوع Lossless بسبب الحجم المحدود للرسالة المخفية، وهذا النوع من الضغط يؤدي إلى ضياع جزء من الرسالة المخفية.[12]
3. يجب مراعاة الدقة والعناية عند اختيار الصورة المراد دمج الرسالة بداخلها بسبب محدودية الحجم المتاح للإخفاء.

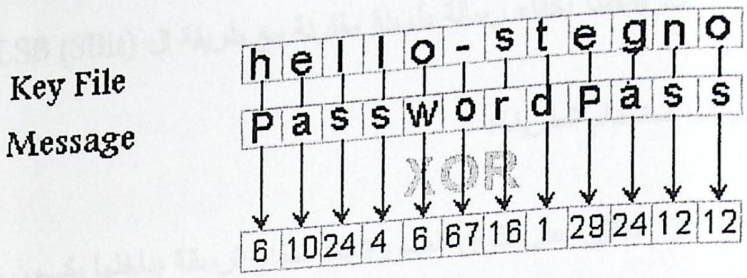
2.2.2 شرح الطريقة الثانية ((Least Significant Bit (LSB 24 Bit):

لإخفاء رسالة نختار صورة من نوع 24 bit_bitmap, ونختار ملف من أي نوع ليكون ملف المفتاح المتفق عليه بين المرسل والمستقبل, وكذلك يتم اختيار الرسالة المراد إخفائها, حيث يتم قراءة الByte الأول من الرسالة وبالمقابل قراءة الByte الأول من ملف المفتاح وعمل XOR بينهما , والقيمة الناتجة تستخدم في تحديد المسافة بين 2 Pixel المراد الإخفاء داخلهما فإذا كان طول ملف المفتاح أقصر من الرسالة فإنه يقوم بتكرار ملف المفتاح, ويستخدم أيضاً ملف المفتاح لتشفير الرسالة المخفية حتى لا يتمكن أي طرف غير مقصود من الوصول إلى الرسالة وإذا شك بوجود رسالة فلا يتمكن من استخراجها إلا بوجود ملف المفتاح, وكلما كان ملف المفتاح أطول كانت جودة الإخفاء أفضل لأن التأثير الظاهر على الصورة أقل انتظاماً بسبب تكرار المفتاح بعد مسافة أطول.

وتكرر هذه العملية على كل Byte للرسالة المراد إخفائها.

---

[12] Implementation of Improved Steganographic Technique for 24-bit Bitmap Images in Communication



الشكل (2.1) مثال يوضح عملية XOR[13]

إن الناتج من عملية XOR يكون رسالة مشفره يتم إخفائها بدلاً من الرسالة الأصلية وذلك لزيادة الأمن على الرسالة المراد إخفائها(كما تم توضيحه في الطريقة الأولى), حيث يتم الإخفاء بالاعتماد على(LSB(24Bit، ويكون ذلك بالتعديل على اخر Bit من كل Byte في ال Pixel الذي تم تحديده من خلال الناتج من عملية XOR, وبذلك يتم تغير لون ال Pixel بالاعتماد على القيم الجديدة .

أما في عملية استخراج الرسالة التي تم إخفائها فإنه يحدث عكس عملية الإخفاء حيث نقوم بتحديد ملف الصورة المدمج بداخلها الرسالة, ومن ثم تحديد ملف المفتاح المتفق عليه بين المرسل والمستقبل ليتم قراءة ال Byte منه حتى يحسب موقع ال Pixel التالي لمعرفة لونه وبعدها يقرأ قيمة (R.G.B) التي تم تعديلها على القيم الأصلية ويضعها في ملف الرسالة الناتج من عملية الاستخراج.

✓ مزايا استخدام الطريقة:

1. صعوبة الوصول إلى الرسالة المخفية من قبل الشخص غير المقصود لأنه تم استخدام ملف المفتاح الذي يقوم بتشفير الرسالة, وبالتالي لا يمكن استخراج الرسالة إلا بوجود ملف المفتاح.
2. في الصورة التي يكون فيها ألوان كثيرة يكون التأثير الظاهر عليها غير واضح بعد الإخفاء, فلا يمكن الشك في وجود رسالة مخفية.

---

[13] [JOH 1998]

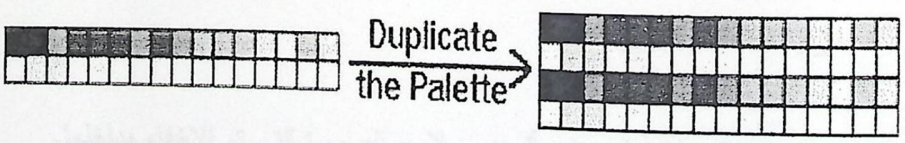
3. يمكننا إخفاء رسالة طويلة مقارنة مع طريقة ال LSB (8Bit).

✓ سيئات استخدام الطريقة:

1. التأثير على الوان الصورة بعد اخفاء الرسالة بداخلها يكـون مرئـي لعـين الإنسان المجردة.
2. تقلل من جودة الصورة بشكل كبير عندما يتم إخفاء معلومات الرسالة السرية بداخلها وخاصة الصور ذات الجودة العالية.
3. تؤثر على حجم الصورة بعد الإخفاء.

2.2.3 شرح الطريقة الثالثة:

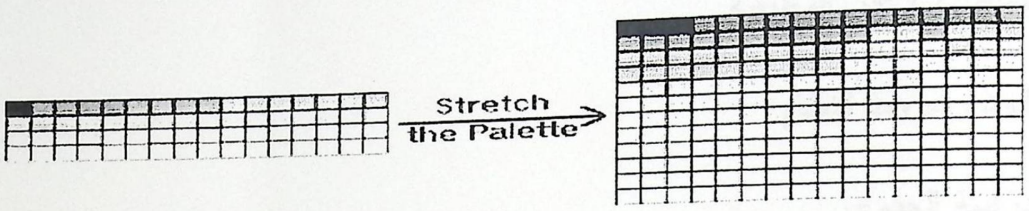
يتم الإخفاء في هذة الطريقة بالإعتماد على ال Palette الاصلية للصورة المراد الإخفـاء بداخلها(Palette مجموعة الالوان في الصورة ولا تحتوي على الالوان المكررة), نحتاج الى زيادة حجم ال Palette لتصبح كافية لإخفاء عد اكبر من ال Byte, فعند مـضاعفة ال Palette عن طريق عن طريق نسخ الالوان , فانه يوجد مشكلة في انها تكون واضحة مما يؤدي الى اكتشافها بسهولة .



الشكل (2.2):عملية مضاعفة ال Palette .

لحل مشكلة مضاعفة ال Palette نقوم بانشاء New Palette يكون فيها في البداية نـسخة عـن ال Palette الاصلية, وبعد ذلك نأخذ كل Pixel من ال Palette الاصلية ونفحص قيمة الون الازرق فيه, فاذا كانت القيمة زوجية فانها تكون موجودة في ال New Palette, اما اذا كانت القيمـة فرديـة

فنجعلها زوجية ونضيفها الى New Palette, ونضيف لكل لون موجود في الNew Palette لون قريب منه بجعل قيمة اللون الأزرق فردية ويكون هذا اللون هو لون مضاف.وبذلك تكون الالوان الاصلية قيمة الون الازرق فيها زوجي والالوان المضافة تكون قيمة الون الازرق فردي, فإذا كانت قيمة الرسالة المراد إخفائها (0) فإنه يتم اخفائها في اللون الأصلي في ال New Palette، أما إذا كانت قيمة الرسالة المراد إخفائها (1) فإنه يتم اخفائها في الألوان المضافة, وتسمى هذه العملية Stretch Palette.



االشكل(2.3):صورة توضح عملية Stretch the Palette

ان عملية إستخراج الرسالة التي تم إخفائها تكون سهلة بسبب وجود Palette واحدة, بالإضافة الى ملف ال key الذي تم تحديده, الذي يقوم بتحديد المسافة بين Pixel_2 التي تم الإخفاء فيهما, فإذا كانت قيمة اللون الأزرق من ال Pixel زوجية فإن قيمة الرسالة المخفية(0), أما إذا كانت قيمة اللون الأزرق من ال Pixel فردية فإن قيمة الرسالة المخفية (1) .

- ✓ مزايا استخدام الطريقة:

1. لا تؤثر على ألوان وملامح الصورة التي تم الإخفاء بداخلها.
2. صعوبة الوصول إلى الرسالة المخفية من قبل الشخص غير المقصود لأنه تم استخدام ملف المفتاح , فلا يمكن استخراج الرسالة إلا بوجوده.

- ✓ سيئات استخدام الطريقة:

1. تؤثر على حجم الصورة بعد الإخفاء .

الفصل الثالث

تخطيط النظام

3.1 المقدمة

3.2 المتطلبات الوظيفية

3.3 المتطلبات غير الوظيفية

3.4 قيود وشروط النظام

3.5 دراسة الجدوى

3.6 جدولة الفترة الزمنية

3.7 توزيع المهام على الوقت

3.1 المقدمة

في هذا الفصل سيتم وصف وشرح المتطلبات الوظيفية بشكل مفصل, بالإضافة إلى شرح المتطلبات غير الوظيفية, ودراسة مصادر النظام وتوضيح القيود والشروط , ودراسة الجدوى الإقتصادية, وتوضيح المخاطر التي من المتوقع أن تواجهنا ودراسة وتوزيع المهام على الوقت.

يشمل هذا النظام مجموعة من المتطلبات تصنف كمتطلبات وظيفية وغير وظيفية، وسوف يتم توضـــيح ذلك من خلال النقاط التالية:

3.2 المتطلبات الوظيفية:

وهي المتطلبات التي تصف وظائف النظام والخدمات التي يقدمها, وتتعلـــق بالنظـــام بـــشكل مباشر, وتقسم المتطلبات الوظيفية إلى قسمين، متطلبات وظيفية للمرسل ومتطلبات وظيفية للمستقبل.

1. المتطلبات الوظيفية الخاصة بالمرسل:
    1. تحديد الطريقة التي بناءً عليها يتم دمج الرسالة.
    2. اختيار الصورة المراد دمج الرسالة بداخلها.
    3. تحديد نوع الرسالة المراد دمجها (نص, صورة).
    4. اختيار المفتاح .
    5. دمج الرسالة وإخفائها.

2. المتطلبات الوظيفية الخاصة بالمستقبل:
    1. اختيار الصورة المدمج بداخلها الرسالة.
    2. تحديد اسم وامتداد ومكان الملف المراد حفظ الرسالة فيه.
    3. اختيار المفتاح.
    4. استخراج الرسالة المدمجة من الصورة.

3.3 المتطلبات غير الوظيفية:

1. بيئة العمل :

- هذا البرنامج عبارة عن واجهتين إحداهما لمرسل الرسالة (Hide)، والأخرى لمستقبل الرسالة (Extract), حيث يُمكّن المرسل من إخفاء رسالة داخل صورة والمستقبل يقوم باستخراج الرسالة من الصورة .
- أن يؤدي الهدف المطلوب منه بطريقة سهلة ومفهومة للمرسل والمستقبل .
- أن يكون النظام متوفر لدى المرسل والمستقبل حيث يتمكن من إخفاء واستخراج الرسالة في أي مكان وزمان .

2. واجهة التطبيق :

أن تكون الواجهة بسيطة تُمكّن المستخدم باختلاف مهاراته وخبراته من التعامل مع النظام بسهولة, واستخدام ألوان مريحة للعين .

3. الدقة :

تتمثل الدقة في عملية دمج الرسالة داخل الصورة دون التأثير على ألوان الصورة الأصلية بشكل واضح.

3.4 قيود وشروط النظام:

1. ضيق الوقت بالنسبة لفريق العمل وذلك لأن مدة إنهاء المشروع فصلاً دراسياً واحداً (14 أسبوع).
2. التكاليف يجب أن تكون ضمن الميزانية المخطط لها .
3. أن يكون النظام قابل للتطوير والصيانة .

3.5 دراسة الجدوى:

مصادر وتكاليف النظام:

يحتاج هذا النظام إلى مجموعة مصادر تطويرية وتشغيلية , وهي كما يلي:

- المصادر التطويرية وتشمل :

1. المصادر البشرية : يحتاج هذا النظام إلى محلل ومبرمج، وهم مسؤولون عن تحليل هذا النظام وبرمجته, ولا بُدّ أن تتوفر لديهم الخبرة الكافية في لغات البرمجة.

الجدول رقم 3.1 يبين المصادر البشرية المستخدمة حيث يتم تحديد عدد الأشخاص والتكلفة الشهرية للشخص الواحد.

المصدر البشري	العدد	التكلفة الشهرية
محلل النظام	1	700 $
مبرمج النظام	1	700 $

الجدول (3.1) المصادر البشرية

تكاليف التطوير البشرية لمحلل النظام في الفترة المتوقعة لتحليل النظام وهي لمدة شهر(700$).

تكاليف التطوير البشرية لمبرمج النظام في الفترة المتوقعة لبرمجة النظام وهي لمدة ثلاثة اشهر (700$ * 3= 2100$).

1. المصادر الفيزيائية : يوضح الجدول التالي المصادر الفيزيائية المستخدمة في النظام، ومواصفات وتكلفة كل مصدر. [14]

[14] http://www.zap.co.il/search.aspx

المصدر الفيزيائي	المواصفات	التكلفة
جهاز حاسوب	معالج :Dual-Core 2.16 GHz ذاكرة بحجم : 1024 MB قرص صلب بحجم: 160 G DVD _Writer :CD_ROM شاشة: 17 بوصة لوحة مفاتيح وفأرة.	1000 $
Flash Memory	512 MB	10 $
المجموع		1010 $

الجدول (3.2) المصادر الفيزيائية

2. المصادر البرمجية : يوضح الجدول التالي المصادر البرمجية وتكلفة كل مصدر[15].

المصدر البرمجي	التكلفة
Microsoft Windows XP Professional	156 $
Microsoft office 2007	265 $
Microsoft Visio 2007	180 $
Microsoft Visual Studio.Net 2005	38 $
المجموع	639$

الجدول (3.3) التكاليف البرمجية

[15] www.spiritus.co.il/info

التكاليف الكلية التطويرية وتشمل تكاليف بشرية و فيزيائية وبرمجية خلال فتـــرة العمـــل المتوقعـــة (3 شهور), كما هو موضح في الجدول التالي:

التكاليف البشرية	التكاليف الفيزيائية	التكاليف البرمجية	المجموع
2800 $	1010 $	639$	4449 $

الجدول (3.4) التكاليف التطويرية

- المصادر التشغيلية وتشمل :

1. المصادر الفيزيائية : يوضح الجدول التالي التكلفة التشغيلية للمصادر الفيزيائيـــة اللآزمـــة لعملية تشغيل النظام .

المصدر الفيزيائي	المواصفات	التكلفة
Personal Computer	معالج : Pentium IV 1200 MHz. ذاكرة بحجم : 1 G. قرص صلب بحجم: 20 G.B. شاشة: 15 بوصة. لوحة مفاتيح وفأرة.	350 $
المجموع		350 $

الجدول (3.5) التكاليف التشغيلية للمصادر الفيزيائية

2. المصادر البرمجية : يوضح الجدول التالي التكلفة التشغيلية للمصادر البرمجيـــة اللازمـــة لعملية تشغيل النظام .

المصدر البرمجي	المواصفات	التكلفة
Microsoft Windows XP Professional	156 $	156 $
المجموع		
156 $		

الجدول (3.6) التكلفة التشغيلية للمصادر البرمجية

التكلفة الكلية التشغيلية وتشمل التكلفة البرمجية والفيزيائية كما موضح في الجدول التالي:

التكاليف الفيزيائية	التكاليف البرمجية	المجموع
350 $	156 $	506 $

الجدول (3.7) التكاليف التشغيلية

وبناء على التكاليف السابقة ستكون التكلفة الإجمالية للمشروع هي:

التكلفة التطويرية + التكلفة التشغيلية = 4449$ + 506 $ = 4955 $

3.6 جدولة الفترة الزمنية:

في هذا الجزء سيتم عرض الزمن المتوقع استغراقه في كل مرحلة من مراحل بنـــاء النظـــام، والجدوال (3.8) يعرض جدولة الوقت لكل مرحلة من مراحل بناء النظام ويبين بأنه يوجد تداخل ما بين هذه المراحل، حيث يوجد تداخل ما بين التوثيق وباقي مراحل بناء النظام.

المهام (Tasks)	المدة اللازمة/ الأسبوع	الرمز	الإعتمادية
المقدمة	2	T1	—
شرح طرق في الإخفاء	3	T2	—
التخطيط للنظام	2	T3	T1
تحليل النظام	2	T4	T2
تصميم النظام	1	T5	T2,T3,T4
برمجة وتطوير النظام	4	T6	T5,T4,T3,T2
فحص النظام	1	T7	T6
النتائج والتوصيات	2	T8	T4,T6
التوثيق	16	T9	T1,T2,T3,T4, T5,T6,T7,T8,T9

الجدول(3.8) الوقت المتوقع لكل مرحلة من مراحل بناء النظام

3.9 مخطط سير العمليات: (مخطط سير العمليات التطويريةGANT CHART)

الجدول 3.9 يبين الوقت المتوقع مع الوقت الفعلي لإنجاز هذا العمل كاملاً.

المهمة	الوقت بالأسبوع													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
المقدمة														
شرح طرق في الإخفاء														
التخطيط للنظام														
تحليل النظام														
تصميم النظام														
برمجة وتطوير النظام														
فحص النظام														
النتائج والتوصيات														
التوثيق														

الجدول(3.9) الوقت الفعلي والمتوقع لإنجاز المهام(Gant Chart)

الوقت المتوقع. الوقت الفعلي.

الفصل الرابع

تحليل متطلبات النظام

4.1 المقدمة

4.2 متطلبات النظام:

4.2.1 متطلبات النظام الوظيفية.

4.2.2 متطلبات النظام غير الوظيفية.

4.3 مخطط محتوى النظام (Context Diagram)

4.4 مخطط تدفق البيانات (Data Flow Diagram)

4.1 المقدمة:

تعتبر مرحلة تحليل المتطلبات من الخطوات المهمة والأساسية لتطـــوير وإكمـــال أي نظام، وفي هذا الفصل سيتم تحليل المتطلبات الوظيفية وغير الوظيفية وتوضيح مخطط محتوى النظام وكذلك مخطط تدفق البيانات.

4.2 متطلبات النظام:

يشمل هذا النظام مجموعه من المتطلبات، وتقسم إلى متطلبات وظيفية وغير وظيفيـــة وسيتم تحليلها:

تحليل المتطلبات الوظيفية الخاصة بالمرسل:

1. تحديد الطريقة التي بناءً عليها يتم دمج الرسالة.

الوظيفة	تحديد الطريقة التي بناءً عليها يتم دمج الرسالة.
الوصف	يقوم المرسل بتحديد الطريقة التي يعتمد عليها في تحديد طريقة دمـــج الرســـالة داخل الصورة.
المدخلات	الطريقة المراد دمج الرسالة بالأعتماد عليها.
المصدر	واجهة النظام.
المخرجات	تحديد الطريقة المعتمدة في آلية الدمج داخل الصورة.
الهدف	تحديد الطريقة التي بناءً عليها يتم دمج الرسالة.
المتطلبات	لا شيء.
شروط قبل التنفيذ	لا شيء.
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المرسل بالدخول على واجهة النظام ، ومن ثم يقوم بتحديد الطريقة المعتمدة في دمج الرسالة داخل الصورة .

2. اختيار الصورة المراد دمج الرسالة بداخلها.

الوظيفة	تحديد الصورة المراد دمج الرسالة بداخلها.
الوصف	يقوم المرسل بتحديد الصورة التي يريد دمج الرسالة بداخلها.
المدخلات	الصورة الأصلية.
المصدر	الواجهة الخاصة بالمرسل(Hide)
المخرجات	عرض الصورة المراد دمج الرسالة بداخلها.
الهدف	تحديد الصورة المراد دمج الرسالة بداخلها.
المتطلبات	نوع الصورة (Bitmap) .
شروط قبل التنفيذ	لا شيء.
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المرسل بتحديد الطريقة التي يعتمد عليها في تحديد طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهه الخاصة بعمل Hide ، يقوم بتحديد الصورة التي يريد دمج الرسالة بداخلها من نوع Bitmap .

3. تحديد نوع الرسالة المراد دمجها (نص, صورة).

الوظيفة	تحديد نوع الرسالة المراد دمجها (صورة، نص).
الوصف	يقوم المرسل باختيار نوع الرسالة التي يريد دمجها داخل الصورة سواء كانت صورة أو نص.
المدخلات	نوع الرسالة (نص أو صورة).
المصدر	الواجهة الخاصة بالمرسل(Hide).
المخرجات	لا شيء.
الهدف	تمكين المرسل من تحديد نوع الرسالة المراد دمجها.
المتطلبات	لا شيء.
شروط قبل التنفيذ	الملف النصي من نوع txt. الصورة من نوع Bitmap.
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المرسل بتحديد الطريقة التي يعتمد عليها في تحديد طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهه الخاصة بعمل Hide يختار نوع الرسالة التي يريد دمجها داخل الصورة سواء كانت صورة أو ملف نصي .

4. اختيار المفتاح.

الوظيفة	اختيار المفتاح .
الوصف	يقوم المرسل باختيار ملف واضافته من اجل حماية الرسالة المخفية من الوصول اليها من أي طرف غير مقصود حيث يكون هذا المفتاح متفق عليه من قبل المرسل والمستقبل.
المدخلات	المفتاح .
المصدر	الواجهة الخاصة بالمرسل(Hide).
المخرجات	اضافة المفتاح الى البرنامج.
الهدف	اختيار المفتاح من أجل حماية الرسالة المخفية.
المتطلبات	أن لا يكون محتوى المفتاح فارغ .
شروط قبل التنفيذ	لا شيء.
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المرسل بتحديد الطريقة التي يعتمد عليها في تحديد طريقة دمج الرسالة داخل الصورة.ومن خلال الواجهه الخاصة بعمل Hide، يختار المفتاح ثم يضيفه ليتم تخزينه في البرنامج.

5. دمج الرسالة واخفائها.

الوظيفة	دمج الرسالة التي تم اخفائها.
الوصف	دمج محتوى الرسالة (نص,صورة) داخل الصورة.
المدخلات	محتوى الرسالة المراد اخفائها. المفتاح .
المصدر	الواجهة الخاصة بالمرسل(Hide).
المخرجات	عرض الصورة بعد الإخفاء.
الهدف	إخفاء محتوى الرسالة داخل الصورة.
المتطلبات	ادخال المفتاح . ادخال الرسالة المراد اخفائها.
شروط قبل التنفيذ	يجب أن يقوم المرسل بادخال محتوى الرسالة بحيث يكون حجم الرسالة اصغر من حجم الصورة (عدد الـ Bit في الرسالة المراد دمجها اقل من عدد الـ Bit المتاحة في الصورة الاصلية).
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المرسل بتحديد الطريقة التي يعتمد عليها في تحديد طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهه الخاصة بعمل Hide, يدخل الرسالة التي يريد اخفائها والمفتاح ومن ثم يتمكن من اخفاء الرسالة التي تم اخفائها.

وصف المتطلبات الوظيفية الخاصة بالمستقبل:

1. اختيار الصورة المدمج بداخلها الرسالة.

الوظيفة	اختيار الصورة المدمج بداخلها الرسالة.
الوصف	يقوم المستقبل بتحديد الصورة المدمج بداخلها الرسالة.
المدخلات	الصورة المدمج بداخلها الرسالة.
المصدر	الواجهة الخاصة بالمستقبل(Extract).
المخرجات	عرض الصورة المدمج بداخلها الراسلة.
الهدف	تمكين المستخدم من تحديد الصورة المدمج بداخلها الصورة.
المتطلبات	نوع الصورة (Bitmap).
شروط قبل التنفيذ	وصول المستقبل للصورة المدمج بداخلها الرسالة.
شروط بعد التنفيذ	تحديد المستقبل للصورة المدمج بداخلها الرسالة.
الإجراءات	يقوم المستقبل بتحديد الطريقة التي تم الاعتماد عليها في طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهة الخاصة بعمل Extract للرسالة، يحدد الصورة المدمج بداخلها الرسالة.

2. اختيار المفتاح.

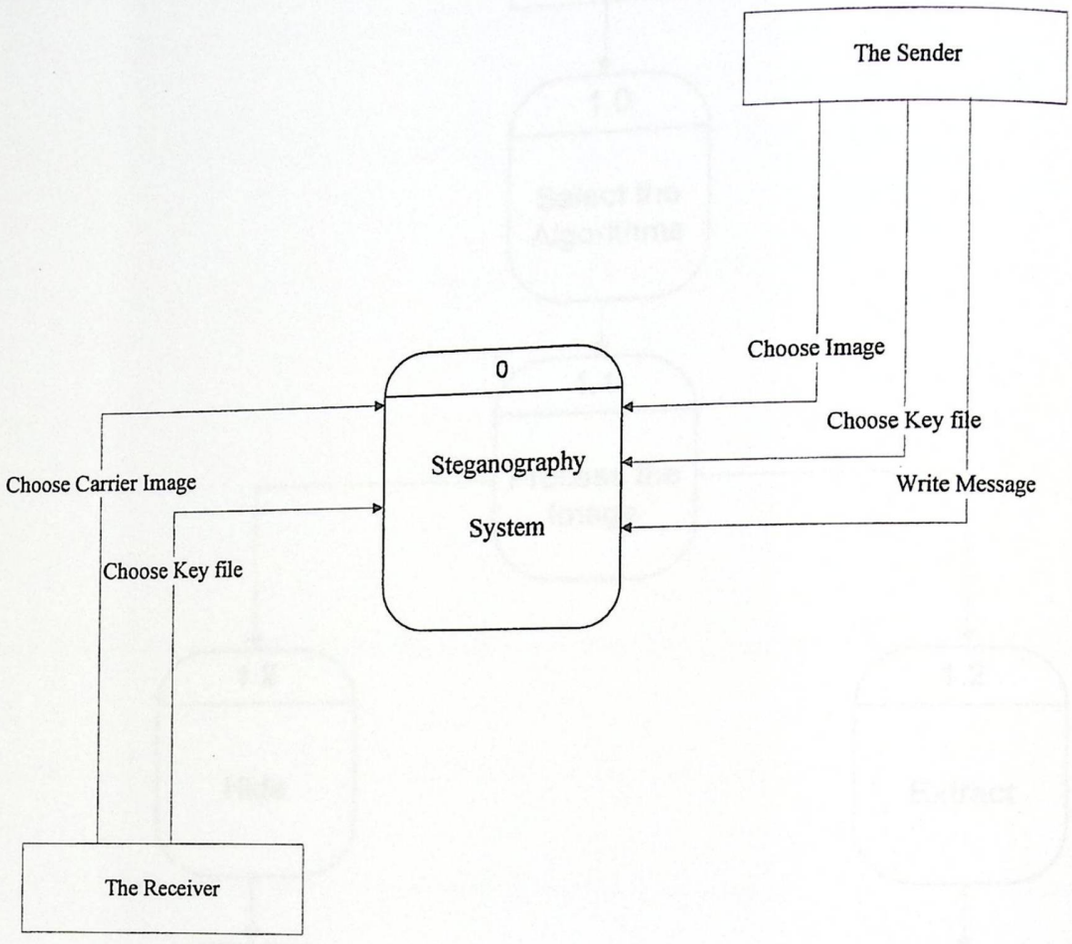
الوظيفة	اختيار المفتاح.
الوصف	يقوم المستقبل باختيار المفتاح المتفق عليه من قبل المرسل والمستقبل .
المدخلات	المفتاح.
المصدر	الواجهة الخاصة بالمستقبل(Extract).
المخرجات	اضافة المفتاح.
الهدف	اختيارالمفتاح من أجل حماية الرسالة المخفية.
المتطلبات	أن يكون المفتاح متفق عليه بين المرسل والمستقبل .
شروط قبل التنفيذ	لا شيء.
شروط بعد التنفيذ	لا شيء.
الإجراءات	يقوم المستقبل بتحديد الطريقة التي تم الاعتماد عليها في طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهه الخاصة بعمل Extract، يختارالمفتاح المتفق عليه ويضيفه الى البرنامج.

4. استخراج الرسالة المدمجة من الصورة .

الوظيفة	استخراج الرسالة المدمجة من الصورة .
الوصف	يقوم المستقبل باستخراج الرسالة من الصورة المدمجة.
المدخلات	الصورة المدمج بداخلها الرسالة المفتاح المتفق عليه .
المصدر	واجهة فك الاخفاء.
المخرجات	الرسالة التي تم دمجها.
الهدف	استخراج الرسالة المدمجة داخل الصورة.
المتطلبات	الصورة المدمج بداخلها الرسالة. مفتاح التشفير المتفق عليه.
شروط قبل التنفيذ	وجود الصورة المدمج بداخلها الرسالة. وجود ملف التشفيرالمتفق عليه ين المرسل والمستقبل.
شروط بعد التنفيذ	استخراج الرسالة دون التغيير على محتواها.
الإجراءات	يقوم المستقبل بتحديد الطريقة التي تم الاعتماد عليها في طريقة دمج الرسالة داخل الصورة, ومن خلال الواجهة الخاصة بعمل Extract، يقوم بتحديد الصورة المدمج بداخلها الرسالة, وتحديد المفتاح المتفق عليه بين المرسل والمستقبل لاستخراج الرسالة المدمجة.

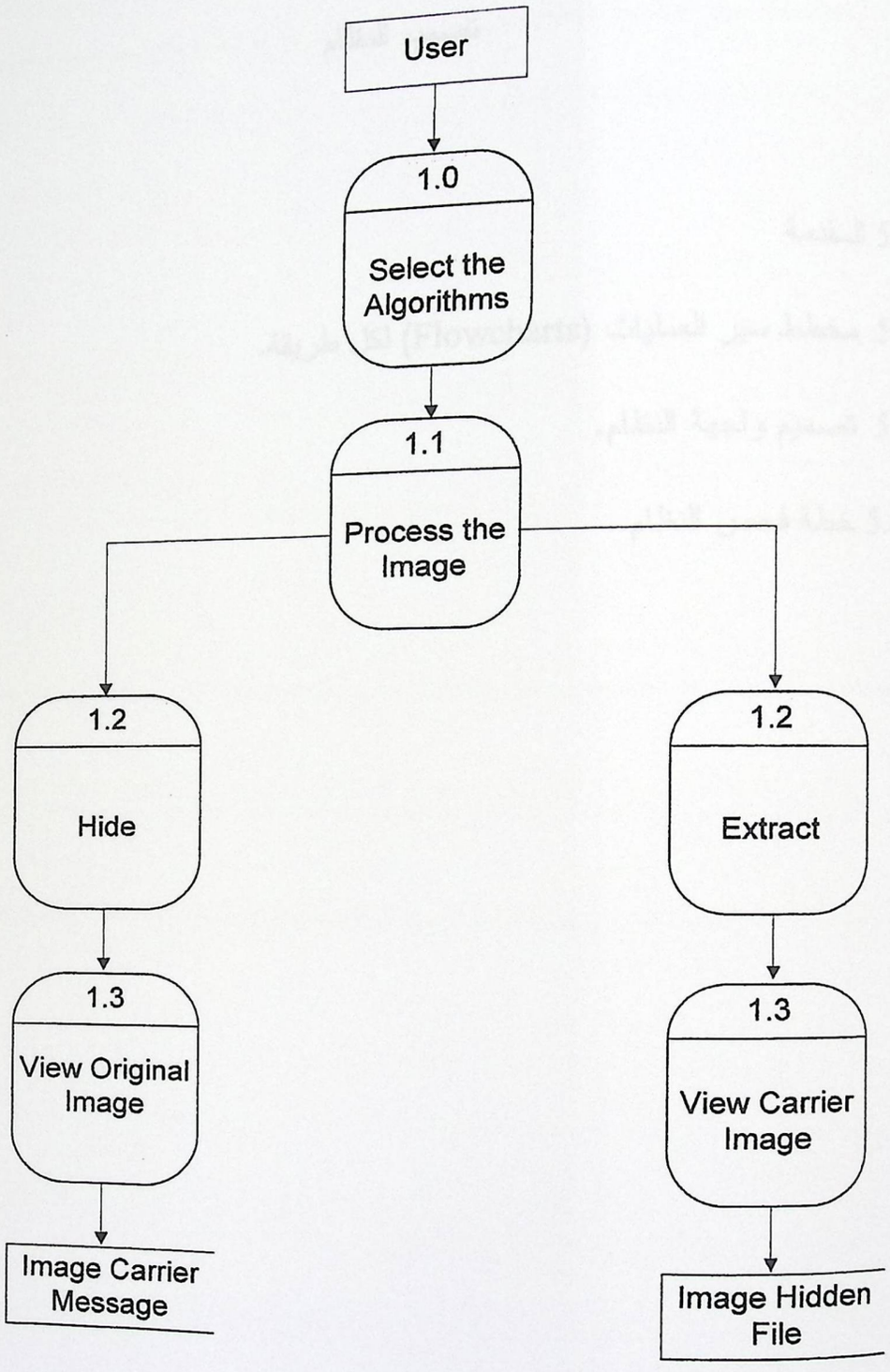
4.3 مخطط محتوى النظام (Context Diagram):

يتم توضيح علاقة النظام بالأنظمة المحيطة به من خلال مخطط محتوى النظام:



الشكل(4.1) مخطط محتوى النظام(Context Diagram)

4.4 مخطط تدفق البيانات (Data Flow Diagram(DFD)) :



الشكل (4.2) مخطط تدفق البيانات(Data Flow Diagram)

الفصل الخامس

تصميم النظام

5.1 المقدمة

5.2 مخطط سير العمليات (Flowcharts) لكل طريقة.

5.3 تصميم واجهة النظام.

5.4 خطة فحص النظام.

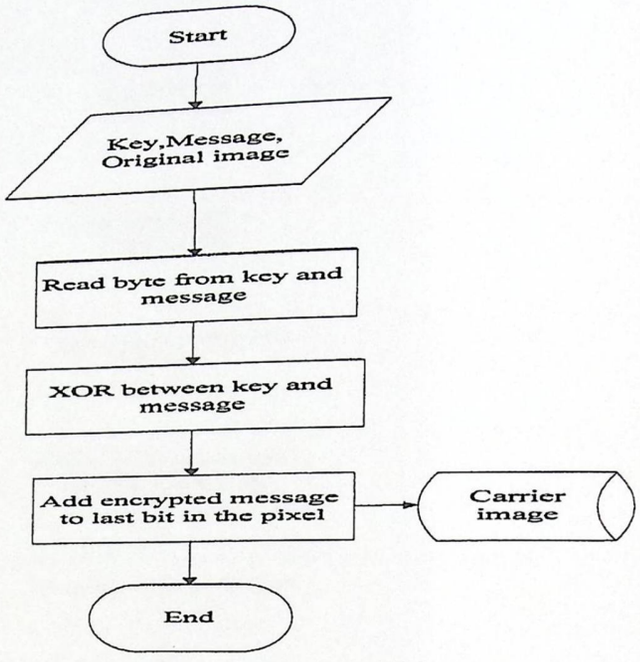
5.1 المقدمة:

في هذا الفصل سيتم توضيح مخطط سير العمليات لكل طريقة تم تطبيقها وتـــصميم شاشـــات النظـــام, وأيضاً سيتم توضيح خطة فحص النظام.

5.2 مخطط سير العمليات (Flowchart):

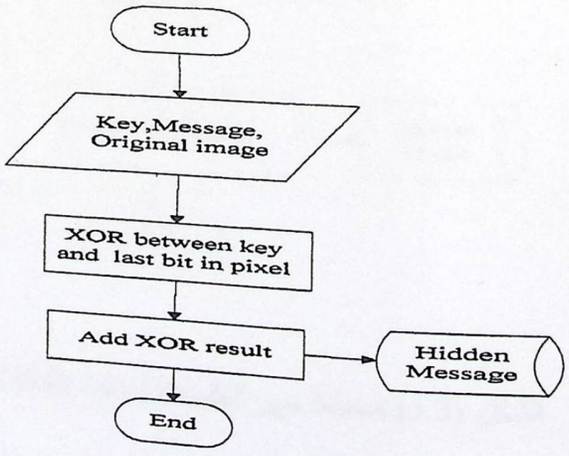
5.2.1 مخطط سير العمليات للطريقة الأولى:

مخطط سير العمليات الذي يوضح عملية ال Hide في الطريقة الأولى:



الشكل(5.1) مخطط سير العلميات لعملية Hide في الطريقة الأولى

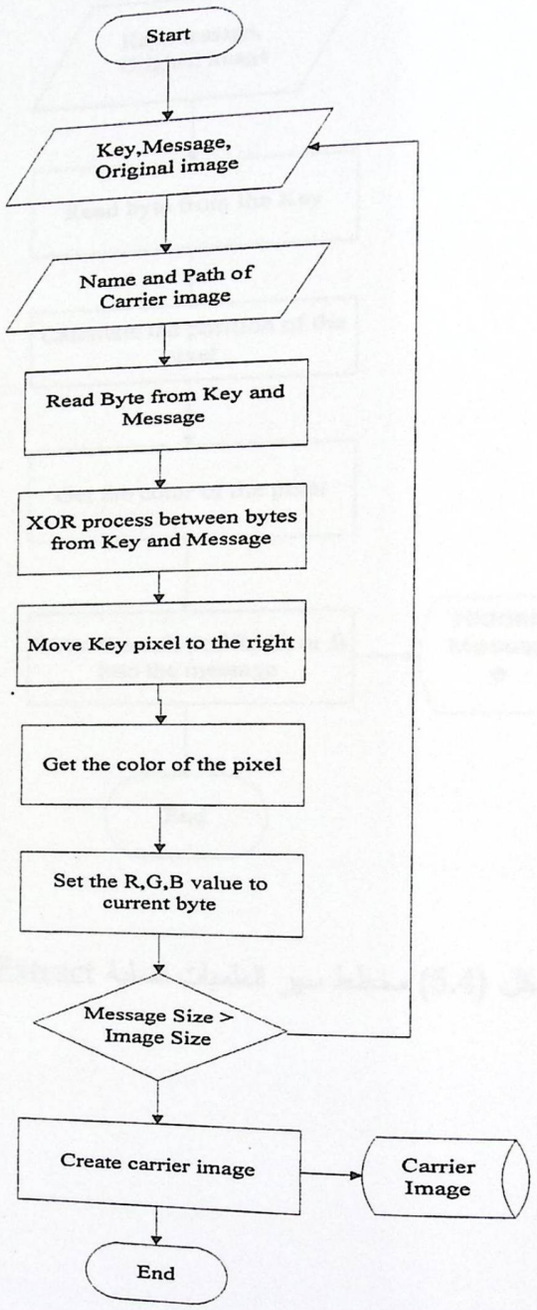
مخطط سير العمليات الذي يوضح عملية ال Extract في الطريقة الأولى:



الشكل(5.2) مخطط سير العلميات لعملية Extract في الطريقة الأولى

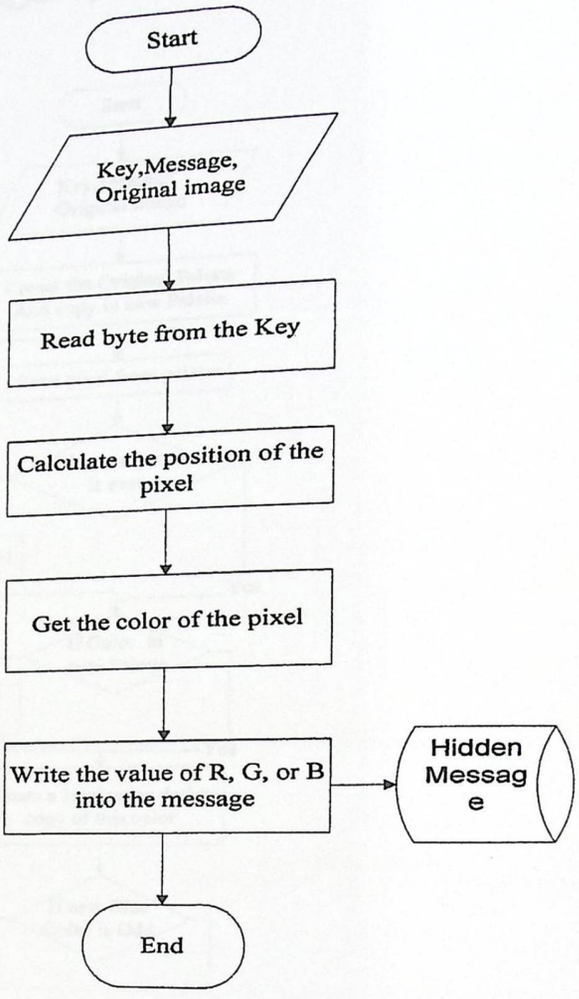
5.2.2 مخطط سير العمليات للطريقة الثانية:

مخطط سير العمليات الذي يوضح عملية ال Hide في الطريقة الثانية



الشكل (5.3) مخطط سير العلميات لعملية Hide في الطريقة الثانية

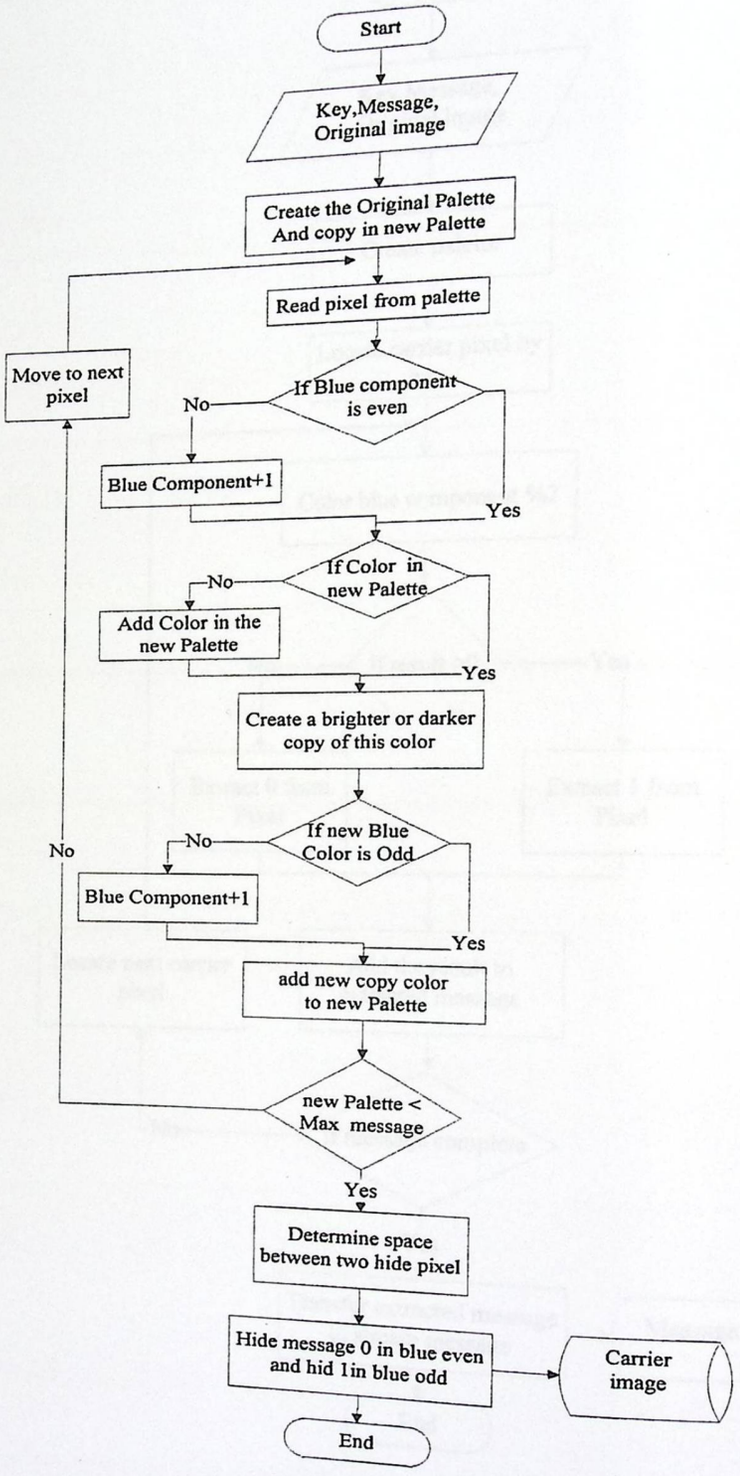
مخطط سير العمليات الذي يوضح عملية Extract في الطريقة الثانية:



الشكل (5.4) مخطط سير العلميات لعملية Extract في الطريقة الثانية

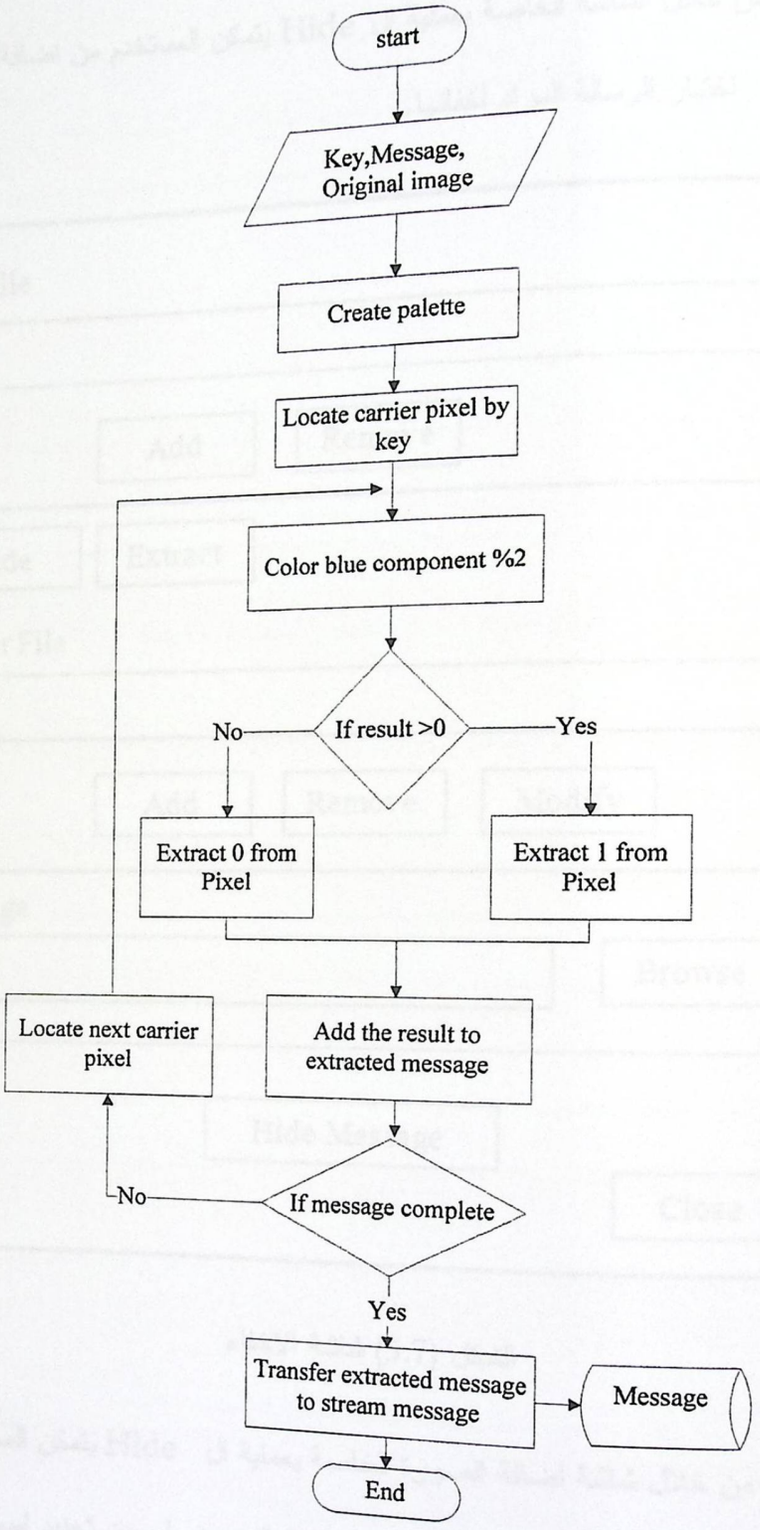
مخطط سير العمليات الذي يوضح عملية ال Hide في الطريقة الثالثة:

5.2.3 مخطط سير العمليات للطريقة الثالثة:



الشكل (5.5) مخطط سير العلميات لعملية Hide في الطريقة الثالثة

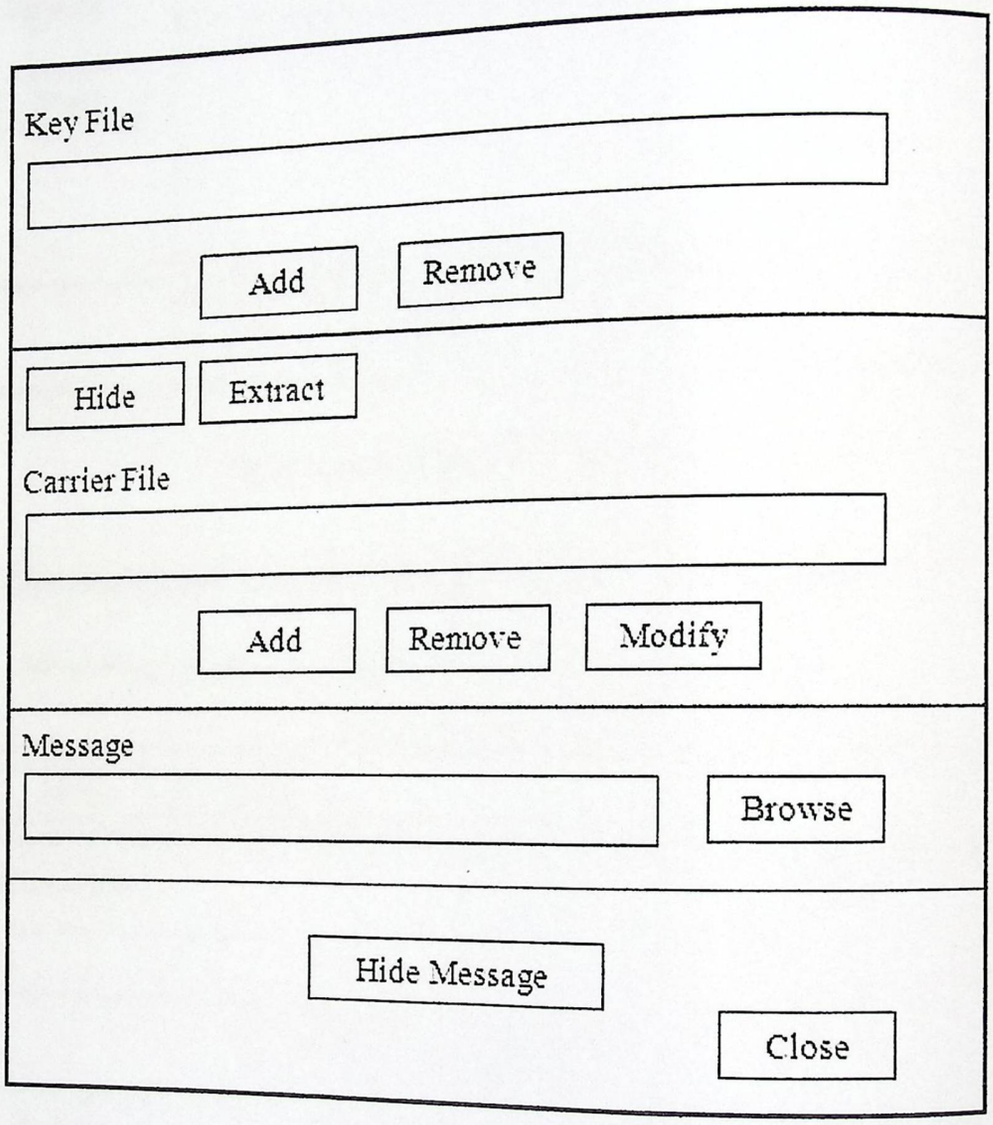
مخطط سير العمليات الذي يوضح عملية ال Extract في الطريقة الثالثة



الشكل (5.6) مخطط سير العلميات لعملية Extract في الطريقة الثالثة

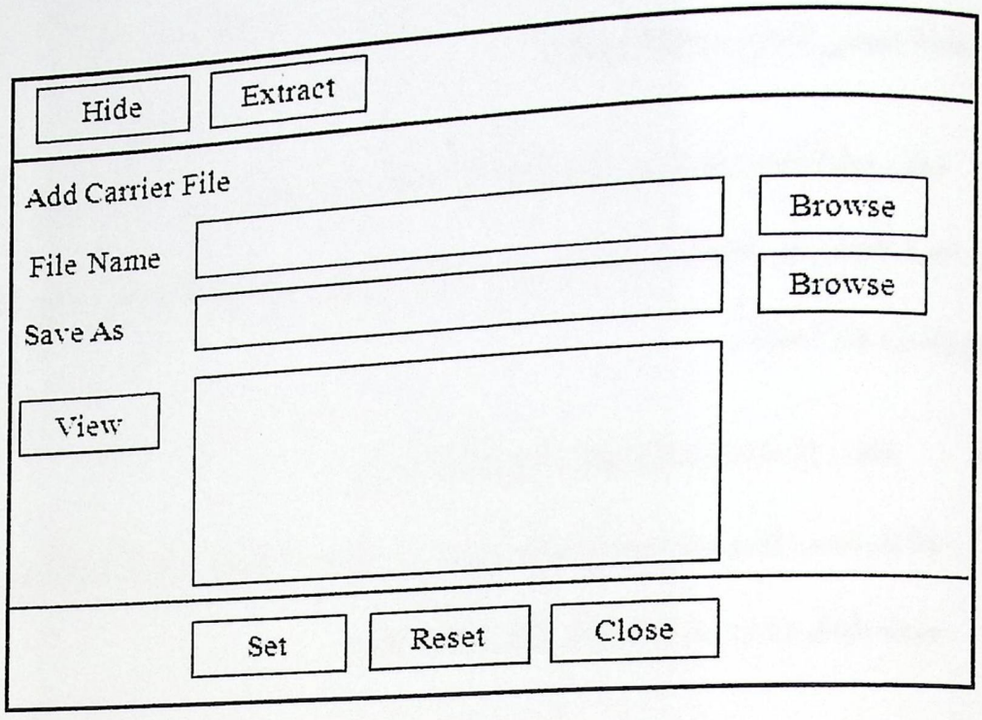
5.3 تصميم واجهات النظام:

- من خلال الشاشة الخاصة بعملية ال Hide يتمكن المستخدم من اضافة المفتاح ومـن اختيار الرسالة المراد اخفائها.



الشكل (5.7) شاشة الاخفاء

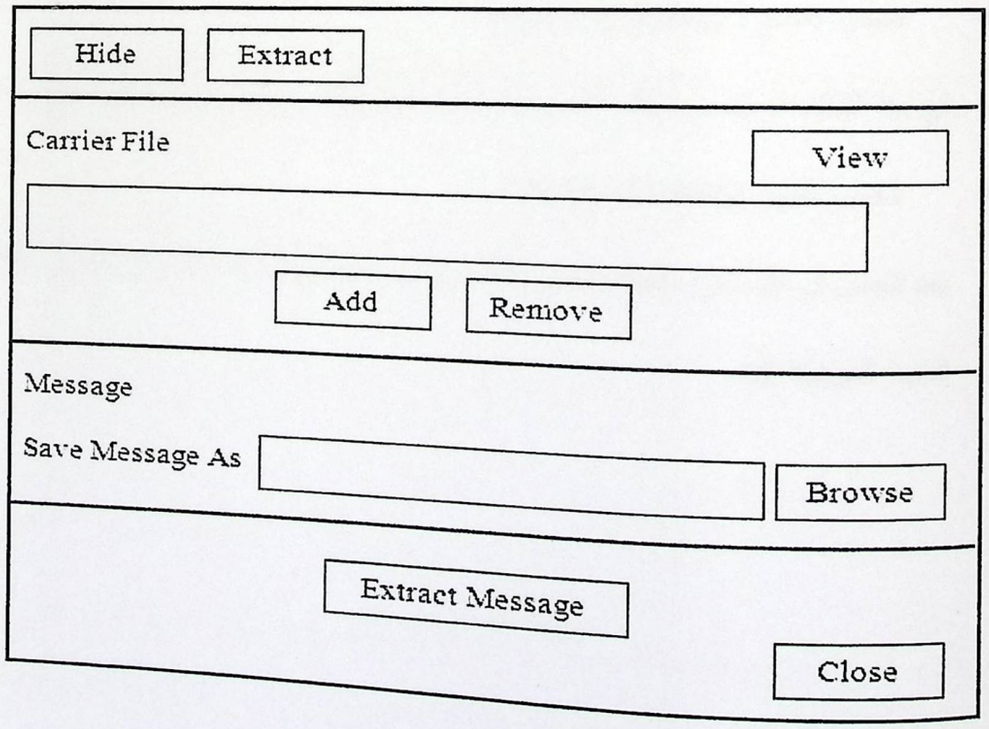
- من خلال شاشة اضافة الصورة الخاصة بعملية ال Hide يتمكن المستخدم من تحديد الصورة المراد الإخفاء بداخلها مع امكانية عرضها, ومن تحديد اسم ومكان الصورة المراد حفظ النتيجة بها.



الشكل (5.8) شاشة إضافة الصورة الاصلية

- يتمكن المستقبل من خلال شاشة ال Extract من تحديد الصورة الحاملـة للرسـالة ,

ومن تحديد ملف لحفظ الرسالة بداخله ليتمكن من استخراج الرسالة المخفية.



الشكل (5.9) شاشة إضافة الصورة الحاملة للرسالة

5.4 خطة فحص النظام (Test Plan)

تعتبر عملية فحص النظام من أهم مراحل بناء النظام، حيث يتم بها فحص أجزاء النظام كاملة، وتكمن أهمية الفحص في التحقق من أن كل جزء من أجزاء النظام يقوم بالوظيفة المطلوبة منه بـشكل صحيح وتشمل هذه العملية :

- فحص الوحدات ونماذج النظام (Unit Testing) .

هنا يتم فحص كل وحدة موجودة بشكل منفصل عن الوحدات الأخرى, وهذه الوحدات لإثبـات صحة النظام وخلوه من أي مشاكل أثناء عملية التشغيل.

- فحص التكامل (Integration Testing)

في هذا القسم يتم فحص التكامل بين مكونات النظام وذلك بفحص التفاعل بين مكونات النظـام وشاشات النظام.

- فحص النظام (System Testing)

في هذا النظام تم فحص النظام كأنه وحدة واحدة حتى نتأكد من أنه يعمل بشكل صحيح.

- فحص القبول (Accept Testing)

بعد فحص أن كل أجزاء النظام تعمل بشكل متكامل ومتوافق يتم بعد ذلك مدى قبـول النظـام للجهة الموجهة إليه.

الفصل السادس

فحص النظام

6.1 المقدمة

6.2 فحص الوحدات والنماذج

6.3 فحص التكامل

6.4 فحص النظام

6.5 فحص قبول النظام

الفصل السادس

فحص النظام

6.1 المقدمة

6.2 فحص الوحدات والنماذج

6.3 فحص التكامل

6.4 فحص النظام

6.5 فحص قبول النظام

6.1 المقدمة:

بعد إنهاء مرحلة تطبيق وبرمجة النظام يوضع النظام تحت عمليات الفحص المختلفة للتأكد من مطابقة النظام لمتطلباته الوظيفية وأنه يحقق المواصفات والمتطلبات المطلوبة منه.

وتكمن أهمية فحص النظام من خلال التحقق من إعتمادية كل وحدة وجزء من النظام على حده، وفي هذا الفصل سنتناول مراحل عملية فحص الوحدات والنماذج وفحص التكامل وفحص النظام وقبوله.

6.2 فحص الوحدات والنماذج:

سيتم في هذه المرحلة فحص جميع الوحدات التابعة للنظام كل وحدة على حده ,وقد تمت عملية فحص كل وحدة من خلال إدخال عدة مدخلات والتحقق من صحة المخرجات، وبعد إتمام عملية فحص جميع الوحدات، تم التأكد أن جميع وحدات النظام تعمل بشكل صحيح كما هو مطلوب.

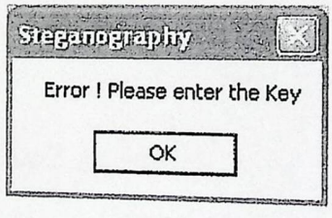
حيث سيتم فحص المدخلات لعملية الاخفاء والاستخراج ويتم ذلك لكل طريقة من الطرق التـــي تم استخدامها كما يلي:

6.2.1 فحص الطريقة الأولى:

عملية الإخفاء (Hide):

1) فحص ادخال ملف المفتاح:

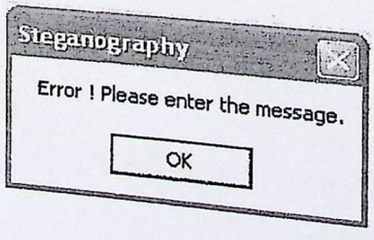
- اذا لم يدخل المرسل ملف المفتاح (ترك الحقل فارغاً): تظهر رسالة خطـــأ لاختيـــار ملف المفتاح.



الشكل(6.1) فحص إدخال ملف المفتاح إذا كان فارغ

2) فحص ادخال الرسالة المراد اخفائها:

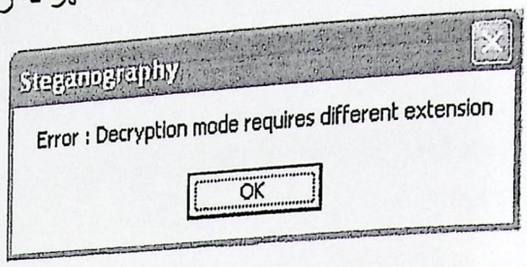
- اذا لم يدخل المرسل الرسالة التي يريد اخفائها تظهر له رسالة خطأ لكتابتها.



الشكل (6.2) فحص إدخال الرسالة إذا لم يتم إدخالها

3) فحص ادخال الصورة المراد الاخفاء بداخلها:

- اذا ادخل المرسل صورة من نوع غير Bitmap تظهر له رسالة خطأ.



الشكل (6.3) فحص إدخال الصورة المراد الإخفاء بداخلها

عملية الاستخراج (Extract):

1) فحص ادخال ملف المفتاح:

- اذا لم يدخل المستقبل المفتاح تظهر له رسالة خطأ لإدخالها كما في عملية الإخفاء.
- اذا ادخل المستقبل مفتاح مختلف عن المفتاح الذي تم استخدامه في عملية الإخفاء يعطي نتيجة ولكن غير صحيحة.

2) فحص ادخال الصورة الحاملة للرسالة:

- اذا تم اختيار صورة غير الحاملة للرسالة تظهر النتيجة رسالة غير صحيحة.

6.2.2 فحص الطريقة الثانية :

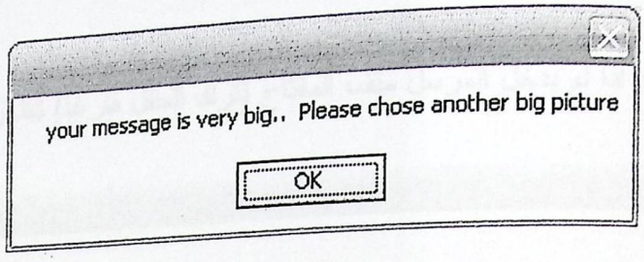
عملية الإخفاء (Hide):

1) فحص ادخال المفتاح :

- يتم ادخال ملف المفتاح من أي نوع من الملفات سواء كان صورة بمختلف امتداداتها مثل JPG أو Bitmap أم ملف بامتداد txt. أو doc.
- يجب ادخال المفتاح حتى يتمكن المرسل من اخفاء الرسالة.

2) فحص ادخال الصورة المراد اخفاء الرسالة بداخلها:

- لا يستطيع المرسل الإخفاء دون اختيار الصورة المراد اخفاء الرسالة داخلها .
- اذا ادخل المرسل صورة حجمها أقل من حجم الرسالة التي يريد اخفائها تظهر لـه رسالة خطأ كالتالي:



الشكل(6.4) فحص ادخال الصورة

3) فحص ادخال الرسالة المراد اخفائها:

- اذا ادخل المرسل ملف الرسالة فارغاً سوف يتم الاخفاء وعند استخراج الرسالة يكون الملف المستخرج فارغاً.
- لا يستطيع المرسل الاخفاء دون تحديد ملف الرسالة.

عملية استخراج الرسالة (Extract):

1) فحص ادخال ملف المفتاح:

- اذا اختار المستقبل ملف مفتاح غير المستخدم في عملية الإخفاء يكون الناتج عباره عن رسالة غير صحيحة.
- اذا اختار المستقبل ملف مفتاح فارغ تكون النتيجة ملف فارغ لا يحتوي على الرسالة.

2) فحص ادخال الصورة الحاملة للرسالة:

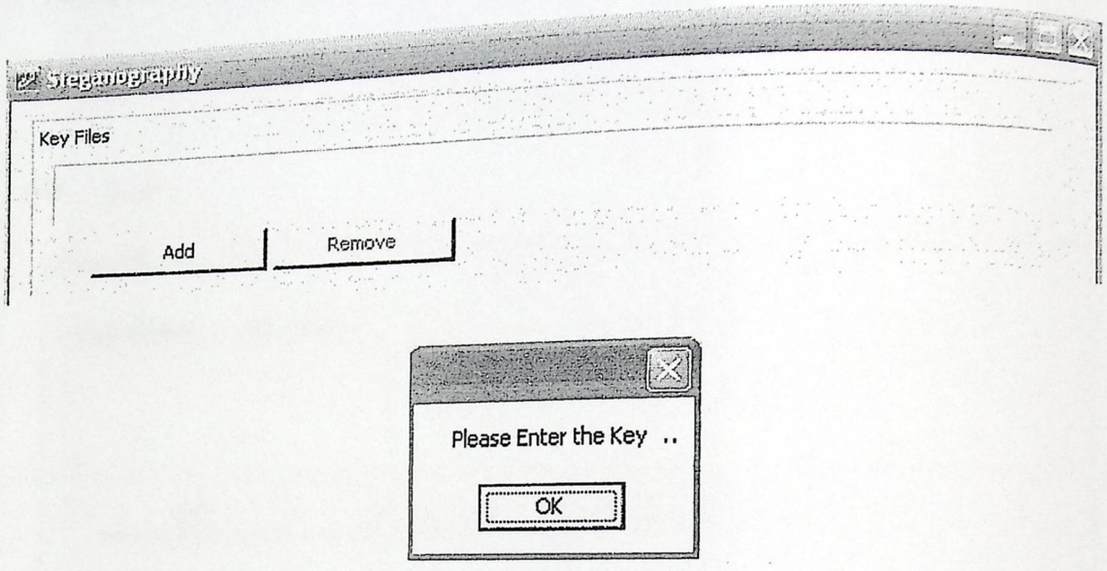
- اذا ادخل المستقبل صورة غير الحاملة للرسالة فيكون الملف المستخرج منها يحتوي رسالة غير صحيحة.

6.2.3 فحص الطريقة الثالثة :

فحص عملية الإخفاء (Hide):

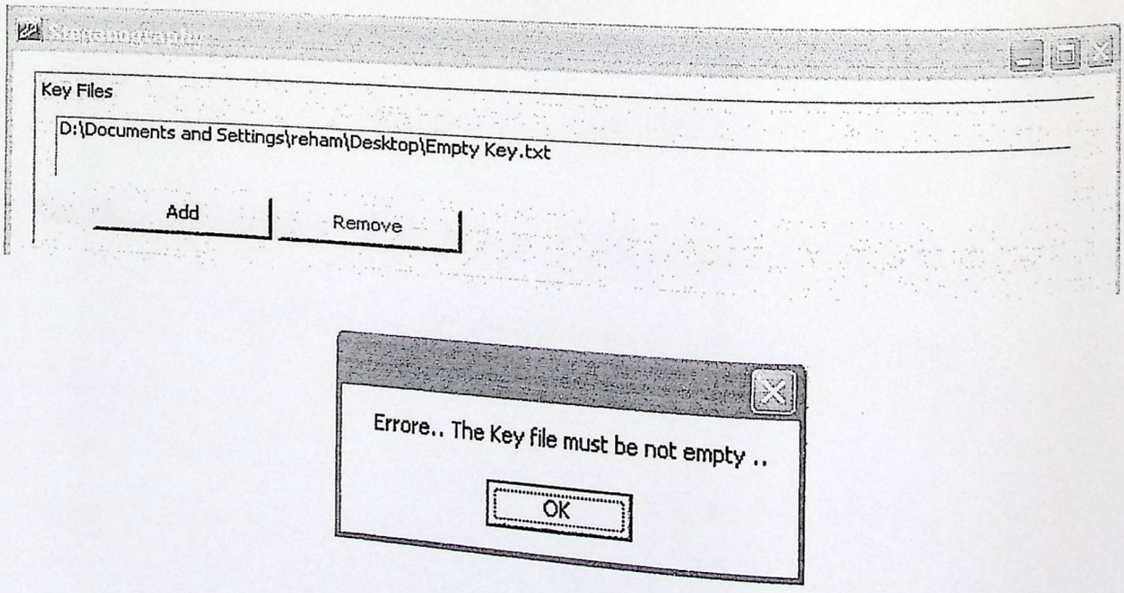
1) فحص المفتاح :

- اذا لم يدخل المرسل ملف المفتاح (ترك الحقل فارغاً) تظهر رسالة خطأ لإدخاله:



الشكل(6.5) فحص المفتاح إذا كان فارغا

- اذا ادخل المرسل ملف مفتاح فارغ تظهر رسالة خطأ :

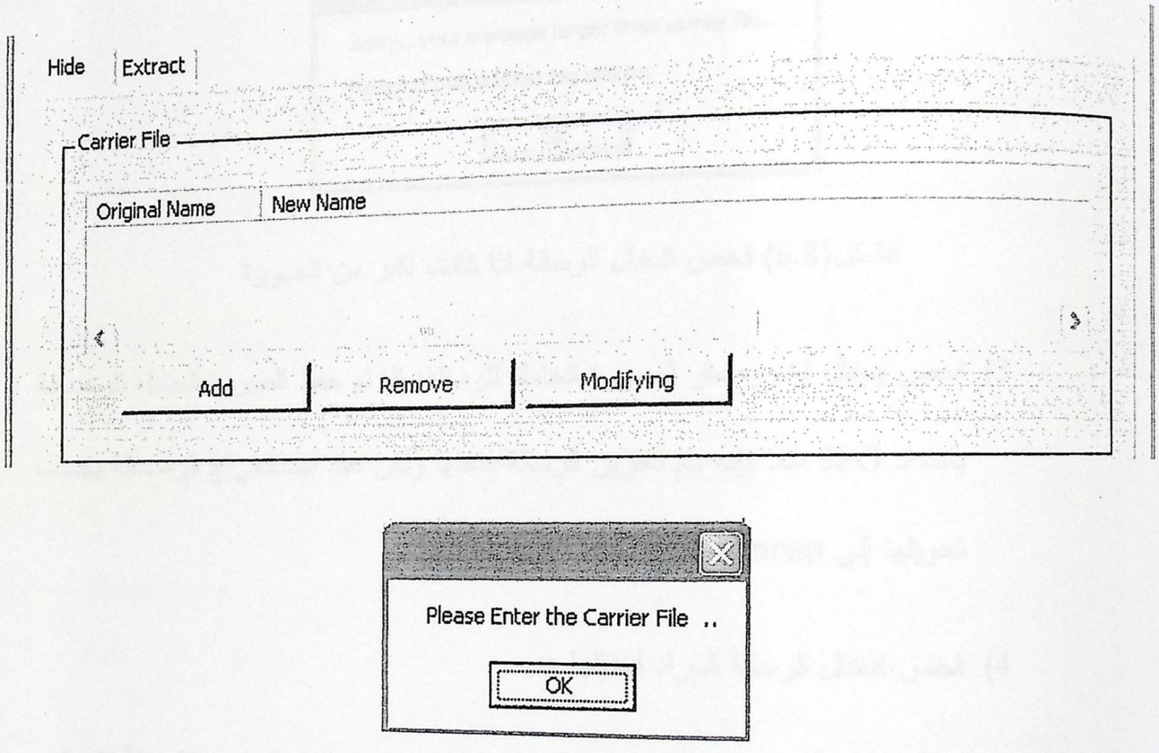


الشكل(6.6) فحص المفتاح اذا كان الملف فارغا

- اذا ادخل المرسل ملف المفتاح صورة من أي نوع مثلً JPG أو ادخل ملف Documents أو Text فإنه يتم الاخفاء دون أي خطأ.

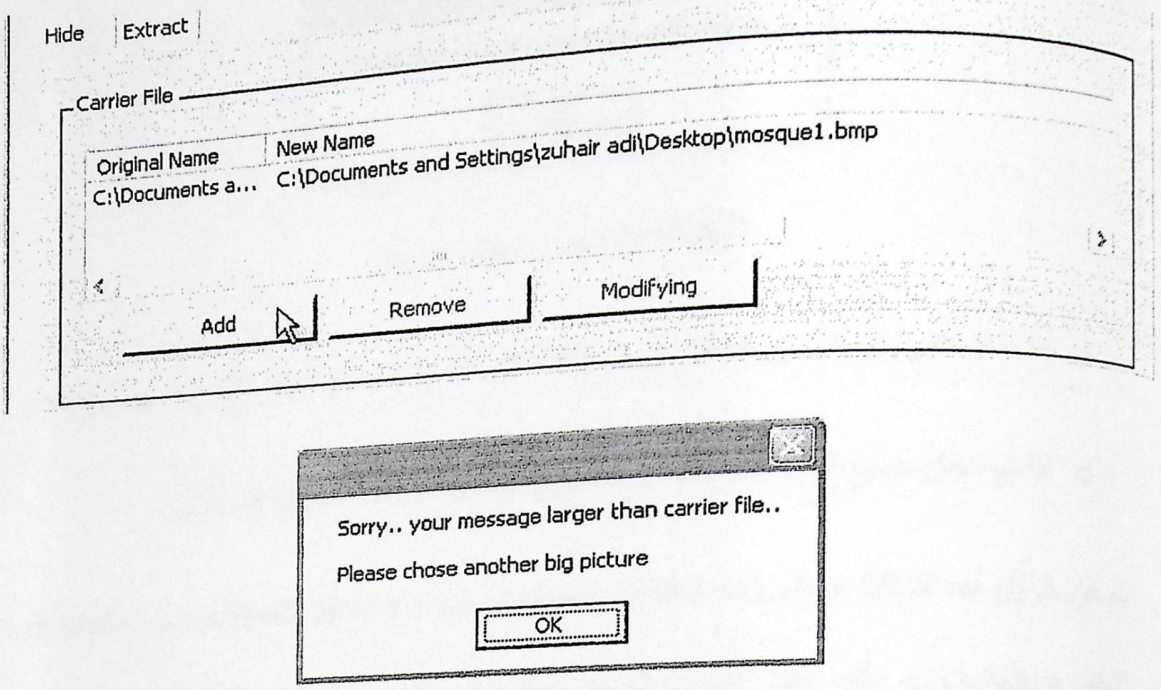
2) فحص ادخال الصورة المراد الاخفاء داخلها:

- اذا لم يدخل المرسل صورة (ترك الحقل فارغاً): تظهر رسالة خطأ لإدخال الصورة.



الشكل(6.7) فحص ادخال الصورة

- إذا ادخل المرسل صورة حجمها أصغر من الرسالة المراد اخفائها : تظهر رسالة خطأ تبين أنه لا يمكن اخفاء الرسالة لأنه حجمها أكبر من حجم الصورة.

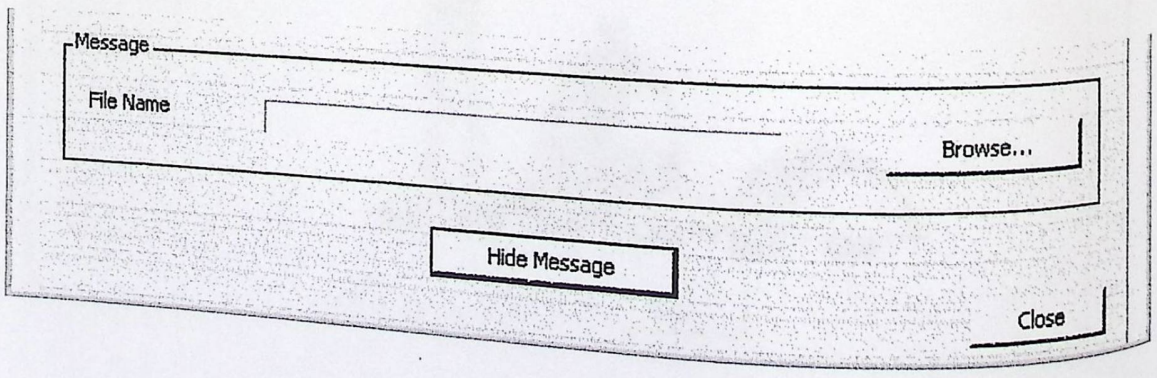


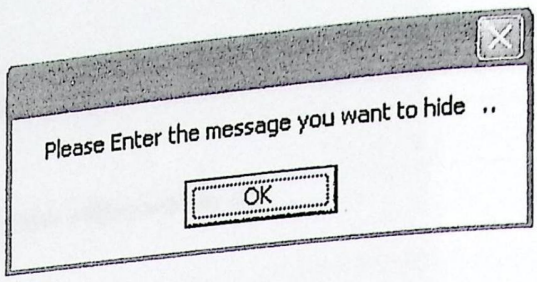
الشكل(6.8) فحص ادخال الرسالة اذا كانت اكبر من الصورة

3) فحص إدخال اسم ومسار الصورة الحاملة للرسالة: اذا تم حفظ الصورة الحاملة للرسالة بامتداد JPG مثلاً فإنه يتم تخزين الرسالة داخلها ولكن عند استخراج الرسالة يجب تحويلها إلى Bitmap قبل الاستخراج.

4) فحص ادخال الرسالة المراد اخفائها :

- اذا لم يدخل المرسل رسالة لإخفائها (ترك الحقل فارغاً) :تظهر رسالة خطأ لإدخال الرسالة:

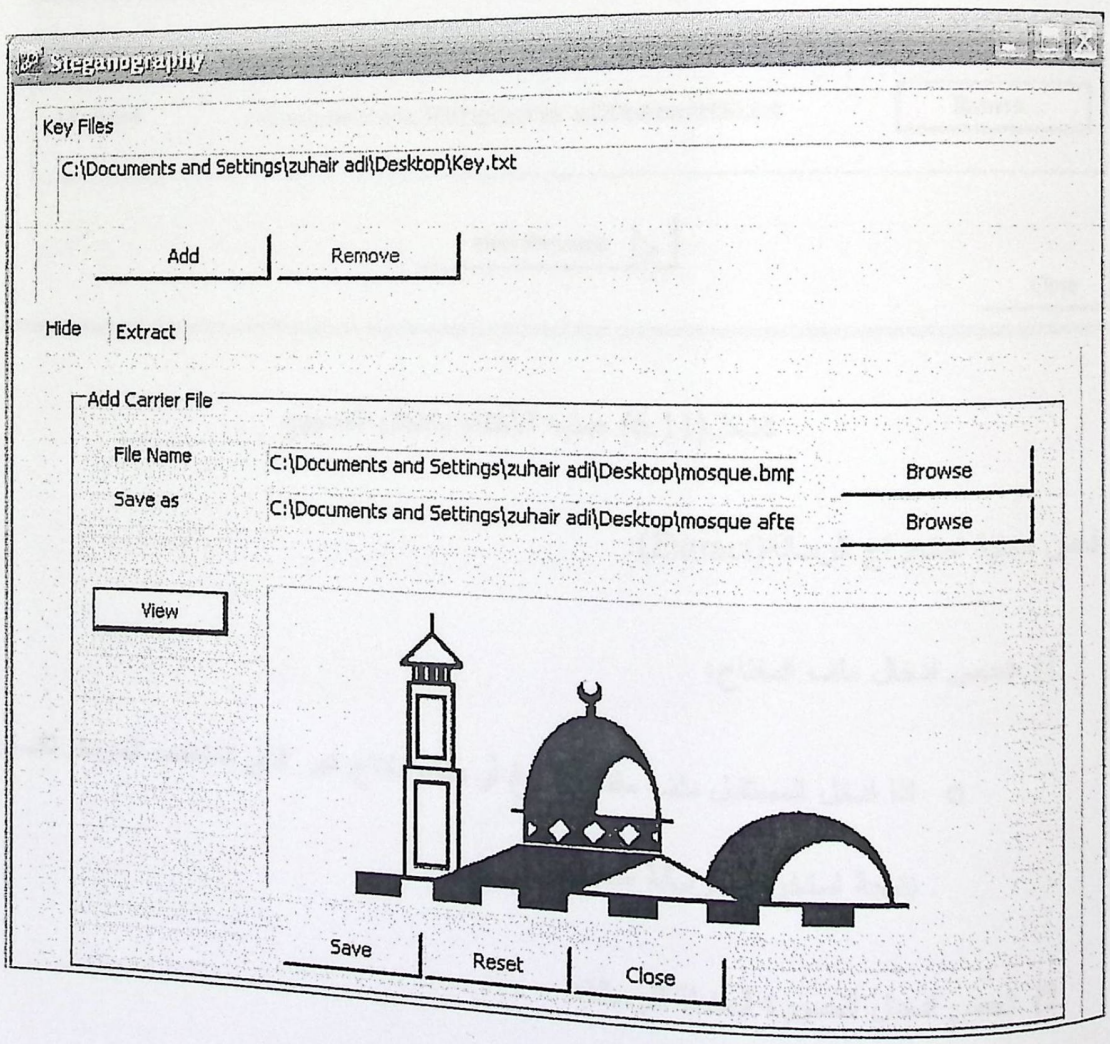




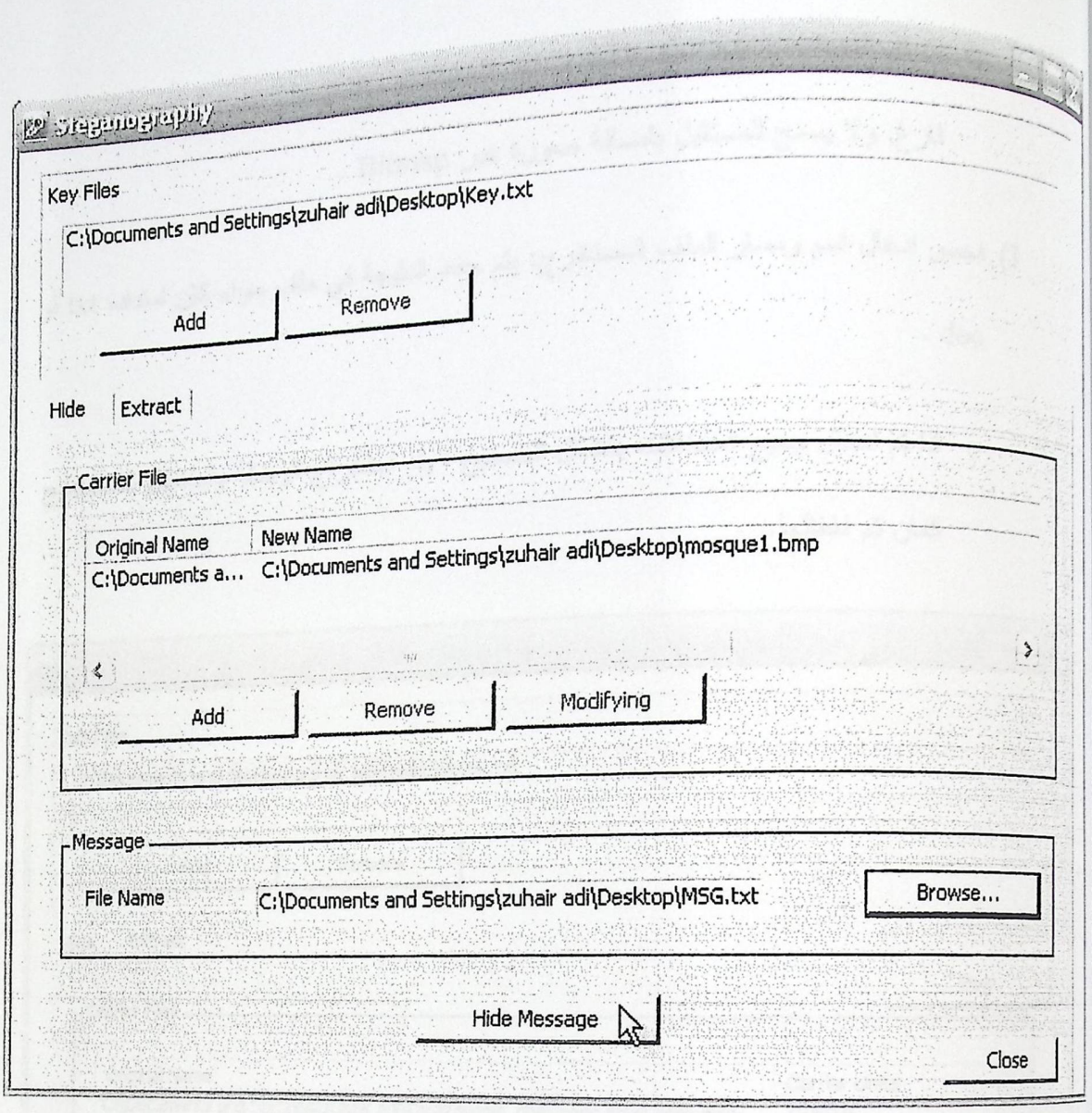
الشكل(6.9) فحص ادخال الرسالة

- إذا ادخل المرسل ملف رسالة فارغ يتم إخفاء الرسالة واسترجاع الملف الفارغ الذي تم إخفائه
- اذا تم ادخال جميع المدخلات بالشكل الصحيح: فإنه يتم الإخفاء بالشكل الصحيح.

يتم عن طريق هذه الشاشة ادخال ملف المفتاح والدخول الى شاشة الHide لإضافة الصورة المراد الاخفاء بداخلها وتحديد مكان حفظ الصورة الجديدة الحاملة للرسالة وعمل عرض للصورة الأصلية.



الشكل(6.10) ادخال المدخلات بالشكل الصحيح



الشكل(6.11) عملية الأخفاء بالشكل الصحيح

فحص عملية استخراج الرسالة(Extract):

1) فحص ادخال ملف المفتاح:

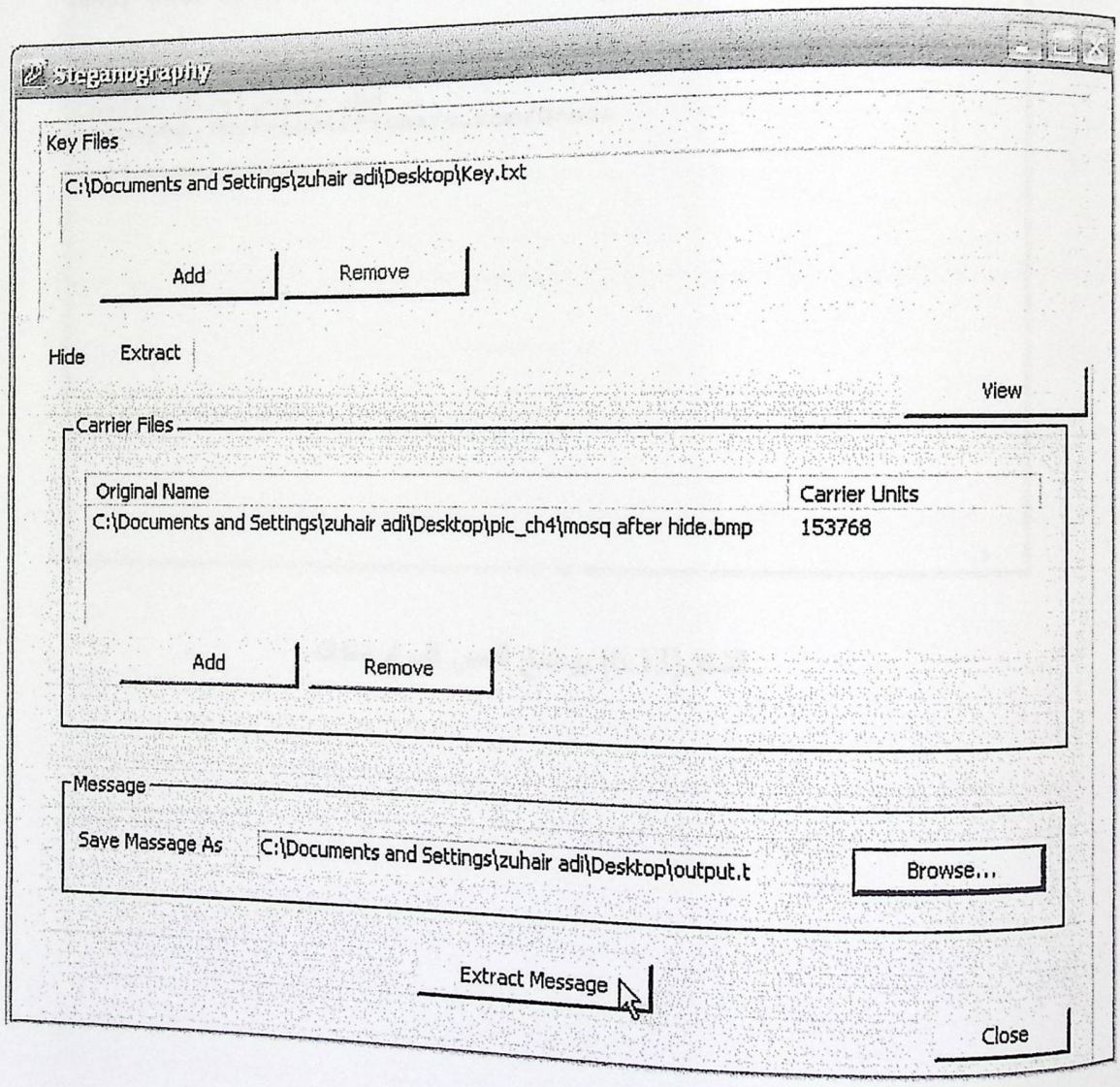
- اذا ادخل المستقبل ملف مفتاح فارغ أو ملف مفتاح غير الذي استخدمه المرسل تكـون نتيجة استخراج الرسالة ملف فارغ .

2) فحص ادخال الصورة الحاملة للرسالة:

- اذا قام المستقبل بتحديد صورة أخرى غير الحاملة للرسالة فيعطي نتيجة الاستخراج ملف فارغ, ولا يسمح للمستقبل باضافة صورة غير Bitmap .

3) فحص ادخال اسم ومسار الملف المستخرج: يتم حفظ النتيجة في ملف سواء كان امتداده txt أو doc .

- اذا تم ادخال جميع المدخلات بالشكل الصحيح : يتم استخراج الرسالة بالشكل الصحيح كمان تم اخفائها.

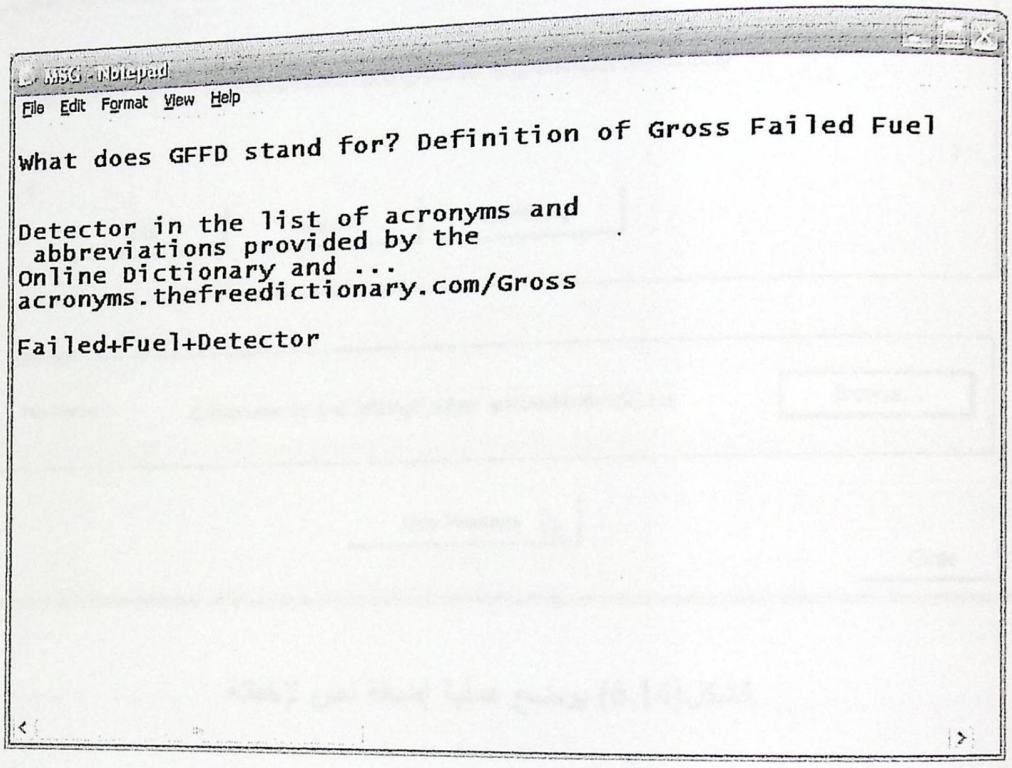


الشكل(6.12) مدخلات عملية استخراج الرسالة بالشكل الصحيح

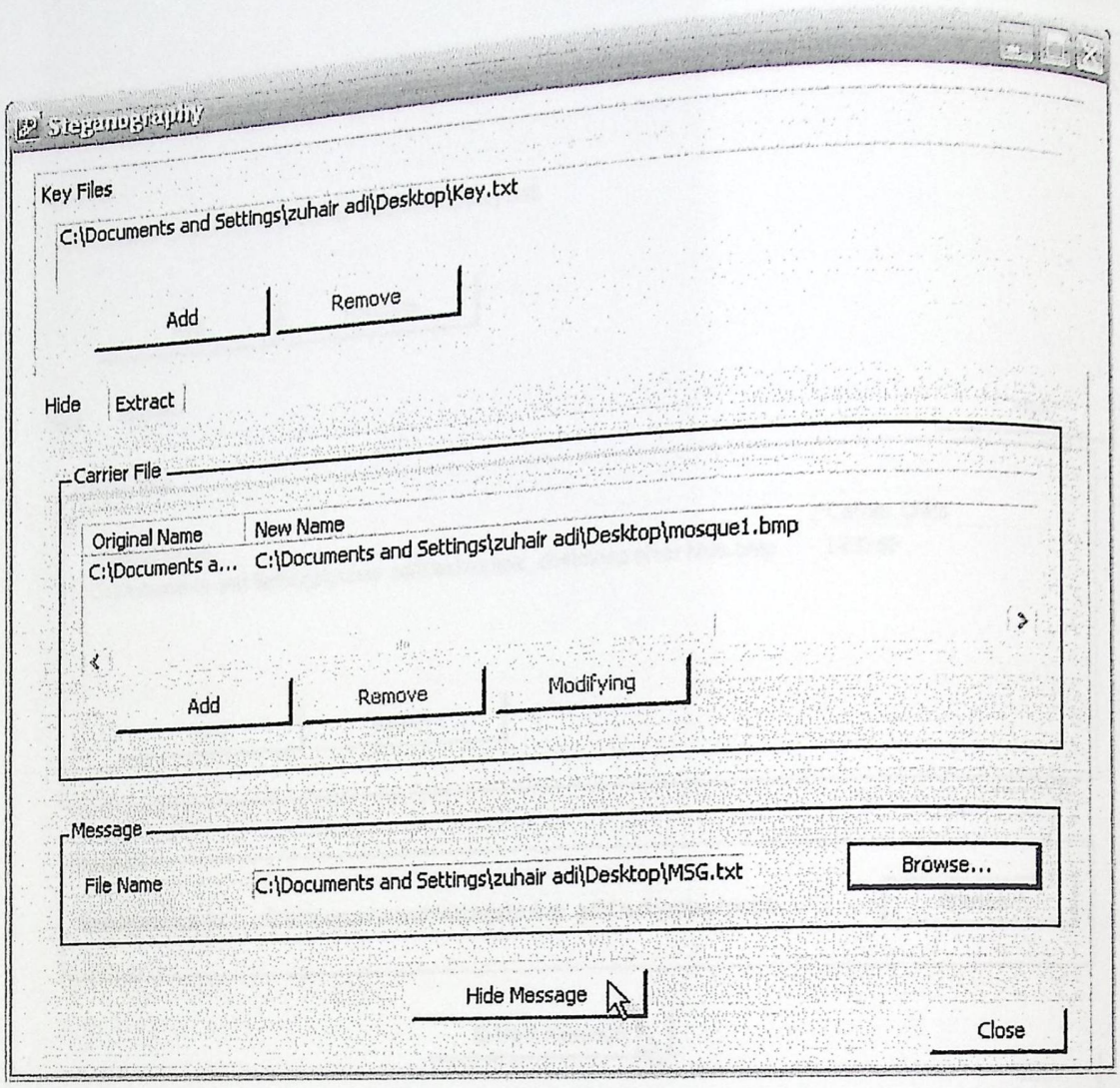
6.3 فحص التكامل:

تم فحص التكامل بين الأجزاء المختلفة للنظام وذلك بفحص التفاعل بين هذه الأجزاء وقد تم تطبيقه على كافة الطرق ومن الأمثة على هذه الأجزاء التي تم فحص التكامل بينها:

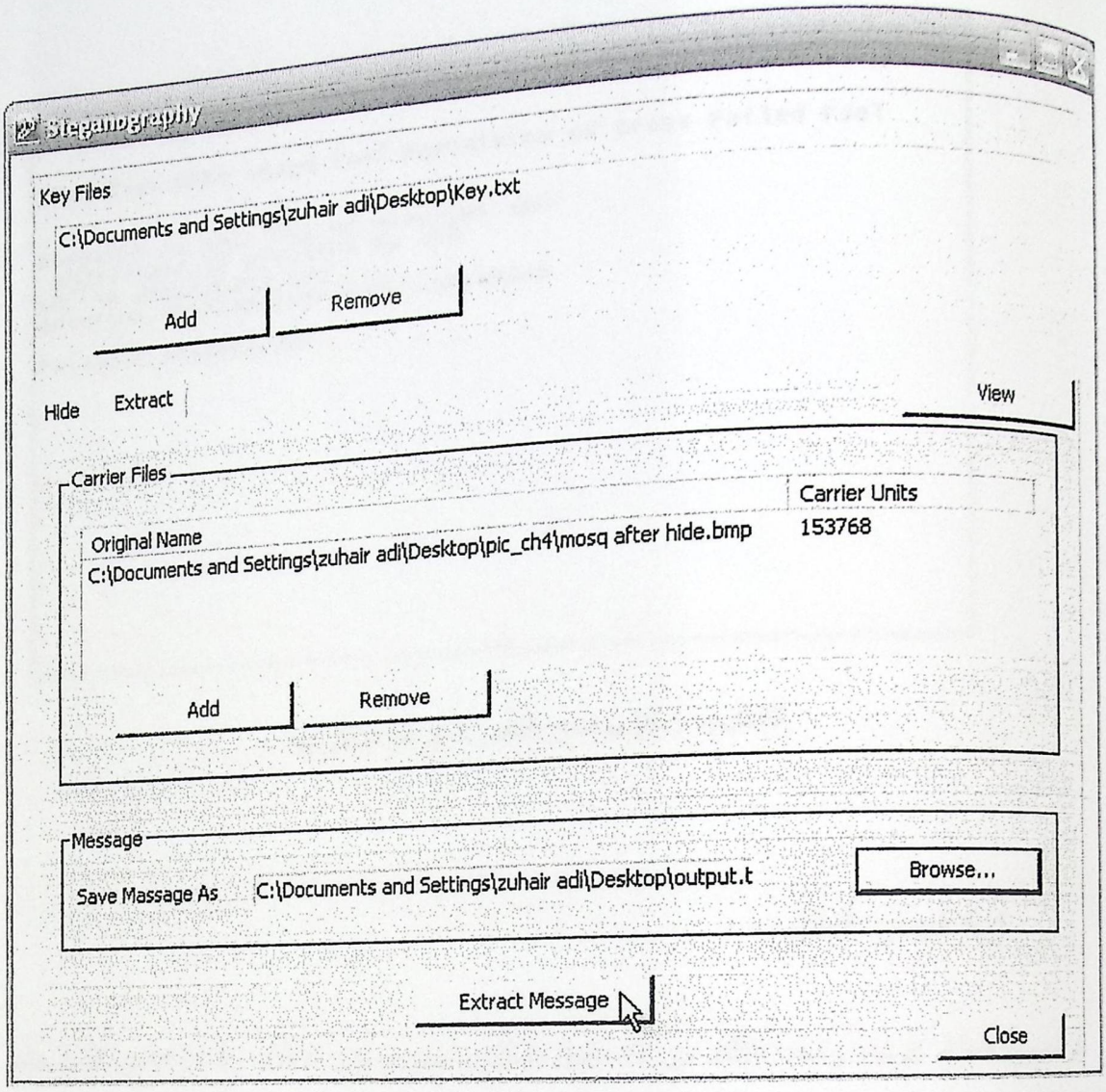
- فحص إضافة نص واستخراجه



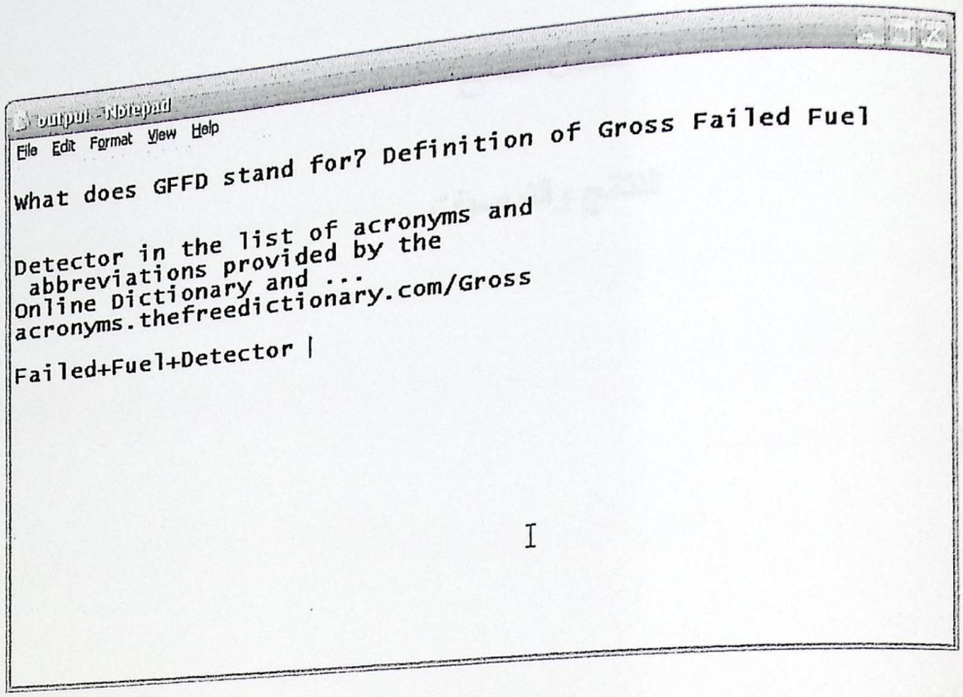
الشكل(6.13) يوضح النص المراد اخفائه



الشكل(6.14) يوضح عملية إضافة نص لإخفائه



الشكل(6.15) يوضح أنه تم استخراج النص من الصورة



الشكل(6.16) يوضح النص الذي تم استخراجه

6.4 فحص النظام:

تم فحص النظام كوحدة واحدة للتأكد من أنه يعمل بشكل صحيح وبدون أخطاء, وقد تم فحص العمليات التي يقوم بها النظام مع ملاحظة تأثيرها على أجزاء النظام الأخرى .

6.5 فحص قبول النظام:

تم في هذه المرحلة معرفة مدى تلبية النظام للمتطلبات التي تم ذكرها في الفصلين الثاني والثالث، ومن خلال مرحلة الفحص بكافة فروعها تم التوصل إلى أن النظام يطابق ويلبي المتطلبات.

الفصل السابع

النتائج والتوصيات

7.1 المقدمة

7.2 النتائج

7.3 التوصيات

7.1 المقدمة:

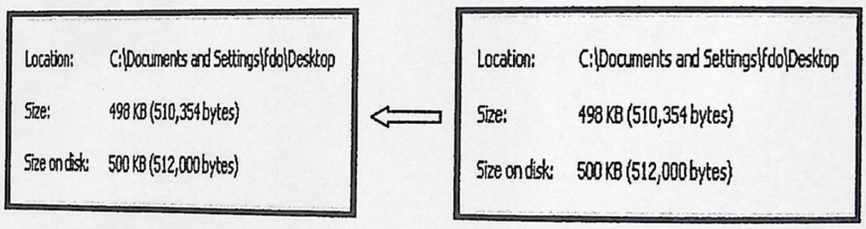
بعد الانتهاء من عملية تطوير نظام إخفاء الرسالة داخل الصورة، توصل فريق عمل المشروع إلى تحقيق الأهداف التي كان قد خطط لعملها, ونتائج تطبيق كل طريقة من طرق الإخفاء, بالإضافة إلى ذلك تم التوصل إلى مجموعة من التوصيات من شأنها تحسين النظام وزيادة كفاءته بالمستقبل.

7.2 نتائج تطبيق كل طريقة:

7.2.1 الطريقة الأولى:

عند إخفاء الرسالة بالاعتماد على طريقة LSB (8 bit)، سواء كانت الرسالة المـراد إخفائهـا قصيرة أو طويلة, فإن نتائج تطبيق هذه الطريقة تظهر كما يلي:

- المقارنة من حيث التأثير على الحجم: سواء كانت الصورة ملونه , أبيض وأسود, أم رمادية فإنه لا يوجد تأثير على حجم الصورة بعد الإخفاء داخلها وذلك لأنه يتم التعديل على قيمة آخر Bit من كل Pixel, فلا يوجد زيادة على عـدد ال Pixel في الصورة .



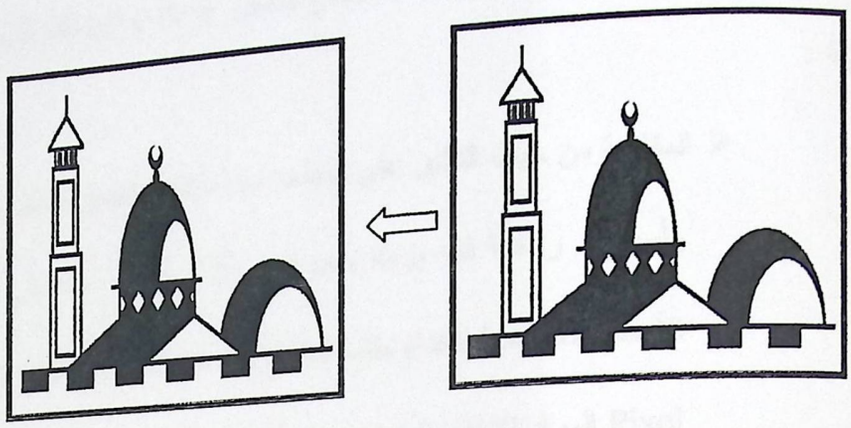
الشكل (7.1) مقارنة الحجم قبل وبعد الإخفاء باستخدام(LSB(8 Bit

- المقارنة من حيث التأثير على ألوان وملامح الصورة: سواء كانت الصورة ملونه, أبيض وأسود , أم رمادية فإنه لا يوجد تأثير على ملامح وألوان الـصورة بعـد الإخفاء داخلها, لأنه يتم التعديل على لون ال Pixel بدرجة واحدة, فمثلاً لإضـافة Bit قيمته 1 على ال Pixel فان التغير يظهر كما يلي:

Pixel ⇨ 11111000 11001001 00000011

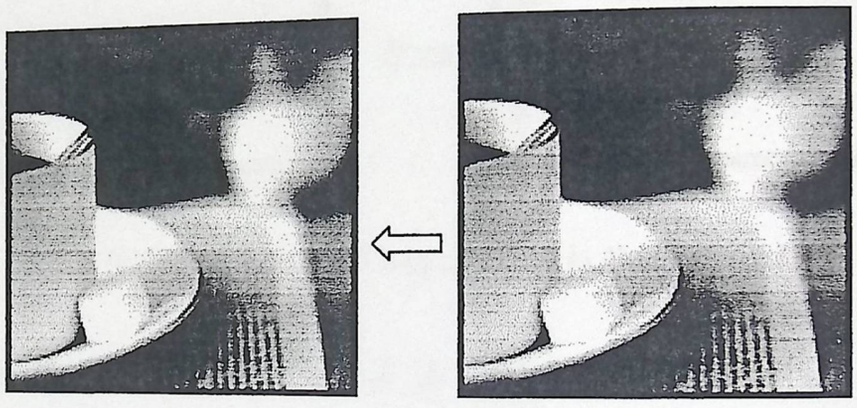
أزرق(3) أخضر(201) أحمر(248)

فإن اللون الأزرق يتغير بدرجة واحدة, فلا يكون لها تأثير واضح علـى اللـون النهائي في ال Pixel .



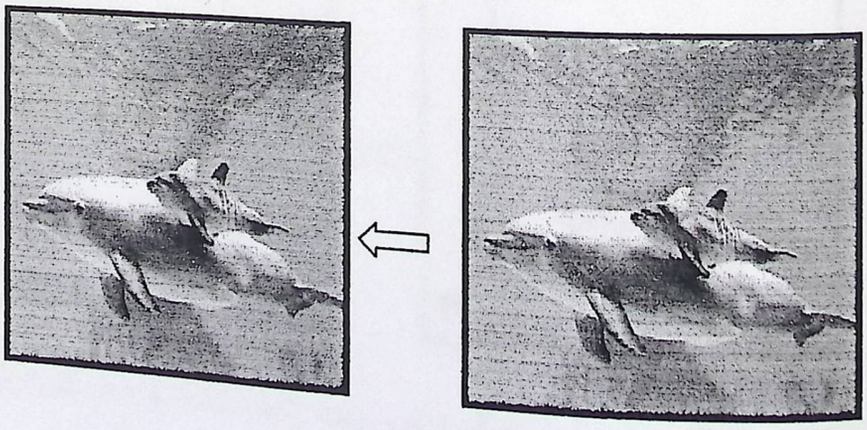
الشكل (7.2) صورة أبيض وأسود قبل وبعد الإخفاء باستخدام(LSB(8Bit

- في الصور الرمادية :



الشكل (7. 3) صورة رمادية قبل وبعد الإخفاء باستخدام LSB(8 Bit)

- في الصور الملونـــة :

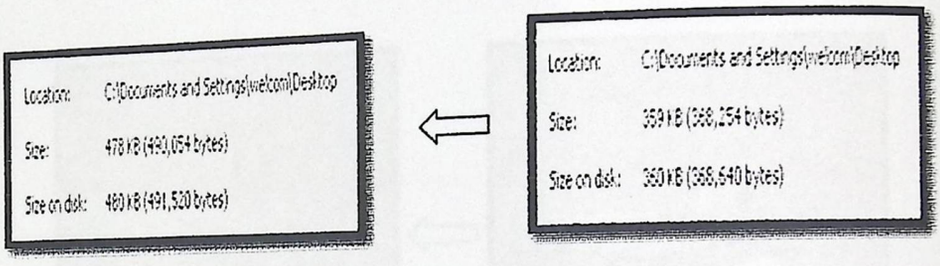


الشكل (7. 4) صورة ملونة قبل وبعد الإخفاء باستخدام(LSB(8 Bit

7.2.2 الطريقة الثانية:

عند الإخفاء في هذه الطريقة باستخدام ملف المفتاح للتشفير إذا كانت الرسالة المـراد إخفائهـا طويلة :

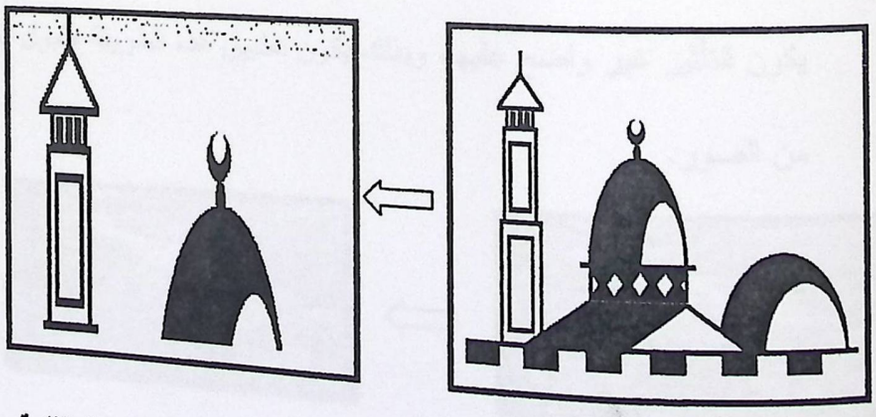
- المقارنة من حيث التأثير على الحجم: سواء كانت الصورة ملونـه, أبـيض وأسود, أم رمادية فإنه يزداد حجم الصورة الحاملة للرسالة عن حجم الصورة الأصلي لأنه يتم استخدام ملف المفتاح في هذه الطريقة لتحديد المسافة بين 2 Pixel المراد الإخفاء فيهما، وهذه القيم يتم الإحتفاظ بهـا وبالتـالي يزيـد حجمها.



الشكل (7.5) مقارنة الحجم قبل وبعد الإخفاء باستخدام الطريقة الثانية.

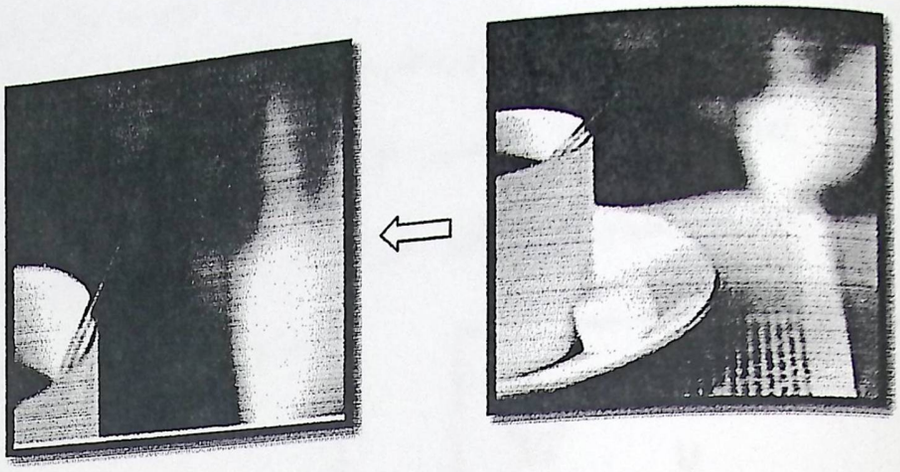
- المقارنة من حيث التأثير على ألوان وملامح الصورة: يكون التأثير نفسه على كل أنواع الصور لكن في الصور أبيض وأسود تكون اكثر وضوحاً .

▪ في الصور أبيض وأسود:



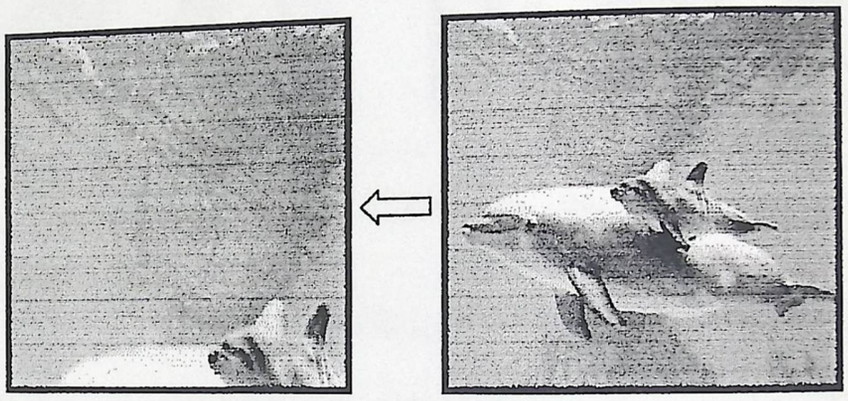
الشكل (7.6) صورة أبيض وأسود قبل وبعد الإخفاء باستخدام الطريقة الثانية

▪ في الصور الرمادية:



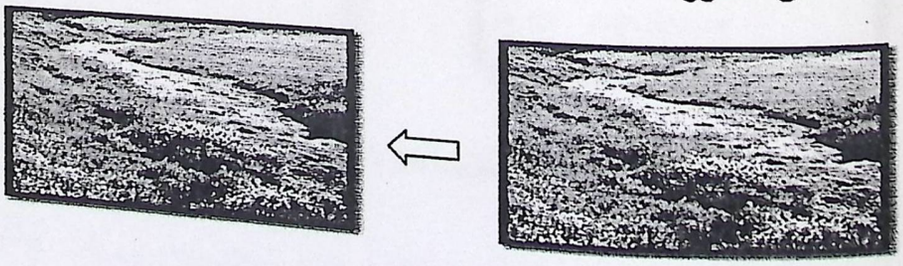
الشكل (7.7) صورة رمادية قبل وبعد الإخفاء باستخدام الطريقة الثانية

▪ في الصور الملونة:



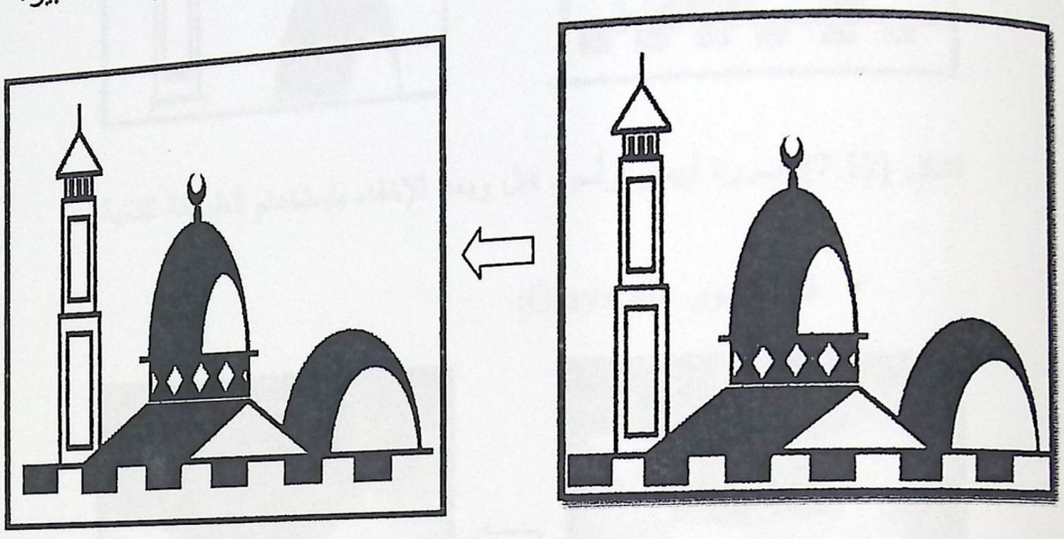
الشكل (7.8) صورة ملونة قبل وبعد الإخفاء باستخدام الطريقة الثانية

▪ وفي حالة تطبيق هذه الطريقة على الصور الملونة التي تحتوي على ألـوان كثيـرة، يكون التأثير غير واضح عليها، وبذلك يكون تطبيق هذه الطريقة مقبول لهذا النـوع من الصور.



الشكل(7.9) صورة ذات ألوان كثيرة قبل وبعد الإخفاء باستخدام الطريقة الثانية

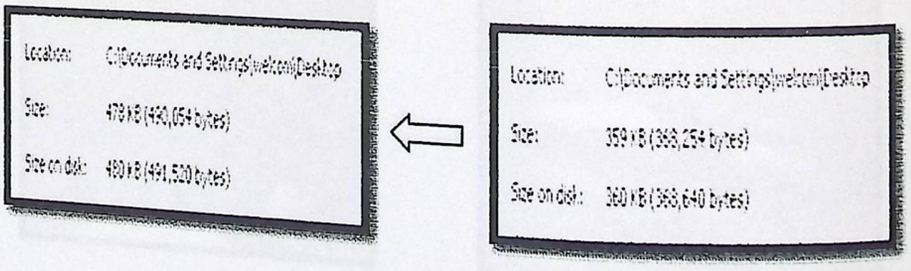
- عند تطبيق هذه الطريقة لإخفاء صورة داخل صورة، يجب مراعاة أن تكون الصورة الأصلية حجمها كبير والصورة المراد إخفائها حجمها صغير،لأنه يتم إخفاء في 3bit من كل Pixel من الصورة الأصلية لذلك نحتاج لزيادة حجم الصورة المراد الإخفاء بداخلها، ويكون التأثير على الصورة الحاملة للرسالة واضح بشكل كبير.



الشكل(7.10) إخفاء صورة داخل صورة باستخدام الطريقة الثانية

نتائج تطبيق هذه الطريقة إذا كانت الرسالة المراد إخفائها قصيرة:

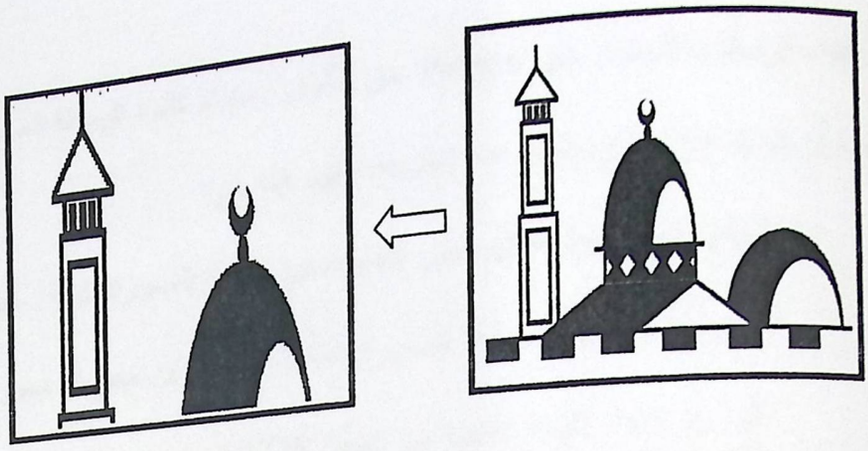
- المقارنة من حيث التأثير على الحجم: سواء كانت الصورة ملونة , أبيض وأسود, أم رمادية فإنه يزداد حجم الصورة الحاملة للرسالة عن حجم الصورة الأصلي لأنه يتم إخفاء القيمة الناتجة من عملية XOR في الصورة الحاملة.



الشكل (7.11) مقارنة الحجم قبل وبعد الاخفاء باستخدام الطريقة الثانية.

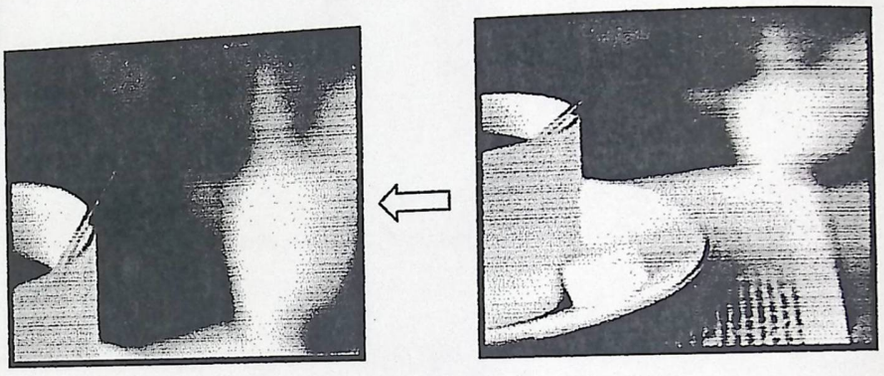
- المقارنة من حيث التأثير على ألوان وملامح الصورة: حيث يكون التأثير أقل على الصورة من لو كانت الرسالة طويلة، لأنه يتم إخفاء عدد أقل من الBit .

- في الصور أبيض وأسود:



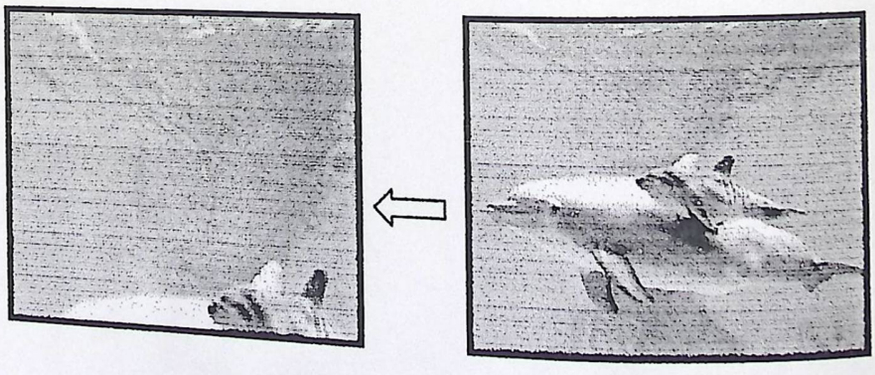
الشكل (7.12) صورة أبيض وأسود قبل وبعد الإخفاء باستخدام الطريقة الثانية

- في الصور Grayscale:



الشكل (7.13) صورة Grayscale قبل وبعد الإخفاء باستخدام الطريقة الثانية

- في الصور الملونة:

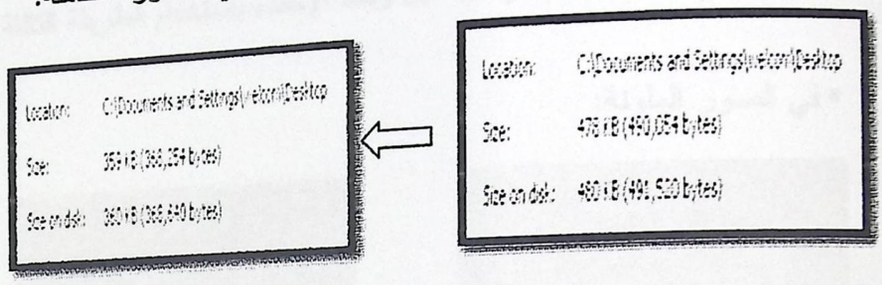


الشكل (7.14) صورة ملونة قبل وبعد الإخفاء باستخدام الطريقة الثانية

7.2.3 الطريقة الثالثة:

عند إخفاء الرسالة بالاعتماد على Palette من الألوان , سواء كانت الرسالة المـراد إخفائهـا قصيرة أو طويلة فإن نتائج تطبيق هذه الطريقة تظهر كما يلي:

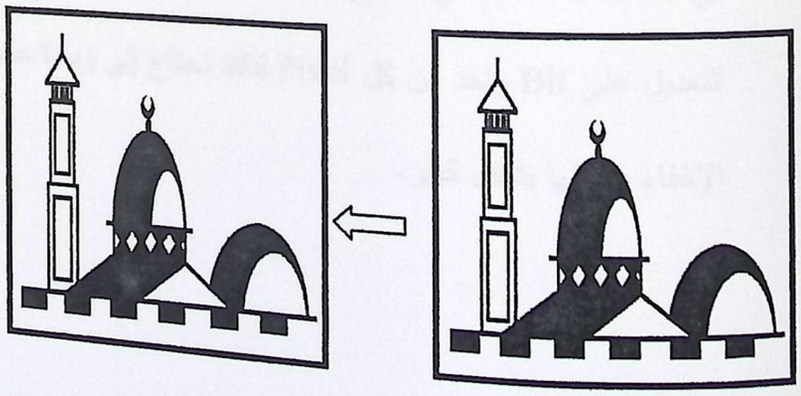
- المقارنة من حيث التأثير على الحجم: سواء كانت الصورة ملونة , أبيض وأسود , أم رمادية فإنه يزداد حجم الصورة الحاملة للرسالة عن حجم الـصورة الأصـلي لأنه يتم إخفاء القيمة الناتجة من عملية XOR في الصورة الحاملة.



الشكل (7.15) مقارنة الحجم قبل وبعد الإخفاء باستخدام الطريقة الثالثة

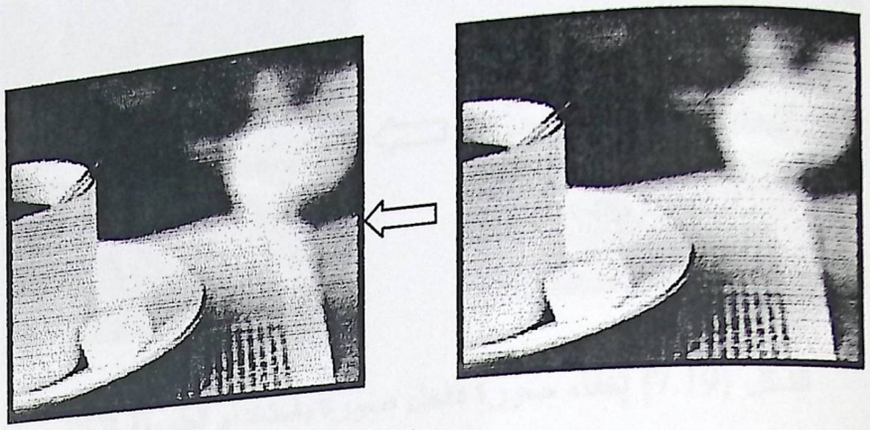
- المقارنة من حيث التأثير على ألوان وملامح الصورة: سواء كانت الصورة ملونة, أبيض وأسود أم رمادية، لا يوجد تأثير على ألوانها وملامحها لأنه يتم الإخفاء في الNew Palette حيث يتم الإخفاء على آخر Bit في ال Pixel الذي تم تحديـده عن طريق ملف المفتاح.

▪ في الصور أبيض وأسود:



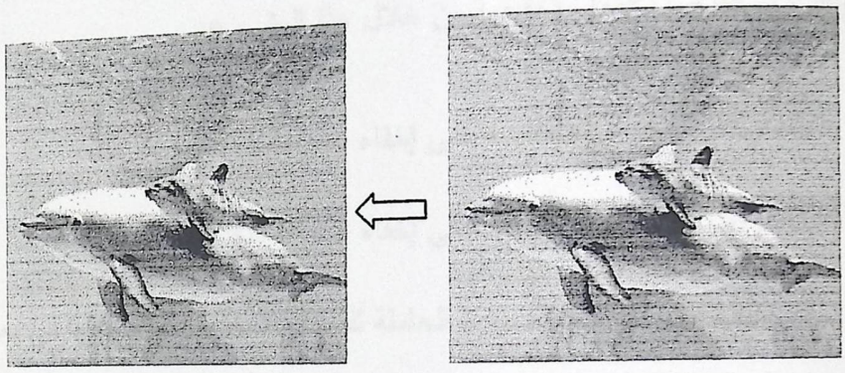
الشكل (7.16) صورة أبيض وأسود قبل وبعد الإخفاء باستخدام الطريقة الثالثة

▪ في الصور Grayscale:



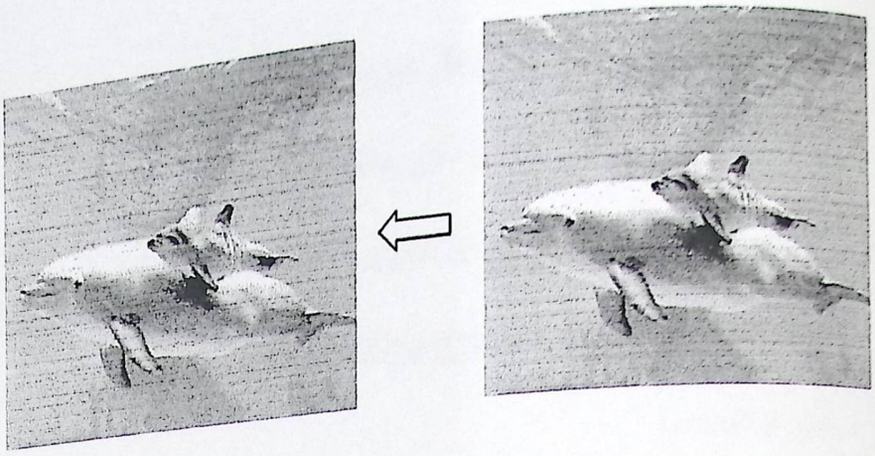
الشكل (7.17) صورة Grayscale قبل وبعد الإخفاء باستخدام الطريقة الثالثة

▪ في الصور الملونة:



الشكل (7.18) صورة ملونة قبل وبعد الإخفاء باستخدام الطريقة الثالثة

▪ عند تطبيق هذه الطريقة لإخفاء صورة داخل صورة، يجب مراعاة أن تكون الصورة الأصلية حجمها أكبر من الصورة المراد إخفائها، لأنه في هذه الطريقة يتم الإخفاء في new Palette التي تحتوي على ألوان إضافية للألوان الأصلية، حيث يتم التعديل على Bit واحد من كل Pixel لذلك نحتاج إلى زيادة حجم الصورة المراد الإخفاء بداخلها بشكل كبير.



الشكل (7.19) إخفاء صورة داخل صورة باستخدام الطريقة الثالثة

7.3 النتائج :

النتائج التي تم التوصل إليها وتحقيقها من خلال هذا المشروع:

1. بناء وتطوير نظام له القدرة على إخفاء نص داخل صورة.
2. بناء وتطوير نظام له القدرة على إخفاء صورة داخل صورة.
3. المحافظة على نوعية الصورة الحاملة للرسالة المخفية ومواصفاتها في بعض الطرق.
4. المحافظة على ألوان ومظهر الصورة الحاملة للرسالة بحيث لا يثير الشك بوجـود أي تغيير في بعض الطرق.
5. المحافظة على أمان الرسالة المخفية حتى وصولها إلى الطرف المقصود، وقدرته على فك الإخفاء والحصول عليها باستخدام ملف مفتاح الإخفاء.

7.4 التوصيات:

كالشمس التي لا تتوقف عن الإحتراق لتنير عالمنا سيبقى تطوير مشروعنا، وفي الوقت الراهن لقد قمنا باستنفاذ كافة جهودنا التي نستطيع بذلها لنخرج عملاً متكاملاً متقنـاً كجمـال الـسماء فابتساعها تطوير مشروعنا سيبقى، ومن توصياتنا المستقبلية:

1. أن يتم تعزيز وتوسيع عمل النظام على مختلف أنواع ملفات الصور، مثل: GIF، JPEG، وأن لا يكون مقتصراً على ملفات الصور من نوع Bitmap.
2. تطوير النظام والعمل على تقسيم الصورة الحاملة للرسالة المخفية إلى أجزاء على شكل Block، لنستطيع استرجاع بيانات الرسالة من الصورة إذا تم فقدان جزء من أجزاء الصورة.
3. العمل على تحسين الأمان الأكثر لمحتوى الرسالة (Authentication).
4. العمل على زيادة كفاءة تقنيات الحماية لمقاومة الآليات المستخدمة لكشف الرسالة المخفية واختراق النظام.
5. أن يتم تعزيز وتوسيع عمل النظام ليشمل اخفاء ملفات صوتية داخل الصور.
6. أن يتم تعزيز وتوسيع عمل النظام بأن يتم الإخفاء داخل ملفات نصية أو ملفات فيديو.

(n.d.). Retrieved from www.zap.co.il.

Cole, E. (October, 2003). *Hiding in Plain Sigh.* Wiley publishing.

Elizabeth. (25-27 July 2004). *COVERING ENCRYPTING INFORMATION USING IMAGES* .

Johnson, N. (February1998). *ExploringSteganography* .

Katzenbeisser, S. *Information Hiding Techniques for Steganography and Digital Watermarking.*

Kipper, G. (2004). *Investigator's Steganography.* CRCnetBASE.

Mamta Juneja, P. S. (2005). *Implementation of Improved Steganographic Technique for 24-bit Bitmap Images in Communication* .

Rymon, D. (2008/9). *Steganography and history of cryptography* .

ع .و ,الرحيم. *مقدمة في التشفير بالطرق الكلاسيكية*(Classical Cryptography).

سعد), و. (. (2000-2005). *أمن المعلومات!*