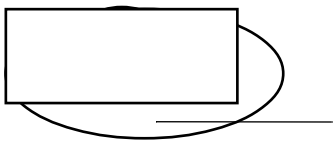


بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية علوم الحاسوب وتقانة المعلومات

تحسين إخفاء المعلومات داخل الصورة الرقمية بإستخدام الإخفاء متعدد الطبقات

Improve hide information within digital hide using a multi-layered image

بحث مقدم كأحد متطلبات الحصول علي درجة البكلاريوس في علوم الحاسوب

اشراف:

أ: متوكل فيصل

إكتوبر 2016م

بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية علوم الحاسوب وتقانة المعلومات

تحسين إخفاء المعلومات داخل الصور الرقمية باستخدام الإخفاء متعدد الطبقات

إعداد:

- إسراء تاج الدين حماد الشيخ هجو
- خديجة الصافي عبد الرحمن حسين
- محمد عبد الرحمن المبارك الجابري

بحـث مقـدم كأحـد متطلبـات الحصـول علـي درجـة البكلاريوس في علوم الحاسوب

إشراف:

أ: متوكل فيصل

التوقيع:..... تاريخ

التوقيع :.....

إكتوبر 2016 م

الآية

قـــال تعالـــى :

(قَالُوا سُبْحَانَكَ لا عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيم)

سورة البقرة الآية (32)

الإهداء

باسم معاني الود والاحترام يسعدني أن أهدى هذا الجهد المتواضع ,,,

إلى ...الذي يكابد الآلام ويعانق الصعاب لينير لنا الآفاق ... من علمنا أن لأحيد عن مبادئنا ولا نساوم بقيمنا ...إلى من كان مربيا ومرشداً لنا...

(ابائنا)

إلى ...رمز المحبة والصبر ..إلى شجره الظل...إلى الحنون...إلى من تحته قدميها جنات الخلد ..إلى من رفعت أكفها إلى السماء داعية لنا بتذليل الصعاب ...وتيسير دروبنا.

(اُمهاتنا)

إلى ...من نفخر بهم ونعتز بوجودهم...إلى زهور تملأ القلوب بهجة والحياة فرحاً والأيام جمالاً...

(أخوتنا)

إلى ...كل من ساندنا وساعدنا...الى من أضاءوا لنا دروب العلم والمعرفة.

الشكر والعرفان

الحمد والشكر لله رب العالمين الرحمن الرحيم عالم الغيب والشهادة القوى المتين خالق الإنسان مجربالزمانمكون المكـان الحميـد المنعـم المنـان علـى صـفوه خلقه ودره رسله الشـفيع المشـفع صـاحب الخلـق العظيـم والطبـع الكريـم والـرأي السليم والقلب الرحيم سيدنا ومولانا محمد بن عبدالله النبي الأمي الأمين وعلى آله الطاهرين الطيبين وصحابه الغر الميامين وعلى من تبعه هداء وسار على نهجـه إلـى يوم الدين.

بعبارات تسقي الـورود عـبير وشـذي وتملا الكـون جمـالاً وسـعداً كلمـات تتجـه الـى أساتذتنا لم قدموه لنا من آداب ومكارم الأخلاق والتقدير.

والشكر إلى كل من ساهم معـي فـي أن نبلـغ هـذه المرحلـة المتواضـعة وكـل مـن ساندنا ومدنا بفكره وجهده ووقته.

المستخلص

توجد مجموعة من التقنيات لحمايه المعلومات مثل إخفاءها. Steganographyهي واحده من تقنيات إخفاء المعلومات حيث تقوم بإخفاء المعلومات أوالرسائل في داخل رساله أخرى بدون لفت الانتباه لذلك. هنالك عدة وسائط لإخفاء البيانات منها الفيديو وملفات الصوت لكن الصور الرقمية هي الأكثر استخداما.

حماية البيانات عن طريق التشفير يجذب الإنتباه لمهاجمته. لذلك تم إستخدام تقنية إخفاء المعلومات في هذا البحث. يهدف هذا البحث لإخفاء المعلومات السريه في عدة طبقات، الطبقه الاولي هي عباره عن تشفير النص المراد ارساله والطبقة التانية يقوم النظام بإخفاء النص المشفرة في الصورة.

تم قياس نتائج الصور باستخدام تقنيات PSNR و MSE على عدة صور باحجام **مختلفة وطول نص مختلف. أظهرت النتائج مقاييس جيدة من حيث إخفاء الرسالة السرية.الشخص** الذي ينظر للصورة، لايمكنه تمييز وجود نص داخلها.

Abstract

A lot of techniques are used to protect the information such as information hiding. Steganography is one of the information hiding Techniques that hide a message inside another message without drawing any suspicion.

There are many modes to hide digital data, include video and audio files but digital image is more use. Data protection through encryption attracts the attention of some people to attack the encryption cryptanalysis.

This research aimsto hide secret information in many layers, the first layer is encrypting the text to be sent and in second layer the system hides the encrypted text within picture.

Results were measured using images PSNR and MSE on several pictures of different sizes and different text’s length. The results showed good measures in term of hide the secret message. The person who sees the image cannot distinguish that there are a text within it.

المصطلحات

المصطلح	التعريف
LSB	Least Significant Bit
MLS	Multi-Level Steganography
UML	Unified Modeling Language
K	Key
HTTP	Hyper Text Transfer Protocol
SSCE	Secret Steganography Code for Embedding
PMM	Pixel Mapping Method
PSNR	Peak Signal to Noise ratio
MSE	Mean Squire Error

شرح الرموز المستخدمة في تحليل ال UML

وصف الشكل

اسم الشكل

الشكل

قد يكون شخص،أو ألة،أو جزء اخر من نظام.

Actors

يصف ويبين تفاعل وحيد مع مرور الزمن للمستخدم النهائي للنظام لاداء وظيفة محددة.

use cases

نوع العلاقة العام بين العناصر.

Association

association

العلاقات بين حالات الاستخدام

Extend

<-----.Extend---

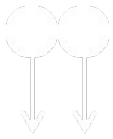
Decision Node

No

Yes]

يشير إلي الإجراء (او الإجرات) الأول في النشاط.

Initial Node



نهاية النشاط.عند وصول رمز مميز ،النشاط ينتهي.

Final Node

فيها المستخدمون أو البرامج يقومون بتنفيذ بعض المهام.

Activity/Action Node

فهرس الأشكال

فهرس الجداول

الفهرس المحتويات

الباب الأول

المقدمة

1.1 المقدمة:

عملية الاتصال بين الناس من أهم الوسائل التي ساعدت على النمو البشري، وتتطلب هذه العملية سرية البيانات المنقوله، ولهذا الغرض فقد سعى الإنسان إلى إيجاد طرق متنوعة يضمن من خلالها وصول البيانات بسرية مطلقة.يوجد العديد من التقنيات المستخدمة للحفاظ علي امن وسرية المعلومات كالتشفيرو (Watermarking) .

ظهرالتشفير كطريقة جيدة لحماية البيانات المرسلة, وكانت الفكرة بان الاتصالات قد تكون في امان من خلال تشفير لكن هذا نادرا ما يكون صحيح في الوا قع العملي, فبرزت الحاجة لإيجاد طرق لإخفاء الرسائل بدلا من تشفيرها.

ومع ومع تطور عمليات الاختراق أصبح بإمكان المتطفلين الاطلاع على المعلومات وتغييرها، فظهرت الحاجة إلى اعتماد تقنية أكثر تطورا وأكثر سرية وحفاظا على المعلومات. لذا تم استخدام نظام الإخفاء الذي تكون فيه المعلومات المرسلة غير مرئية لأي شخص وذلك عن طريق إخفائها داخل الوسائط المرسلة، مثل الصوت، الصورة والفيديو.

الهدف الأساسي من الإخفاء هو توفير الحماية للأشخاص ليتم الحفاظ على أمن معلوماتهم.وكما هو معلوم فلا يمكن الاستغناء عن ميزة أمن المعلومات في المواقع الحساسة مثل البنوك والتجارة الالكترونية والمواقع الأمنية.

2.1 مشكلة البحث:

تكمن مشكلة البحث الأساسية فى أن حماية البيانات عن طريق التشفير يجذب انتباه البعض لمهاجمة التشفير (cryptanalysis) .

3.1 منهجية البحث:

سيتم عمل نظام متعدد الطبقات لإخفاء البيانات يقوم بتشفير النص ثم وضعها في الخانة الثانية الاقل اهمية مع مفتاح في(Header) الخاص بالصورة لزيادة سرية النص، ثم يتم إخفاء النص المشفر في الصورة .

4.1 أهداف البحث:

- إستعمال اكثر من مستوي من إخفاء البيانات مما يزيد من سرية البيانات التي تم إخفاؤها.زيادة تعقيد في استرجاع البيانات المخفية.

- إنشاء تطبيق يقوم بعملية الإخفاء وإسترجاع البيانات.

5.1 حدود البحث:

إستخدام تقنية ((LSB في إخفاء البيانات داخل الصور فقط بإستخدامتقنيةالإخفاء متعدد المستويات .(MLS)

6.1 هيكلية البحث:

هذا البحث مقسم الى عدة ابواب الباب الأول يستعرض مقدمة عامة عن البحث والباب الثاني الفصل الأول يشرح مفاهيم عامة عن علم إخفاء المعلومات والفرق بين علم التشفير وعلم الإخفاء, والفصل الثاني يعرض أهم الدراسات والم قترحات التي قدمت في علم إخفاء المعلومات في الصورة, والباب الثالث يعرض تحليل النظام الم قترح والتقنيات والأدوات المستخدمة, والباب الرابع يستعرض التطبيق, الباب الخامس يتضمن النتائج التي توصلنا اليها والتوصيات الم قترحة.

الباب الثاني

الفصل الاول

أدبيات البحث

1.1.2 مقدمة:

مع نشأة الحاسوب وتطور الوسائل المعلوماتية لأرسال وإستقبال ومعالجة المعلومات برزت الحاجة الى إيجاد وسائل لمنع المتطفلين من سرقة وكشف البيانات والمعلومات المهمة.[1]

2.1.2 التشفير:

هوعبارة عن تحويل النص الصريح الي مبهم، تستخدم أغلب خوارزميات التشفير مفتاح (K) في بعض الأحيان تكون مفاتيح التشفير وفتح الشفرة هي نفسها ويسمى هذا النوع من التشفير بالتشفير المتناظر(Symmetric). وفي أحيان اخرى تكون مفاتيح التشفير وفتح الشفرة على شكل أزواج تسمي خوارزميات التشفير هذا النوع غير متناظر [1] .(Asymmetric)

وعلى الرغم من كون التشفير طريقة جيدة لحماية المعلومات إلا أنه سهل الإكتشاف، ويمكن لأي متطفل التلاعب بها، فكانت الحاجة إلى تـ قنية أكثر تطورا وأكثر سرية وحفاظ على المعلومات وخصوصا مع ظهور وتطور الشبكة العالمية للمعلومات(Internet) فتم اللجوء إلى نظام الإخفاء، لأن رؤية البيانات بصيغتها المشفرة تكفي لدفع المتطفل أو المهاجم إلى الإعتـ قاد بوجود بيانات مهمة أو حساسة تكمن في العشوائية أو في النص المشفر، فيبدأ بإستخدام التـ قنيات المضادة للتشفير لمحاولة الحصول على محتواها، وحتى لو عجز عن تحـ قيق ذلك فأنه قد يعبث بها أو يحرفها أو يستخدم بعض الوسائل المتاحة لمنع وصولها إلى هدفها.[2]

3.1.2 ثلاثة مفاهيم في التشفير:

- المفاتيح الخاصة والعامة:

أحد أهم المفاهيم التي يتوجب معرفتها في التشفير هو المفتاح يسمح لك المفتاح الخاص بوضع توا قيع ر قمية لا يمكن تزويرها على الرسائل التي ترسلها إلى الآخرين، والمفتاح العلني هو ملف يمكنك إعطاؤه للأخرين أو نشره.

- شهادات الأمان:

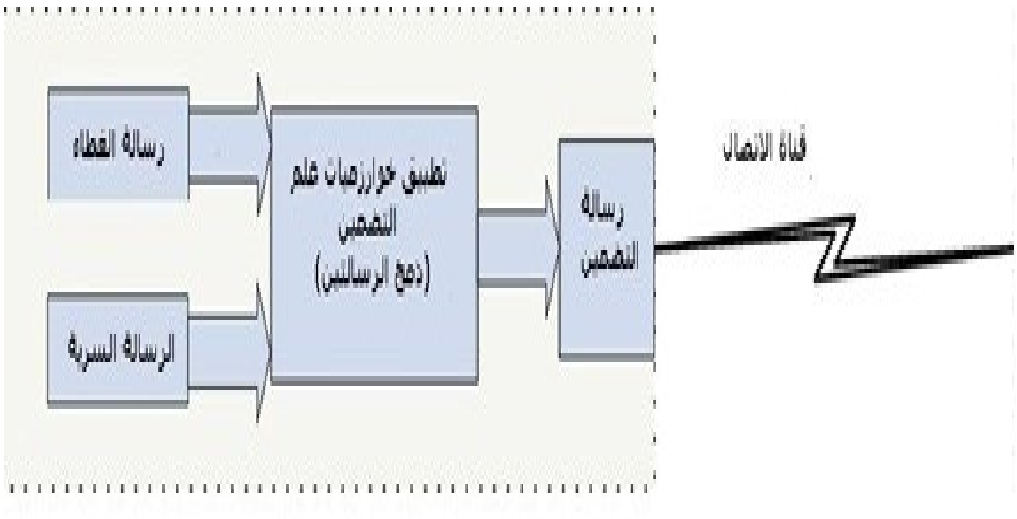
شهادة الأمان هي مفهوم آخر من المهم معرفتة وفهمة، يمكن لمتصفح الإنترنت على جهازك إجراء إتصالات مشفرة مع المواقع باستخدام(HTTP)، عندما يقوم بذلكفإنه يتفحص الشهادات للتأكد من المفاتيح العلنية لأسماء النطاقات، مثل www.google.com أو www.amazon.com أو ssd.eff.org الشهادات هي إحدى الطرق لتحديد ما إذا كنت تعرف المفتاح العلني الصحيح لشخص أو موقع ما، بحيث يمكنك التواصل معهم بشكل آمن.

- بصمات المفاتيح:

إحدى إستخدامات المصطلح هي "بصمة المفتاح"، وهي سلسلة من الأحرف مثـل "1928 2192 6c63 ff10 0912 bd20 2309 342e " تسـمح لـك بالتحقق بشكل فريد من أن شخصاً مـا علـى الإنـترنت يسـتخدم المفتـاح الخـاص الصحيح .

4.1.2 الإخفاء:

هو علم وفن وتضمين البيانـات المـراد إرسـالها (قـد تكـون رسـائل نصـية أو صورة)داخل بيانات مرسلة (قد تكون صورا أو ملفـات الصـوت أو الفيـديو) وذلـك لإحتوائها علي كمية كافية من البيانات التي تمكن المسـتخدم مـن إخفـاء البيانـات داخلها كما مبين في الشكل التالي:[3]



الشكل(1.2): تقنية إخفاء المعلومات

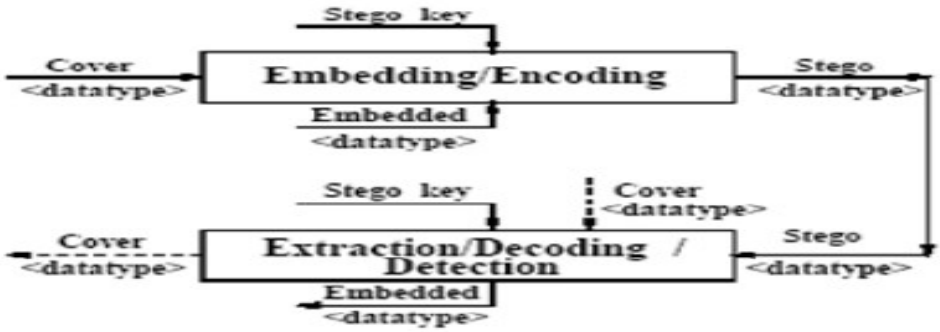
(Steganography)الكلمـة مـن أصـل يونـاني و (stegano)تعنـي "مغطـاة أوالخفية"و(graphy) كتابة تم تحديد فيم الإخفاء المعلومات أربعة أشياء [4]:

أ/النص (Hidden Message): الرسالة السرية المراد إخفاها.

ب/غطاء (cover): الصورة أوالصوت التي سيتم إستخدامها لإخفاء النص.

ج/مفتاح(key): هو مفتاح يستخدم لتضمين النص داخل الغطاء.

د/كائن Stego: هو جمع بين النص، غطاء ومفتاح.



الشكل(2.2): نظام إخفاء العام

5.1.2 تاريخ علم الإخفاء:

علم الإخفاء لا يعد من العلوم المستحدثة، كان أول ظهور لهذا العلم في العصرالإغريقي، **حيثقـامأحد رجالات العصرالتواصلمع احد أقربائهفي اليونان، عنطريق حلق شعر رؤوس** عبيده ثم وشم الرسائل على رؤوسهم بعد ذلك يقوم بانتظار نمو شعر رأسهم ثم إرسالهم إلى **الشخص الذي يهدف إلىالتواصلمعه ثم جاء بعده العديد من الأشخاص الذين إستخدموا الناس** والحيوانات والخشب المغطى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية.

وإستمر تطور هذا العلم حتى توصل العالم إلى إختراع الحبر الخفي إبان الحرب العالمية الثانية والذي ساهم كثيرًا في التواصل بين الجبهات في الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الأسرار، و قد تطور علم الإخفاء في الوقت الحالي كثيرًا، فأصبح يستخدم المعلومات الرقمية والحواسيب كوسيلة لنقل البيانات [5].

6.1.2 طرق اخفاء البيانات:

Pure Steganography هو النوع أو النمط العادي والخام من الأنماط المستخدمة لإخفاء المعلومات، هنا يتم تضمين المعلومات أو الرسالة الخفية داخل الوسيط بشكل مباشر وبدون كلمة سرية.

Secret Key Steganographyهو يعني إخفاء المعلومات بإستخدام مفتاح أو كلمة سرية تضاف للرسالة المخفية عند إخفاؤها داخل الوسيط المستهدف، وهكذا لا يمكن إسترجاع أو قراءة الرسالة المخفية من قبل الطرف الثاني إلا بمعرفة الكلمة السرية، وبإضافة الكلمة السرية لعملية الإخفاء تكون العملية آمنة ومعقدة أكثر.

Public Key Steganography هو يعني إخفاء المعلومات بإستخدام مفتاح عام، والعملية هنا تشبة العملية المتبعة في التشفير عن طريق إستخدام

مفتـاحين، الأول مفتـاح "عـام" ويسـتخدمه الشـخص الأول عنـد عمليـة إخفـاء المعلومة، ويتم إستخدام المفتاح الثاني "الخـاص" مـن قبـل الشـخص المسـتقبل عند إسترجاعه للمعلومة المخفية، مع العلم أن المفتاح الخاص له علاقـة مباشـرة مع المفتاح العام [3].

7.1.2الوسائط المستخدمة في إخفـاء البيانات:

1. الملفات النصية:

عن طريق إخفـاء الرسـالة المـراد إرسـالها بإسـتخدام النصـوص، وتتـم هـذة الطريقة إما بطريقة نصية، مثلا: يكونأول حرف مـن كـل كلمـة يمثـل حـرف مـن الرسالة المخفيةأو بطريقة نحوية أو لفظية، ويعتـبر هـذا النـوع مـن الإخفـاء مـن أصعب أنواع الإخفاء.

2. الملفات الصوتية:

عن طريق إخفاء الرسالة المراد إرسالها بإستخدام داخل إشارة صوتية يمكن أن تكون في مجال الزمن أو مجال الطيف.

3. مقاطع الفيديو:

يعتبر الإخفاء بإستخدام ملفات الفيديو جـزءا مشـتقاً مـن الإخفـاء بإسـتخدام الصور، وذلك لأن ملفات الفيديو عبارة عن صورة مجتمعة، لأجل هـذا تقنيـات بالصور يمكن إستخدامها في هذه الطريقة.

4. الصور:

عن طريق إخفاء الرسالة المراد إرسـالها بإسـتخدام ملـف صـوري، يعـد هـذا النوع من الإخفاء من أكثر الأنواع إنتشارا في الإستخدام لمـا تتميـز بـة الصـورة من صفات تجعلها الوسط المثالي للإخفاء.

ويتم تطبيق هذه النوع من الإخفاء بإستخدام أحد الطرق التالية:

- الإخفاء بإستخدام التحويل الزاوي المتقطع (Discrete Cosine Transformation)
- **الإخفاء باستخدام التحويل الموجي** (Discrete Wavelet Transform)
- الإخفاء باستخدام الإدخال في البت الأقل أهمية (Least Significant Bit)

وتعد طريقة الإخفاء في البت الأقل أهمية من أكثر الطرق شيوعًا، التي سوف يتم إستخدامها في هذا المشروع.

8.1.2 تقنية البت الأقل أهمية(LSB) :

تتم عملية الإخفاء بصورة عامة بتحويل الملف المراد إخفائه إلى سلسلة من (Bits) يتم إخفاؤها داخل (Bytes) عناصر الصورة وذلك باستبدال عدد من بايت عنصر الصورة بنفس العدد من بتات الحرف المراد اخفاؤه في مواقع البتات الأقل أهمية. [5]

9.1.2 الفرق بين الإخفاء والتشفير:

إخفاء المعلومات وتشفير المعلومات عبارة عن وسيلتان مختلفتان من وسائل حماية المعلومات, ففي التشفير يمكن لأي طرف أن يكتشف إن ثمة طرفين يتصلان بطريقة مشفرة، أما في إخفاء المعلومات فيخفى أصلا وجود الاتصال فلا يمكن لأحد أن يلاحظ وجود طرفين يتبادلان الرسائل عبر قنوات الاتصال. وثمة فروقات عديدة بين إخفاء المعلومات والتشفير وهي موضحة في الجدول التالي:[1]

جدول(1.1.2): **الفرق بين إخفاء المعلومات والتشفير**

إخفاء المعلومات	التشفير
يعمل على إخفاء وجود المعلومات	يعمل على إخفاء محتويات المعلومات
يحاول إخفاء وجود اتصال	يكون الاتصال دليلا
النتيجة النهائية لإخفاء المعلومات هي عنصر الإخفاء	النتيجة النهائية للتشفير هي النص المشفر
ليست ثمة خوارزمية محددة بل يعتمد على الطبيعة البشرية في الإخفاء	يعتمد على خوارزميات معروفة

الفصل الثاني

الدراسات السابقة

1.2.2 المقدمة:

تعتبر الصورة واحدة من أكثر أنواع الوسائط المستخدمة في إخفاء البيانــات لما تمتاز بة من مواصفات تجعلها وسيط مناسب للإخفاء ومن مميزاتها عدم تغيــر الحجم والوان الصورة قبل وبعد الإخفاء كما أن الصورة المضمنة بداخلها الرسـالة السرية يمكن نشرها بسهولة علي مواقع الانترنت.

أمافي هذة الدراسـة سـوف نتنـاول تقنيـة(MLS) تسـمي هذةالتقنيـة إخفـاء متعدد المستويات، الإخفاء متعدد المسـتويات لديـة ميـزة صـعوبة الفـك وإمكانيـة إرسال رسالتين سريتين من خلال كائن واحد.

2.2.2 الدراسات السابقة:

1. **زيادة سعة اخفاء المعلومات بطريقة ال(LSB) للنص والصورة:**

هذه الدراسه مقدمـة مـن قبـل ((pallaviN.Halanka, ArchanaAthawale 6]]أقترحت تحسين طريقة الخانة الثنائيه الأقل أهميه لزيادة سعة التضمين والـدقه، وهـذه الطريقـة يمكـن تطبيقهـا علـي الصـوره ذات الحجـم 24 خـانه ثنائيـة، ويتـم إستخدام مفتاح سري طوله ثمانية خانة ثنائيـة وقبـل أن تتـم عمليةالتضـمين تجـري عمليه (XOR) للمفتاح السري والخانات الثنائية في الرسالة وكل نقطة في الصـورة تحلل ويتم إجراء العمليات الاتية:

- إذا كـانت قيمـة النقطـة فـي الصـورة أكـبر مـن أو يسـاوي 240 وأقـل مـن أويساوي 255 سوف يتم تضمين أربعه خانات ثنائية من البيانات السرية فــي أربعه خانات من الجهة اليسري.
- إذا كانت قيمة النقطـه أكـبر مـن أو يسـاوي 224 وأقـل مـن أويسـاوي 239 سوف يتم تضمين ثلاثة خانات ثنائية من البيانات السرية في ثلاثة خانات مــن الجهة اليسري .
- إذا كانت قيمة النقطـة فـي الصـورة اقـل مـن أو يسـاوي 223 وأكـبر مـن أو يساوي 192 سوف يتم تضمين خانتين ثنائتين من البيانات السرية في خانتين من الجهة اليسري.

إذا كانت قيمة الصورة أقل من أو يساوي 192 وأكبر من أو يساوي 0 سـوف يتـم تضمين خانة ثنائيه من البيانات السرية في الخانة الأخيرة من الجهة اليسري، هذة الطريقة لها مميزات منها زيادة السعة لتضمين المعلومات وسهولة وأداء افضل.

2. إخفاء البيانات بسعه عالية مبنية علي طريقة LSB

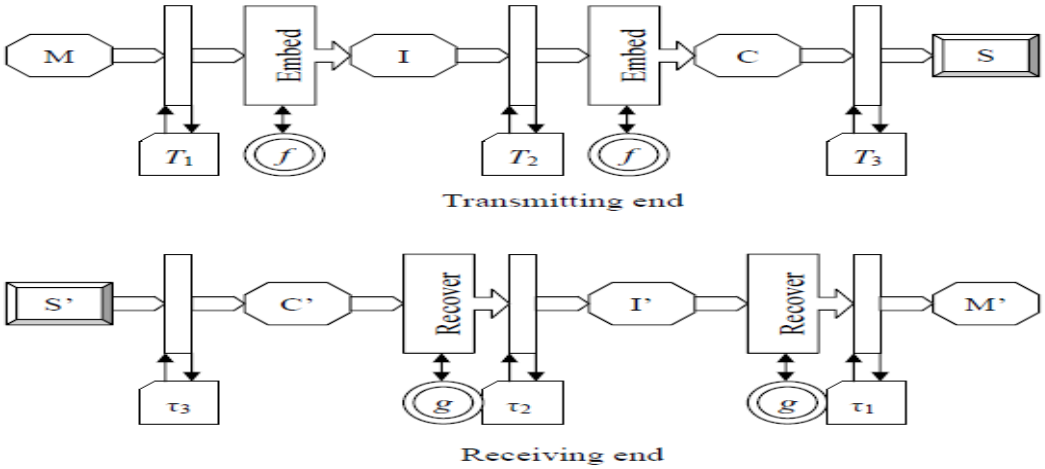
في الدراسة التي قدمها ((Rajanikanth Reddy Koppola[7]الهدف منها إقتراح تقنية جديدة لإخفاء كمية كبيرة من البيانات. وهذة التقنية تسمح بإخفاء صورة داخل صورة أخرى لها نفس الحجم يتم تقليل حجم الرسالة السرية قبل الإخفاء لإخفاء كمية أكبر من البيانات . ويتم إخفاء البيانات في المناطق من الصورة التي لا تستطيع العين إدراك الإختلاف في الألوان . تم إستخدام تقنية (RGBA) عباره عن قيمة تتراوح بين 0-255 حيث قيمة 0 تعني الصورة شفافة والقيمة 255 تعني الصورة معتمة . هذة التقنية صعب الهجوم عليها عند رؤية الصورة ولكنها قابلة للهجوم عن طريق الطرق الإحصائية ويمكن التغلب عليها بإستخدام الضغط لزيادة سرية الصورة المستخدمة كغطاء. من مساؤي هذه الدراسة تعاني من فقدان البيانات عند الاسترجاع لكنها تمتاز بجودة عالية بالإضافة إلي كمية كبيرة من البيانات.

3. تقنية تعدد المستويات في الصور:

في الورقة النجار[8] حول إخفاء المعلومات متعددة المستويات، في المستوى الأول يتم وضع الرسالة النصية (M) فى صورة من الأبيض والأسود (الهدف الوسيط (-ID)، والمستوى الثاني ياخذ من خرج المستوى الأول "اخفاء صورة ابيض اسود " كمدخل إلى صورة RGB (الثانية تغطى الهدف (C)). افترض ان العناصر M تعطى فى شكل مجموعة {M} من حجم المصفوفة | M |. يتم ترميز كل عنصر من عناصر M ب (nb (M لكل بت. وبالمثل، {I} من حجم | ،| I C}} من حجم | C |، و {S} من حجم | S | تحدد مجموعات واحجام كل عنصر لفك الشفرة فى المرحلة المتوسطة (الشفرة المغطاة) على التوالي. وهذه الاهداف الوسيطة {I, or D} تعمل كشكل غطاء للرسالة الستهدفة {M}",, والرسالة المغطاة {C} معا. الرسالة {M} تمر عبر محولات T1 حيث يمكن ان تحتوى اى من الإحتمالات (رسالة مضغوطة, محولة او اى شفرة خاصة او عامة). التحويل T1 يمكن ان يجمع اى من التقنيات حسب التطبيق المفصل. ونفس الشيء يمكن أن يقال عن التحولات الأخرى T2T3. فى المستوى الاول تتضمن الرسالة محتوى الرسالة المخفية {I} or {D},. وخطيا LSB يطلب (M.LSB(0 D.LSB(0).. فى المستوى الثانى الهدف الوسيط (الشرك(D or I,) وهو خرج الستوى الاول صورة رمادية اللون مقاس Nr x Nc pixels مضمنة فى صورة RGB.

النمازج متعددة المستويات أكثر أمانا لإخفاء المعلومات من المستويات العادية. هذا يجب أن يرضى او يلبي رغبات معظم المتسللين hackers. والمستلمين الاساسين للرسالة لديهم المعرفة على حد سواء بما هو مخفى

لمحتوى الرسالة فضلا عن الاحـرف والمفاتيـح (وغيرهـا مـن المعلومـات) المطلوبـة لفك الشفرة او استرداد الرسالة.



الشكل(3.2) :نموذج إخفاء المعلومات متعدد المستويات

5. إخفاء البيانات من خلال إخفاء متعدد المستويات:SSEC

هذه الدراسـة مقترحـة مـن قبـل (Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal) [9]إستخدم الجمع بين ميزات كل من النص والصورة القائمة على تقنية إخفاء المعلومات عـن توصـيل المعلومـات بشـكل أكـثر أماناً بين موقعين. أدرجت فكرة المفتـاح السـري للمصـادقة عنـد كلا الطرفيـن مـن أجل تحقيق مستوى عال من الأمن. ونتيجة لزيادة تحسين مستوى الأمان، تم ترميـز المعلومات من خلال القيم SSCE وجزءا لا يتجزأ في نـص الغلاف الـوارد باسـتخدام طريقة إخفاء المعلومات النص المقترح لتشكيل النص المخفي. وقد استخدمت هذه التقنية الترميز عند كلا الطرفين من أجل تحقيق مستوى عال من الأمن , التـالي تـم تضمين النص المخفي مـن خلال طريقـة PMM فـي صـورة الغلاف لتشـكيل صـورة المخفية. في الجانب المستقبل وقد تم تنفيذ العملية العكسية إلياً ترجـع المعلومـات الأصلية.

5.خوارزميـة إخفاءالمعلومـات لإخفـاء رسالة سرية داخل صورة:

هـذه الدراسـة مقترحـة مـن قبـل (Rosziati Ibrahim and Teoh Suk Kuan)[10] إستخدام خوارزمية رموز الثنائيـة وبكسـل داخـل صـورة وتقـترح هـذة الورقـة خوارزميـة جديـدة لإخفـاء البيانـات الـداخل صـور بإسـتخدام تقنيـة إخفـاء المعلومات لتصميم خوارزمية لإخفـاء كـل البيانـات المدخلـة داخـل الصـورة لحمايـة خصوصية البيانات، بعد ذلك يتم تطويرها يقـوم هـذا النظـام علـى خوارزميـة جديـدة لإخفاء المعلومات، هذا النظام المقترح يوفر منصة صور للمسـتخدم لإدخـال الصـور ومربــع نــص لإدراج النصــوص، يمكــن للمســتخدم إرســال صــورة stego إلــى مستخدمكمبيوتراخر بحيث المستقبل قـادرا علـى إسـترجاع و قـراءة البيانـات الـتي كانت مخفية في الصورة بواسطة إستخدام النظام المقترح نفسه.

3.2.2 مقارنة الدراسات السابقة:

جدول**(1.2.2):** مـ قارنةالدراسات السابـ قة

إسم الورقة	النوع	السنة	level 1	level 2	النتيجة
زيادةســـــعة اخفـــــــــاء المعلومـــــات بطريقـــة ال(LSB) للنـــص والصورة	تشفير النص داخل الصورة		النص	الصور ة	كل ما كان النص صغير كان افضل لكي لا تتاثر الصورة من حيث المنظر الخارجي ولا يحصل لها تشويه حيث لا يتمكن المشاهد بالعين المجردة من معرفة هل الصورة تحتوي علي بيانات ام لا.
إخفاء البانات إخفاءالبيانـات بسـعه عاليـة مبنيـــة علـــي طريقة LSB	إخفاء صورة داخل صورة	2009			وهذة التقنية تسمح بإخفاء صورة داخل صورة أخرى لها نفس الحجم يتم تقليل حجم الرسالة السرية قبل الإخفاء لإخفاء كمية أكبر من البيانات.
تقنيـــة تعـــدد المســـتويات فـــي اخفـــاء المعلومات	تشفيرالص ورة	2003		الصور ة	الاخفاء متعدد المستويات لها فوائد محتملة،أنه يؤدي إلى تعزيز سرية المعلومات السرية باستخدام مستويين إخفاء

					المعلومات صورة في واحد من النظام وإضافة المزيد من التعقيد في عملية إخفاء المعلومات من خلال تطبيقه في مستويين .
إخفاء البيانات من خلال إخفاء متعدد المستويات SSE	تعددالمستويات	2008	نص	الصورة	يضيف هذا النموذج مستوى عال من الأمن من خلال تطبيق تقنية تعددالمستويات MLS))، الغطاء كائن لا يدعو للشك بوجود رسالة ما داخله، لأنها تبدو مشابهة إلى الكائن الأصلي سواء كان هذا الكائن صوره اوصوت او فيديو.
خوارزميةإخفاءالمعلومات لإخفاء رسالة سرية داخل صورة .	تشفيرنص	2011	نص	الصورة	يوفر منصة صور للمستخدم لإدخال الصور ومربع نص لإدراج النصوص، يمكن للمستخدم إرسال صورة stego إلى مستخدمكمبيوتراخر بحيث المستقبل قادرا على إسترجاع و قراءة البيانات التي كانت مخبأة في الصورة stego بواسطة إستخدام النظام المقترح نفسه

الباب الثالث

التقنيات المستخدمة

و تحليل النظام

المقترح

1.3 المقدمة:

يصف هذا الباب التقنيات المستخدمة في إخفاء البيانات وتحليل النظام بإستخدام لغة النمذجة الموحدة(UML) .

2.3 نبذه عن لغة C#:

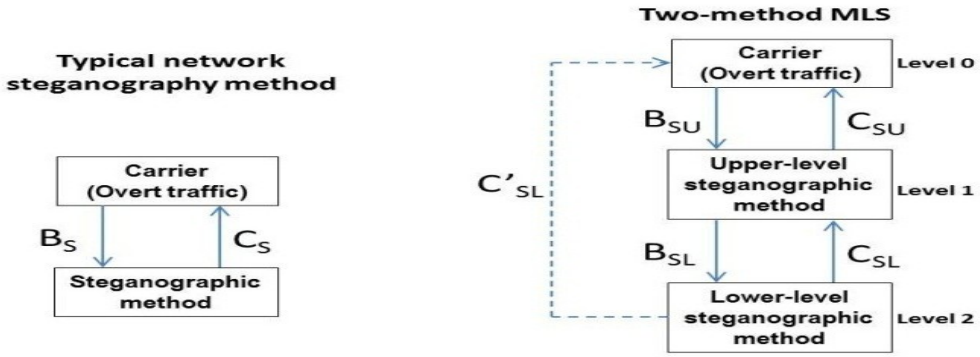
سي شارب (C#)أحد لغات بيئة الدوت نت لتطوير البرامج من أنتـاج شـركة ميكروسوفت يرمز اليها بالرمز c# وتنطق "سي شارب".

تتميز سي شارب بأنهـا أحـد لغـات البرمجـة الشـيئيه وتجمـع صـفات السـي واللبيزك المرئي حيث انها تستخدم القواعد الخاصـه بالسـي وسـرعة التطـوير. و يميز هذه اللغة أنها من أسرعةوأكفأ لغات البرمجة الموجودة في العـالم ولاتحتـاج إلى قاعـدة تسـتند عليهـا ويمكنهاالتواصـل مـع الحاسـب بصـورة مباشـرة ولـذلك تستخدم في إنشاء وبرمجة أنظمة التشغيلالمختلفة والتطبيقات الضخمة. توجد بها العديدمن المميزات الاخري.[11]

لمـاذا اخترنـا ال c# لانهـا سـهلة التعلـم تعمـل علـي بيئـات متعـددة تتـدعم عمـل الخوارزميات و securityمثال تستخدم في تصميم برامج الانتي فايرس.

3.3 تقنية إخفاء متعدد الطبقات:

تقنيـــة (MLS) تعمـــل علـــى مســـتويين علـــى الأقـــل مـــن أســـاليب (Steganography)، أولا يسـتخدم إسـلوب المسـتوى العلـوي المـرور العلنـي بإعتبارها ناقل البيانات السريةالثانية وطريقة المسـتوى الأدنـى، يسـتخدم طريقـة عمل طريقة المستوى العلوي بإعتبارها الناقل [12] .



الشكل (1.3): نوع الوسائط المستخدمة في إخفاء البيانات

4.3 MatLab:

هو أداة وبيئة تطوير برمجية مخصصة للمهامالحسابية، حيث تتوفر فيه الكثير مـن الوظـائف والـدوال الرياضـية المبنيـة داخليـا والتيتسـهل حـل مختلـف أنـواع المعادلات الرياضية. كما تساعد لغة برمجة ماتلاب على كتابةدوال وبرامج خاصة.[13]

5.3 مقياس قمة نسبة الاشارة الى الضوضاء :(PSNR)

طبقت عمليـة الاخفـاء علـى عـدة صـور ولغـرض قيـاس كفـاءة الاخفـاء تـم استخدام مقياس قمة نسبة الاشارة الـى الضوضـاء (PSNR) والـتي تقيـس مـدى دقة الاخفاء وعـدم تمييـز النـص المخفـي فـي الصـورة بـالعين البشـرية. بالنسـبة لاخفاء الصور فمقياس الدقة يتضمن حسـاب مربـع الخطـأ والمعـرف بالمعـادلتين التاليتين : [3]

(PSNR = 10*log10(256*256/MSE

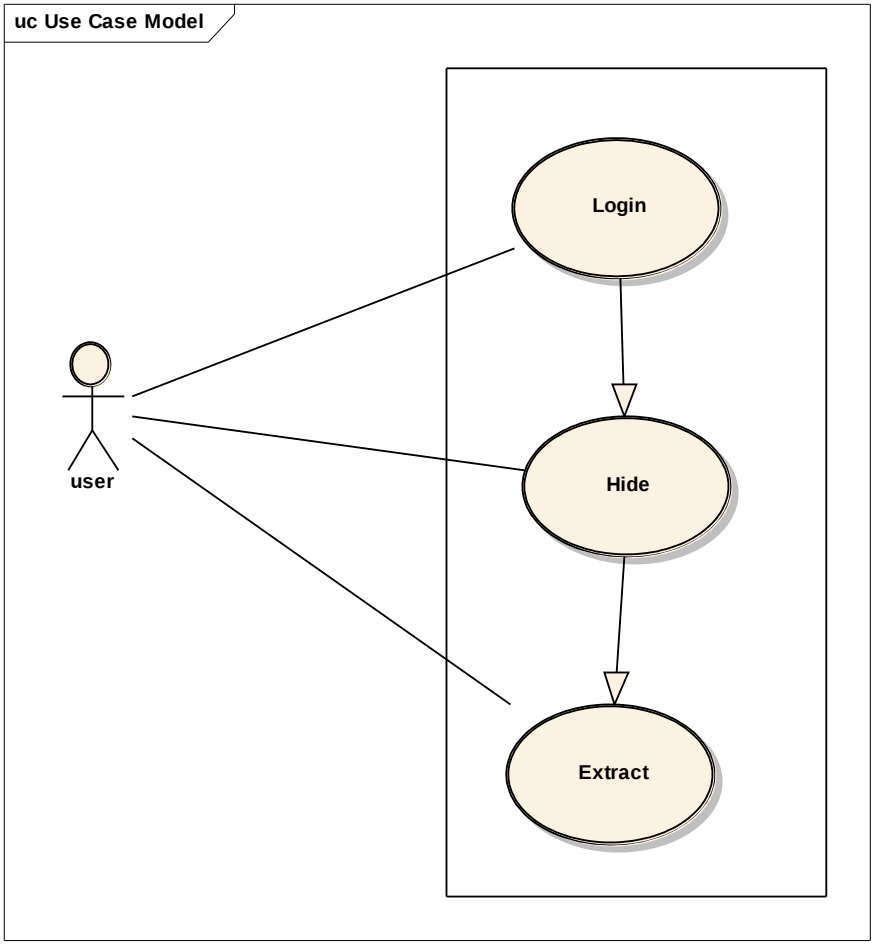
(MSE = sum(sum(error .* error)) / (M * N

M,N:تمثل أبعاد صورة الغطاء.

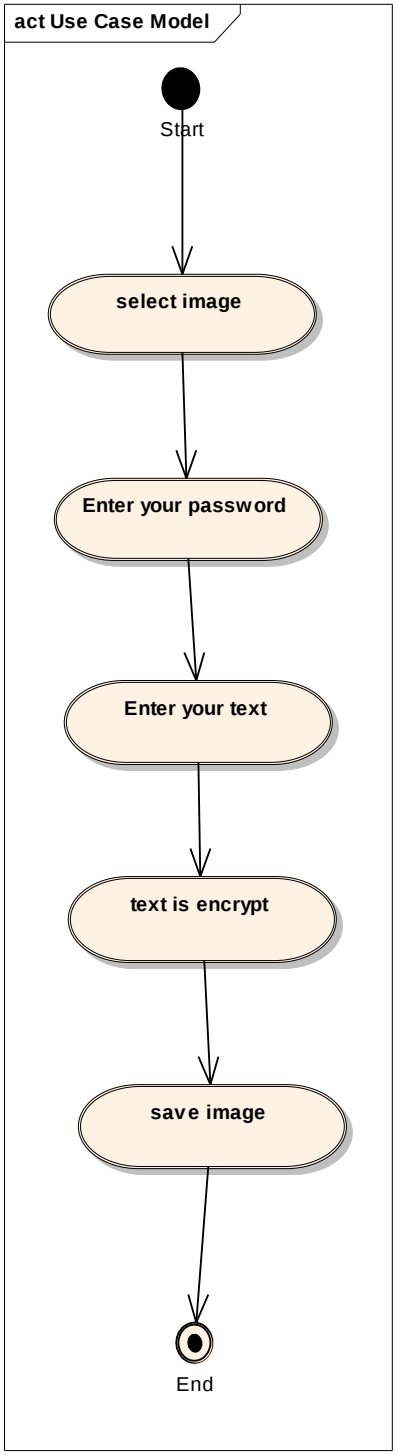
6.3لغة النمذجة الموحدة(UML):

هي لغة نمذجة رسـوميه تقـدم لنـا صـيغة لوصـف العناصـر الرئيسـية للنظـم البرمجية. تستخدم هذه اللغة لعمل رسوم تخطيطيـة لوصـف برامـج الكمـبيوتر مـن حيث العناصر المكونة أو خط سـير العمليـات الـذي يقـوم بـه البرنامـج , يلاحـظ أن UML يوجد فيه العديد من المخططات المختلفة (نمـاذج) والسـبب فـي هـذا التنـوع يعود إلي أن تطوير البرمجيات يشترك فيه عدد مـن الأفـراد ومـن مزاياهـا أنهـا لغـة رسومية للتعبير عن التطور البرمجي للبرنامج وتقدم لنا رموز تنتج بها هذه البرامـج وتلقي رعاية واسـعة فـي الوسـط الصـناعي تقـدم أفضـل الممارسـات فـي مجـال هندسـة البرمجيـات ويسـهل بواسـطتها علـي المحللين والمصـممين والمـبرمجين والعملاء , التخاطب فيمان بينهم وتمرير المعلومات في صيغة نمطيـة موحـدة تـزود بمجموعة من الترميز والمفـاهيم الـتي تلـبي احتياجـات نمذجـة المشـاريع البرمجيـة بصورة مثالية.[14]

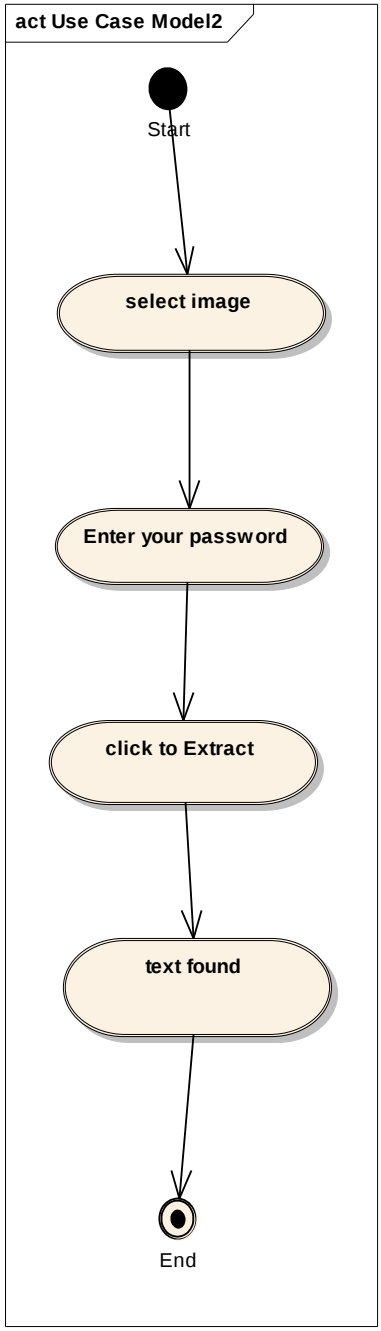
7.3أنواع مخططات لغة النمذجة الموحدة:



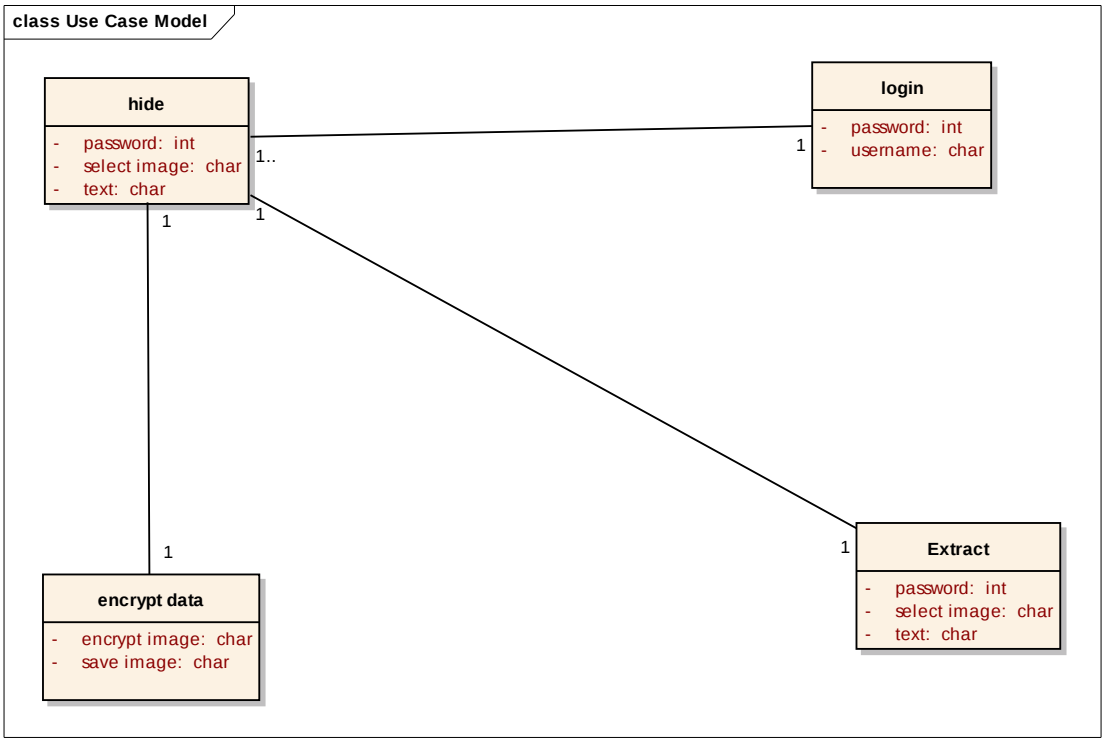
الشكل(2.3): يوضح (Use Case)



الشكل(3.3): يوضح (Activity Diagram) لإخفاء البيانات



الشكل(4.3): يوضح (**Activity Diagram**)لإسترجاع البيانات



الشكل (5.3): يوضح (**Class Diagram**) للنظام

الباب الرابع

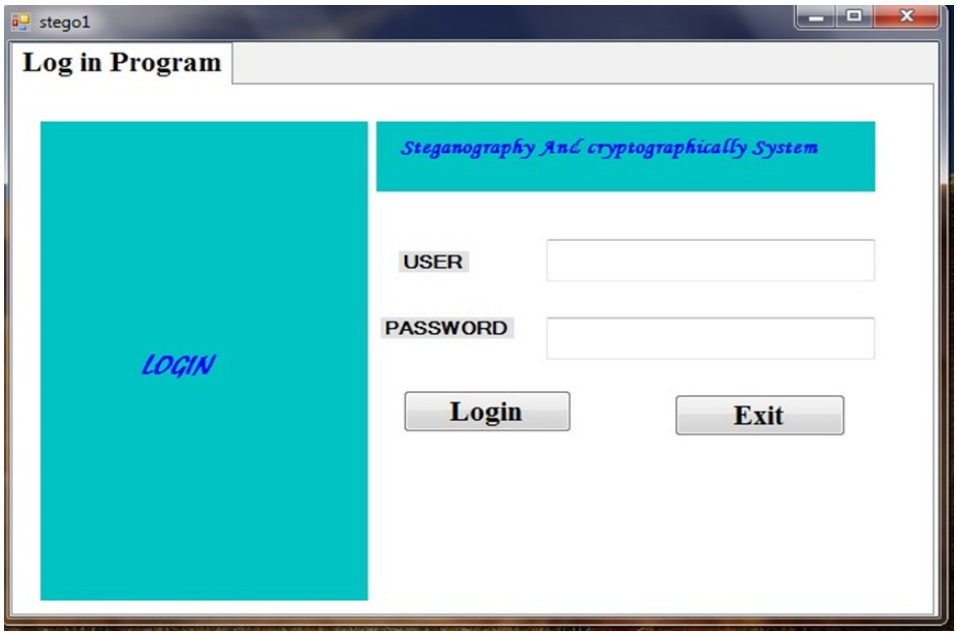
تصميم الذظام

1.4 مقدمة:

بناء علي ما تم التوصل اليه في الابواب السابقة ففي هذا الباب سيتم عرض الشاشات والخطوات المتبعه لتنفيذ البرنامج وهي كما يلي:

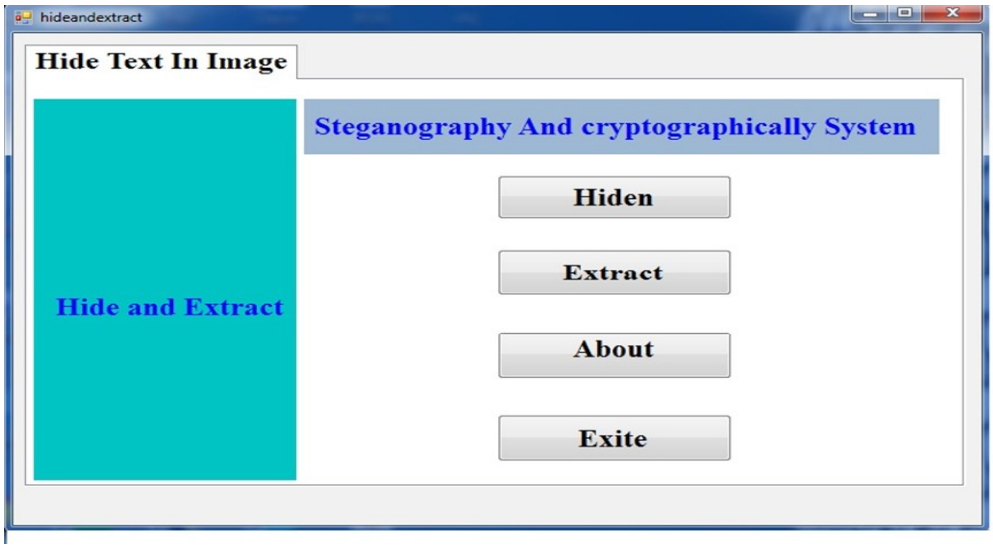
2.4 الشاشة الرئيسية:

يطلب النظام من المستخدم أن يقوم بإدخال الأسم و كلمة السر كمـا فـي الشـكل التالي :



الشكل (1.4) يوضح شاشة تسجيل الدخول للنظام

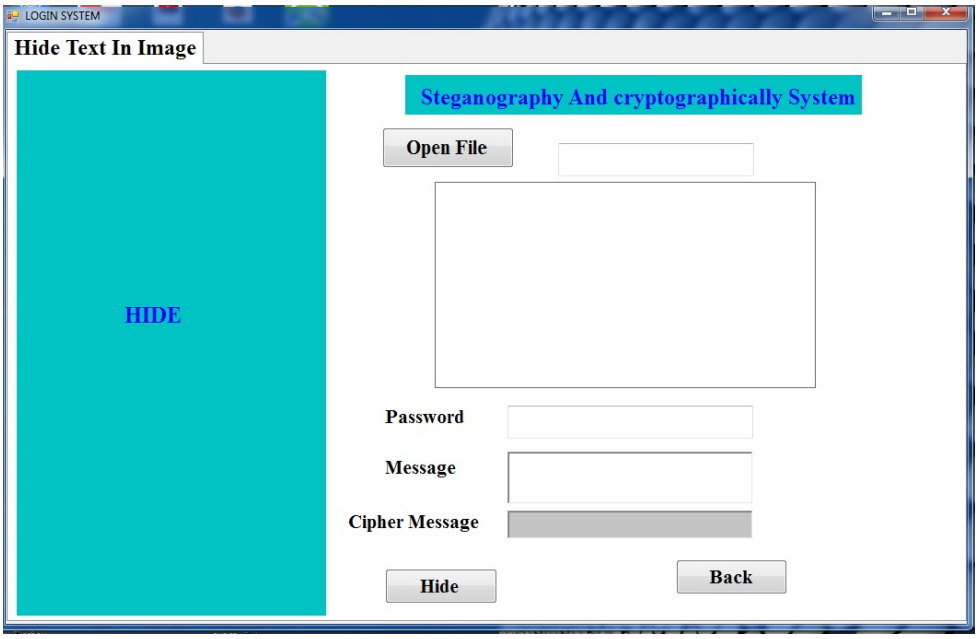
عندما يتم الضغط علي زر الدخول يتم عرض الشاشه الإخفاء والإسترجاع التالية:



الشكل (2.4): يوضح شاشة الإخفاء والإسترجاع للبيانات

3.4 عملية الإخفاء:

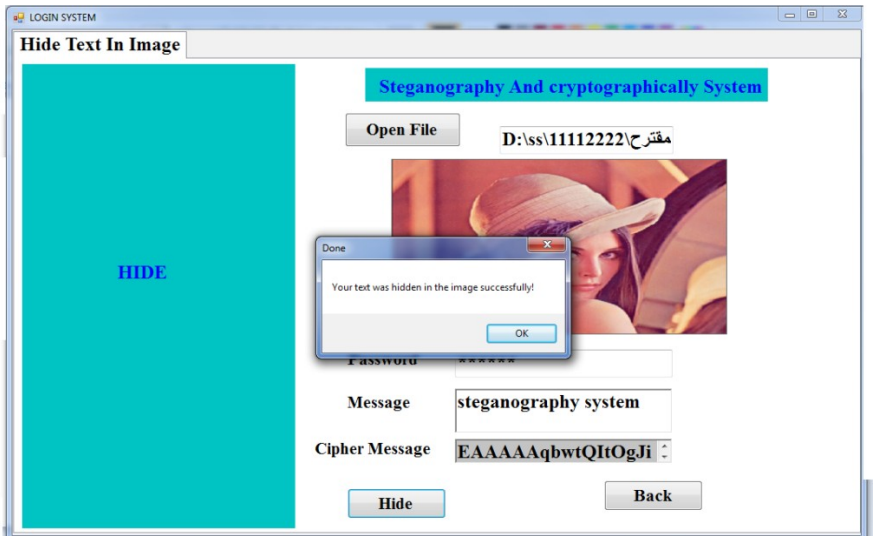
عندما يتم الضغط علي زر الإخفاء يتم عرض شاشة الإخفاء:



الشكل (3.4) يوضح شاشة الإخفاء للبيانات

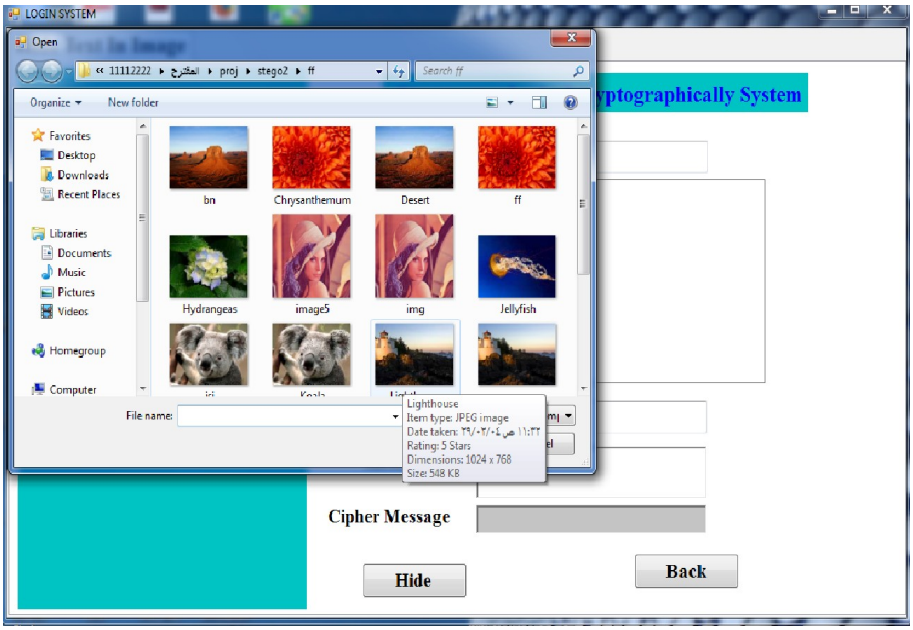
حيث يقوم المستخدم بإختيار الصورة المراد إخفاء النص في داخلها , بالضغط علي زر

open file كما موضح في الشاشه التالية:



الشكل (4.4) يوضح شاشة عملية الإخفاء

عند الضغط علي الرسالة التي تظهر في الشاشة يذهب النظام الي الملف الذي تريد أنتحفظ فيه الصورة كما موضح أدناه:

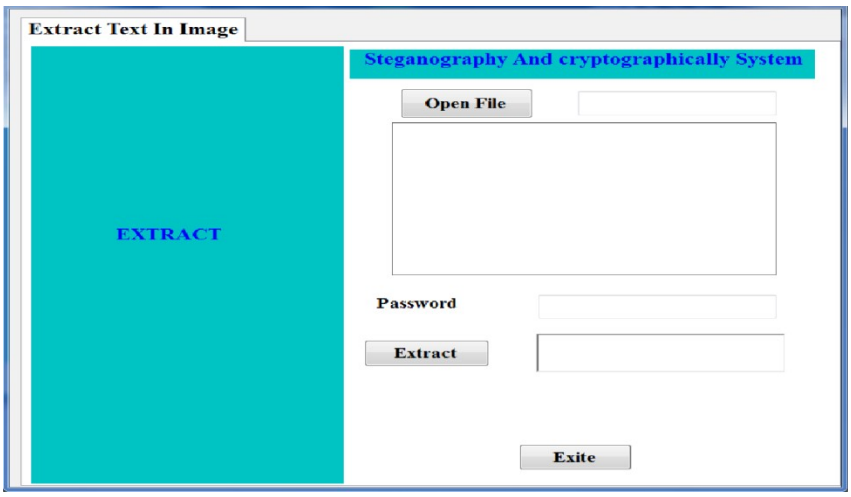


الشكل (5.4) يوضح شاشة حفظ الصورة المغطاة

عند الضغط علي زر الحفظ تكون قد تمت عملية الاخفاء.

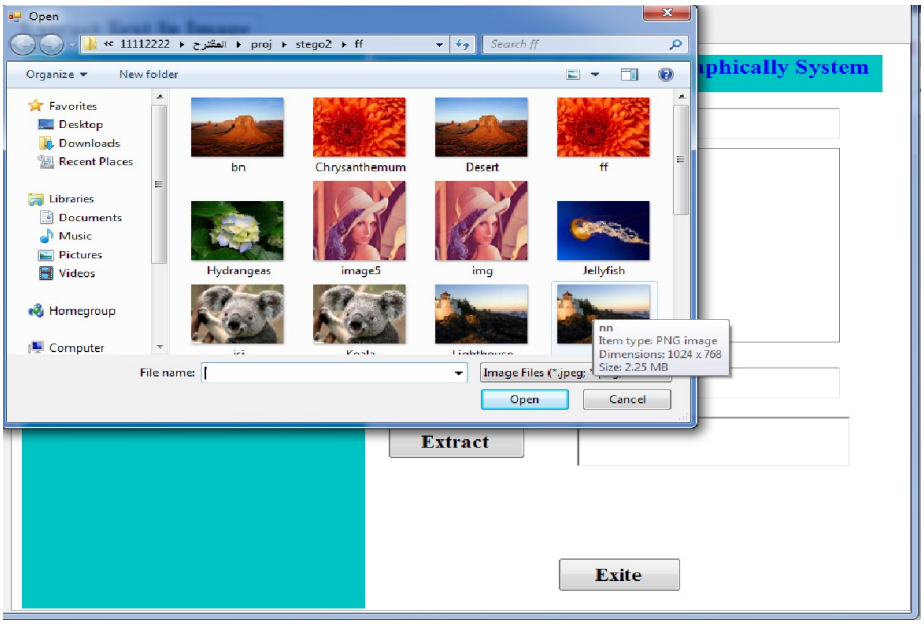
4.4 عملية إستخراج النص:

عند الضغط علي زر الاستخراج من شاشة الإخفاء والإسـترجاع تظهـر لنـا الشاشـة التالية:



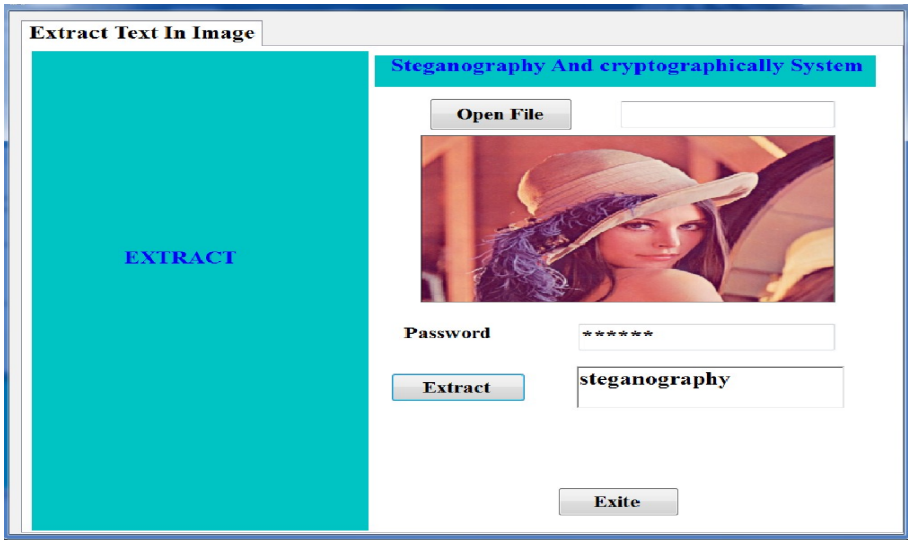
الشكل (6.4): يوضح شاشة الإسترجاع

حيث يقوم المستخدم باختيار الصورة المغطاة عند الضغط علي زر open file وتظهر الشاشة التالية:



الشكل (7.4): يوضح شاشة إختيار الصورة المغطاة

وبعد ذلك يطلب النظام من المستخدم أن يدخل كلمة السر وبالضغط علي زر الإستخراج كما في الشكل ادناه:



الشكل (8.4): يوضح شاشة الإسترجاع النص الأصلي

وبذلك يكون قد تم إستعادة النص الأصلي.

الباب الخامس

النتائج والتوصيات

1.5النتائج:

تـم إسـتخدام علـم إخفـاء المعلومـات فـي الصـورة باسـتخدام تقنيـة إخفـاء المعلومات متعددة المستويات وذلك عن طريق إسـتخدام عمليـة التشـفير الرسـالة المرسلة في المستوي الأول و إخفاء الرسالة المشـفرة فـي المسـتوي التـاني وتـم قياس مدى التشويش بإستخدام PSNRو MSEعلي صورتين، الصورة الاولي ذات حجم (512X512) وعدد أحرف الرسالة كانت (177 و 885 حرف) والصورة الثانية ذات حجم (375X500) وعدد أحرف الرسالة كانت (216 و 1420حرف) وكانت النتائج كالأتي:

جدول **(1.5) :** م قياس **PSNR**و **MSE**علىعدةصوربا حجام مختلفة وطول نص مختلف

PSNR	MSE	Text Length	Image Size	Image Name
72.6421	0.0033	885	512X512	Image 1
72.0039	0.0039	1062	512X512	Image 1
76.9678	0.0012	216	375X500	Image 2
66.9450	0.0130	1420	375X500	Image 2

نستنتج من خلال نتائج PSNR و MSE على عدة صور باحجام مختلفة وطول نص مختلف انة كلما زاد طول النص تزداد قيمة MSE وتـ قل قيمة PSNR وبنسبة قليلة جدا مما يدل على كفاءة الخوارزمية في الاخفاء بالرغم من طول النص المخفي. ولايمكن تمييز وجود نص داخل الصورة.

الشكل (5.1): الصورة قبل الإخفاء علي اليمين وبعدالإخفاء علي اليسار

2.5 التوصيات:

علم اخفاء المعلومات علم واسع التطبيقات والإمكانيات، ونوصي هنا بعض المقترحات لمن يريد السير في هذا المجال :

1. إستعمال اكثر من مستويين في إخفاء البيانات.
2. زيادة كمية البيانات التي يمكن إخفاؤها عن طريق ضغط البيانات قبل التشفير.
3. اختيار خانة اخرى غير الإ قل أهمية.
4. إستعمال اكثر من خوارزمية في التشفير علي حسب حساسيىة البيانات المراد إرسالها.
5. حساب حجم البيانات المراد إخفاؤها في الصورة.

المراجع

المراجع :

[1] الحمامي، علاء حسين، "أخفاء المعلومات الكتابة المخفية والعلامة المائية"، إثراء للنشر والتوزيع، الشارقة، (2008).

[2] رهام جاسم عيسى، إنعام محمد سليمان، "استخدام الخوارزمية الجينية في تشفير بيانات صورية رمادية وإخفاءها في صورة"، كلية علوم الحاسوب والرياضيات، جامعة الموصل ، العراق، (2013).

[3] شهد عبدالرحمن حسو ايلاف اسامة عبد المجيد" تطبيق نظام التغطية على الصور الملونة من نوع (BMP)" ، كلية علوم الحاسوب والرياضيات، جامعة الموصل ، العراق، (2008).

[4] شيماء شكيب، همسة معن،" طريقة خوارزمية جينية مثلى للإخفاء"، كلية علوم الحاسوب والرياضيات، جامعة الموصل ، العراق، (2011).

[5] Steganography Uses and Effects on Society, by Karen Korhorn

.http://cpsr.org/prevsite/essays/2002/2rr3.html

[6] Kekre, H. B., Archana Athawale, and Pallavi N. Halarnkar. "Increased Capacity of Information Hiding in LSBs Method for Text and Image." *International Journal of Electrical, Computer and Systems Engineering* 2.4 (2008): 246-249.

[7] Koppola, Rajanikanth Reddy. *A High Capacity Data-Hiding Scheme in LSB-Based Image Steganography*. Diss. University of Akron, 2009.

[8] Al-Najjar, Atef Jawad. "The decoy: multi-level digital multimedia steganography model." *WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering*. No. 12. World Scientific and Engineering Academy and Society, (2008).

[9] Bhattacharyya, Souvik. "Data hiding through multi level steganography and SSCE." *Journal of Global Research in Computer Science* 2.2 (2011).

[10] Ibrahim, Rosziati, and Teoh Suk Kuan. "Steganography algorithm to hide secret message inside an image." *arXiv preprint arXiv:1112.2809* (2011).

[11] *"Retrieved on (May 10, 2016) (www.kutub.info).*

Sayed, ”Multi Level Network Steganography” Sudan **[12]**
.(University June (2014

.(http://www.boosla.com" Retrieved on on(Aug 20, 2016 " **[13]**