Encrypt Text Data Using the Linear Feedback Shift Registers Algorithm and Hide Inside an Image

Aseel Mazin
College of Computer and Math
Department of Software Engineering
University of Mosul
Aseel20@gmail.com

Raya Jasim Eessa
College of Computer and Math
Department of Software Engineering
University of Mosul
r.essa1980@hahoo.com

Asmaa Salim Yahya
College of Computer and Math
Department of Software Engineering
University of Mosul
Asmma.s.y@gmail.com

Abseract

For the importance to achieving large communications security led to the need to hide information, and because the information does not appear either encrypted or unencrypted visible to others, it is considered a contributing factor to give protection and secure information. This, which attend to use different methods for this purpose as secured and hide information in different media. For a data hiding technique to be successful it needs to have confidentiality, integrity and availability

Steganography allows for the concealment of files and messages within other files, such as pictures, audio and video. This allows for the easy transportation of sensitive data without prying eyes being able to tell a message is being transported. Image steganography has gotten more popular press in recent years than other kinds of steganography, possibly because of the flood of electronic image information available.

This work has been built a security system to hide information in image file. The main algorithm concealment was used to hide in the least important (LSB) Least Significant Bit, transform the image of formula (RGB) to YCbCr image, and put the contents of the message in a one layer of image layers. For more security, the text message was encrypted using a cryptographic algorithm liner stream cipher, and then are included within the image files of BMP and JPEG format.

Keyword: Encrypt Text Data, Linear Feedback Shift, Image

تشفير بيانات نصية باستخدام مسجلات الإزاحة ذات التغذية العكسية وإخفاءها داخل صورة

اسماء سالم يحيى
كلية علوم الحاسوب والرياضيات
قسم هندسة البرمجيات
جامعة الموصل
Asmma.s.y@gmail.com

ريا جاسم عيسى
كلية علوم الحاسوب والرياضيات
قسم هندسة البرمجيات
جامعة الموصل
r.essa1980@hahoo.com

اسيل مازن
كلية علوم الحاسوب والرياضيات
قسم هندسة البرمجيات
جامعة الموصل
Aseel20@gmail.com

تاريخ الاستلام 2012/11/11
تاريخ القبول 2013/03/06

الملخص

نظرا للحاجة الملحة للحفاظ على أمنية الإتصالات دعا للحاجة الى اخفاء البيانات ولأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان فهذا يعتبر عاملاً مساعداً على إضفاء حمايةً وأمناً على المعلومات. فهذا مما دعا ايضا الى إستخدام طرق مختلفة لهذا الغرض كالتشفير وإخفاء المعلومات في وسائط مختلفة. ومن اجل الحصول على تقنية ناجحة لاخفاء البيانات نحتاج لعدة عوامل ومنها الوثوقية والتكامل.

إخفاء المعلومات يسمح لإخفاء الملفات والرسائل داخل ملفات أخرى، مثل الصور والصوت والفيديو. وهذا يسمح لسهولة نقل البيانات الحساسة بعيدا عن أعين المتطفلين. وهنا نذكر ان إخفاء المعلومات داخل الصور هو الاكثر انتشارا في السنوات الأخيرة من أنواع أخرى من وسائط إخفاء المعلومات، وربما يعود ذلك لسهولة التعامل مع تركيب الصورة.

تم في هذا العمل بناء نظام أمني لإخفاء المعلومات في ملفات صورية. وتتلخص خوارزمية الإخفاء في الملفات الصورية باستخدام طريقة البت الاقل اهميهLeast (LSB) Significant Bit حيث تم تحويل صورة من صيغة (RGB) الى صورة YCbCr ووضعت محتويات الرساله في طبقه واحده من طبقات الصورة. وللحصول على امنيه عاليه تم تشفير الرسالة النصيه بإستخدام خوارزمية التشفير الأنسيابي الخطي Linear Stream Cipher ومن ثم تم تضمينها داخل الملفات الصورية والتي من نوع BMP و JPEG.

الكلمات المفتاحية: Encrypt Text Data, Linear Feedback Shift, Image

1- تمهيد

أصبحت عملية تناقل البيانات عبر الإنترنيت عملية سهلة نتيجة التطور الكبير في تقنيات الشبكات، وبات بإمكان الكثيرين الاتصال مع بعضهم البعض بسهولة وسرعة عبرها, إلا أن استخدام الإنترنيت للاتصال ترافقه مشكلة توفير الأمنية [1].

ومن هنا ظهرت الحاجة إلى توفير الوسائل لأمنية البيانات، ومن هذه الوسائل علم التشفير (Cryptography) الذي يعنى بتوفير حماية لخزن البيانات ونقلها عن طريق استخدام مفتاح سري، لذلك كان التشفير وما يزال الطريقة الناجحة لحماية البيانات المخزونة والمرسلة عبر الشبكة، ولكن مع ازدياد شبكات التناقل وشبكة المعلومات العالمية, أصبح من الصعب المحافظة على هذه البيانات، ولاسيما أنها تكون دائما في متناول الجميع عبر شبكة الانترنت في صيغة غير واضحة تبعث على الشك والاهتمام لدى المتطفل والسارق لفتح هذا التشفير أو تدمير المعلومات المرسلة.

ولقد فرضت العديد من القيود لمحاولة منع استخدام التشفير عبر الشبكة، ومن هذه القيود منع انسيابية أية معلومة لمصدر يستخدم التشفير في مراسلاته كما جاء في التشريع الصادر عن دائرة العدل الأمريكية الذي يعني المقاطعة المعلوماتية، لذلك بدأت معظم الحكومات بفرض سيطرتها على التشفير ومنع المؤسسات من التعامل به إلا

من خلال استخدام خوارزميات معروفة. لذلك كان لابد من تطوير أمنية البيانات وإنشاء تقنيات ووسائل جديدة ، ومن هنا ظهر علم إخفاء المعلومات [2].

2- الدراسات السابقة

تقنية البت الاقل اهمية LSB تعد من اوائل التقنيات المستخدمة لاخفاء البيانات , حيث تناولها عدة باحثين لسهولة استخدامها وكذلك تحقيقها للغير مرئية للبيانات المخفية واسباغ هيئة معقولة ومُقنعة على الملف الغطاء الحامل للمعلومات المراد اخفائها.

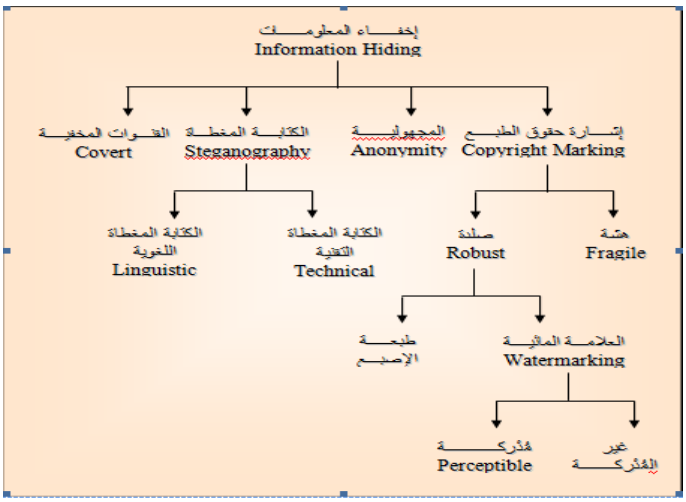
ففي عام 1992 قدم الباحثان Katzenbeisse و Petitolas بحثا لاخفاء صورة داخل صورة بإستخدام تقنية LSB [3]. وفي العام 2001 تناول الباحثان Chandramouli و Memon تقنية طمر البيانات بإخفاء بت واحد لكل نقطة ضوئية bpp (bit per pixel) في الصورة الرمادية واستخدام 3 بت لكل نقطة ضوئية للصورة الملونة RGB [4] . في عام 2002 قدم الصميدعي بحثا لتطبيق نظام تغطية تضمن استخدام تقنيات الإخفاء في الخلية الثنائية الاقل اهمية LSB لاخفاء بيانات سرية في ملفات الوسائط المتعددة (نص, صورة، صوت) [5].

بحث اخر في العام 2005 مقدم من قبل Xiangyang و Fenlin تم فيه اخفاء بإخفاء البيانات في صورة وذلك ببعثرة المعلومات المطلوب اخفائها بشكل عشوائي بإستخدام chaotic system ومن ثم كبس الملف الحامل المعلومات المطلوب اخفائها[6] .

ايضا وبنفس المعطى تناول الباحثون Fabien A. P. Petitcolas, و Morkel.T, J.H.P. هذه الطريقة لشيوعها في تقنية اخفاءالمعلومات [7] [8]. وفي العام2010 تناول الباحث Weiqi Luo طريقة جديدة لاخفاء البيانات في الملف الغطاء [9].

3 - إخفاء المعلومات Information Hiding

يعرف علم اخفاء المعلومات على انه عملية تضمين بيانات سرية في اشكال مختلفة من الوسائط المتعددة كملفات النصوص والصور والملفات الصوتية والفديوية. ومع النمو السريع لتقنيات الشبكات والاتصالات, فإن تقنيات إخفاء المعلومات أصبحت تستخدم بصورة واسعة لتحقيق أغراض متعددة منها حماية حقوق الطبع وتثبيت الملكية وتحقيق الاتصال بصورة سرية [10]. وتُصنَّف تقنيات إخفاء المعلومات إلى تقنيات فرعية طبقا للورشة الدولية الأولى في إخفاء المعلومات وكما مبيّن في الشكل (1).



الشكل (1) تصنيف تقنيات إخفاء المعلومات [1]

3-1 الكتابة المغطاة Steganography

يمكن تعريف الكتابة المغطاة (Steganography) على انها فن وعلم اخفاء المعلومات باستخدام حامل لها (Host) بهدف منع اي متطفل من الشكك بوجود رسالة مخفية داخل الملف الحامل، بطريقة لا تسمح لاي عدو او مراقب بان يكتشف ان هنالك بيانات سرية أخرى، اما كلمة (Steganography) فيرجع اصلها الى اللغة اليونانية ويتكون من المقطعين (Steganos) وتعني المغطاة و (Graphy), اي الكتابة او الرسم والمعنى الحرفي لها الكتابة المغطاة[11][1]. اي انها طريقة لإرسال بيانات سرية من خلال تضمينها في وسائط تعد غطاءً أو حاملاً لها بصورة يتعذر بها تمييز وجود تلك البيانات. وقد تكون الأغطية ملفات نصية أو صورية أو صوتية أو فيديوية، ويمكن أن تكون البيانات السرية نصاً صريحاً (Plain Text) أو نصاً مشفراً (Ciphered Text) أو أية معلومات يمكن تمثيلها على شكل سلسلة من الخلايا الثنائية (Bits). والهدف من الكتابة المغطاة هو نفي الشك بوجود تناقل بيانات سرية, وقد يفشل الحفاظ على أمنية البيانات إن حصل شك بوجودها. وقد صُنفت الكتابة المغطاة إلى صنفين الاول الكتابة المغطاة اللغوية Steganography Linguistic والكتابة المغطاة التقنية Technical Steganography [12] [13].

3-1-1 متطلبات الكتابة المغطاة Steganography Requirements

عند تصميم خوارزميات الكتابة المغطاة يجب مراعاة ثلاث متطلبات [14]. السعة تشير إلى كمية البيانات التي يمكن تضمينها ضمن غطاء معين.

عدم القدرة على الاكتشاف (Undetectability) تشير إلى عدم قدرة الشخص غير المخول على كشف وجود البيانات المضمنة, إذ أنها تكون غير قابلة للكشف إذا كان عنصر الكتابة المغطاة (Stego-Object) متسق إلى حد كبير مع الغطاء.

الصلادة (Robustness) تشير إلى مدى مقاومة عنصر الكتابة المغطاة لهجمات الشخص غير المخول المختلفة قبل تحطيم البيانات المضمنة.

3-1-2 فوائد نظام التغطية ومساوئه

إن الفائدة المرجوة من نظام التغطية هي:

- إمكانية استخدامه للنقل السري للرسائل من دون اكتشافها .
- إن استخدامه يعزز سرية الاتصالات الشخصية ويعد وسيلة مهمة للاتصال خصوصا عبر الانترنيت.

أما المساوئ فهي:

- تحتاج إلى غطاء كبير الحجم لإخفاء عدد قليل من البيانات.
- إن اكتشاف الرسالة المخفية يُعد من عيوب نظام التغطية لأنه بذلك سوف تنتفي الحاجة إلى نظام التغطية وقد يتم اعتراض رسالة سرية ذات أهمية كبيرة، ومن الجدير بالذكر انه تُوجد بعض التطبيقات على شبكة الانترنيت مثل الجدار الناري (Firewalls Internet) التي يمكن من خلالها اكتشاف الرسالة المخفية .
- لايمكن الجمع بين تعظيم قوة الإخفاء مع تعظيم كمية البيانات المخفية قياسا ببيانات الغطاء [15].

3-2 إشارة حقوق الطبع (Copyright Marking)

مجموعة من التقنيات التي ابتكرت لتحديد حقوق الملكية الفكرية للمعلومات وتُصَنف إلى [16] [17]:

- العلامة المائية الهشة (Fragile): والتي يؤدي أي تغيير في الوسط الحامل لها إلى خسارتها.
- صلدة (Robust): والتي تكون مقاومة للهجمات. وصُنفت إلى نوعين:
- طبعة الإصبع(Fingerprinting):
- العلامة المائية القوية (Robust Marking وتصنف الى صنفين:هما العلامة المائية غير المرئية (Invisible Watermarking)والعلامة المائية المرئية (Watermarking Visible) [18] [2].

3-3 وسائط اخفاء المعلومات

يوجد عدة وسائط يتم بواسطتها اخفاء البيانات المتطلب حمايتها ومنها:

3-3-1 إخفاء البيانات داخل النص (Hiding Data in Text) عملية الإخفاء داخل النص

تعد مهمة صعبة نوعا ما ذلك أن النص يحوي على بيانات متكررة قليلة لاستبدالها بالرسالة السرية، ولهذا فأن كمية قليلة من البيانات يمكن إخفاؤها داخل النص لذلك فأن هذه التقنيات تعد(Low data rate)، من المساوئ الأخرى لعملية الإخفاء داخل النص هو إمكانية تحطيم الإخفاء بسهولة عن طريق تغيير النص من صيغة إلى أخرى (مثلا

منTXT. إلى PDF.) من الجدير بالذكر أن كل التقنيات التي تستخدم النص تحتاج إلى معرفة النص الأصلي لغرض استخراج الرسالة السرية [19] [20] .

2-3-3 إخفاء البيانات داخل الصورة (Hiding Data in Image)

تعد الصور الرقمية من أكثر الوسائط المتعددة استخداما في الكتابة المغطاة بوصفها حاملاً للبيانات السرية وذلك بسبب انتشارها الواسع على الإنترنت [10]. لغرض فهم كيفية إتمام عملية الإخفاء داخل الصورة يجب فهم كيفية تمثيل الصورة داخل الحاسبة أولا، الصورة عبارة عن مصفوفة من القيم التي تمثل شدة الإضاءة في تلك النقطة ويتم تمثيل كل نقطة إما ببايت واحد (8bit) أو بثلاث بايتات (24 bit) هذه القيم تمثل مدخلاً إلى جدول ألالوان(Palette) الموجود في بادئة الملف (Header)، إن عدد المستويات اللونية المختلفة التي يمكن تمثيلها في ثمانِ خلايا ثنائية هي 256 مستوى لونيا أي أن جدول تواجدات الألوان يحوي 256 لوناً.

- هناك نوعان من الصور ذات التمثيل الثماني:

1- الصور الملونة يتم تمثيل 256 لوناً فقط من الألوان المتوفرة في جدول تواجدات الألوان الذي يحوي (256*256*256) لوناً، إذ يتم اختزال جميع مستويات الصورة اللونية إلى 256 لوناً بالاعتماد على الألوان الموجودة في الصورة أي يكون لكل صورة جدول ألوان مختلف عن الأخر.
2- الصور ذات التدرجات الرمادية, تم تجاوز مشكلة عدد المداخل اللونية وبقيت الحاجة إلى 256 لوناً فقط والتي تمثل التدرجات الرمادية [21].

هناك عدة عوامل يجب أن تؤخذ بنظر الاعتبار عند اختيار نوع الصورة المراد استخدامها كحاملة للبيانات.

استخدام الصور الملونة الممثلة بثلاث بايتات لكل نقطة توفر مرونة كبيرة عند استخدامها في الإخفاء، لان العدد الكبير من الألوان (اكثر من 16 مليون لون) التي تمتد ما وراء نظام الرؤية البشري((Human Visual System (HVS تجعل من الصعوبة اكتشافها، الفائدة الأخرى هي كمية البيانات الكبيرة التي يمكن إخفاؤها داخل هذه الصور بعكس الصور الممثلة ببايت واحد، ولكن من المساوئ في هذا النوع حجمها الكبير نسبيا الذي يجعلها اكثر عرضة للشكوك من النوع الآخر، لذلك قد نلجا إلى كبس الصورة لتقليل حجمها .[16]

اذا ان البيانات التي تخزن على الحاسبة بأي نوع من أنواع الملفات غالبا ما تكون هذه الملفات كبيرة الحجم داخل الحاسبة على الرغم من أن المعلومات المطلوبة تكاد تكون قليلة لكنها تشغل حيزا كبيرا من الذاكرة وتحتاج إلى زمن كبير في حالة نقلها على شكل حزم لذا أصبحت الحاجة إلى كبس البيانات (الذي هو تحويل البيانات إلى حجم اقل) لتكوين ملفات ذات كفاءة أعلى في الخزن وكذلك في حالة نقل البيانات عبر الأوساط المتعددة (Multimedia) وان التقدم الحاصل في مجال تقنية نقل المعلومات لم يكن عمليا ان لم يضع البيانات على شبكة النقل بدون كبس[22] [23] ..

وهناك نوعين من تقنيات الكبس:

1. الكبس بدون فقدان (بدون خسارة) (Lossless Compression): يحافظ على الصورة الأصلية سليمة تماما ويفضل استخدامها عندما يراد الحفاظ على المعلومات سليمة لذلك تكون مفضلة عند الإخفاء، هذا النوع لا يوفر نسبة كبس عالية مثل الطريقة ومثال على هذا النوع BMP,GIF أي أن هذا النوع لا يسمح بأي اختلاف بين الصورة الأصلية والصوره المركبة بعد أعادتها من الكبس أي أن بيانات الصورة يتم أعادتها بدون فقدان. [22] [23].
2. الكبس بفقدان (بخسارة) Loosely Compression مثل JPEG توفر نسبة كبس عالية لكنها لا تحافظ على سلامة الصورة الأصلية وهذا يؤثر سلبيا على أي بيانات مخفية في الصورة، وذلك نسبة إلى خسارة البيانات غير الضرورية لتوفير مساحة من دون التأثير على كفاءة الصورة ولكن الصورة الناتجة لاتعد نسخة طبق الأصل من الصورة الأصلية، هذا النوع يستخدم بكثرة مع الصور الملونة الممثلة بثلاثة بايتات، إذ توفر نسبة كبس عالية [22] [23]

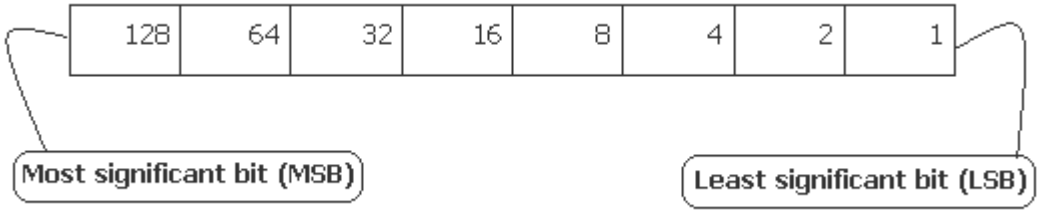
أما أهم التقنيات المستخدمة لطمر البيانات داخل الصورة هي:

1-2-3-3 أهم التقنيات المستخدمة لإخفاء البيانات داخل الصور:-

1- الإخفاء في الخلية الثنائية الأقل أهمية (Least Significant Bit Insertion) تعتبر ابسط الطرق لطمر البيانات في هياكل البيانات الاخرى بواسطة ابدال البت الاقل اهمية [11].اذ يتم تخزين المعلومات ومعالجتها في الحواسيب بشكل بتات وبذلك يكون نظريا البت أصغر وحدة حاملة أو ناقلة لمعلومة أو لمعنى ما معين. عمليا، في الحواسيب والمعالجات الرقمية، البت هو عبارة عن نبضة كهربائية تكون إما

موجبة أو سالبة (في الحقيقة تكون نبضة أقوى من الأخرى مثلا نبضة 5 فولت ونبضة1 فولت) ويرمز لها بأحد الرقمين الثنائيين إما1 أو0 البت عبارة عن خانة واحدة من رقم ثنائي وتسمى كل ثمانية بتات مجتمعة بايت, وله احتمالين أما ان يكون البت 0 أو يكون 1.

ان تقسيم البايت إلى 8 بت، ومعرفة البت الأقل أهمية من بينها، علماً أن البت لا يقبل سوى 0 أو 1 وتوزيع قيم البتات في البايت الواحد، يكون كالتالي:



وهذا ما يوضح أن البايت الواحد يمثل 256 قيمة (من 0 في حال جميع البتات تحمل قيمة 0) إلى (255 عندما تكون كل قيم البتات=1)، فلو أردنا تمثيل الرقم 65 بطريقة النظام الثنائي، بالتأكيد سيكون:[25]

0	1	0	0	0	0	0	1

ويمكن أن تستبدل الخلية الثنائية الأقل أهمية الأولى والثانية من النقاط الضوئية مع بقاء العين البشرية غير قادرة على تمييز الفرق بين الصورتين .وهناك أشكال متعددة لهذه الطريقة إذ يمكن نشر الرسالة السرية بصورة عشوائية على الغطاء باستخدام مفتاح سري يعد بذرة (Seed) لمولد أرقام عشوائية [23]، أو يمكن اختيار بعض المناطق الأقل تأثرا بالتشوهات لتضمين البيانات في الصورة بالاعتماد على خصائص الرؤية لدى الإنسان. وبالرغم من إن التغيرات الحاصلة على الصورة بفعل هذه الطريقة تكون غير واضحة إلا أن هذه الطريقة تكون حساسة جدا لكثير من الهجمات خصوصا هجمات معالجة الصور.

4 - علم التشفير:

علم التشفير (Cryptography) هو العلم الذي يختص بحماية المعلومات من الاشخاص غير المخولين الذين يحاولون ان يتعرضوا المعلومات او العبث بها،وهو الذي يسمح ايضا للمستخدم بالتغيير الجذري للمعلومات لغرض اخفاء محتواها او مغزاها عن طرف ثالث.والتشفير يسمح لمستخدمي شبكات الاتصالات التعامل معها بثقة(6) .وهنالك نوعين من خوارزميات التشفير، خوارزميات التشفير المتماثلة ،اذا يستخدم نفس المفتاح في التشفير وكسر الشفرة ويبقى سريا بين المرسل والمستقبل، وخورزميات التشفير غير المتماثلة فهنالك مفتاحان الاول يستخدم في التشفير والاخر يستخدم في فك الشفرة, هو العلم الذي يختص بحماية المعلومات من الأشخاص غير المخولين الذين يحاولون ان يعترضوا المعلومات او العبث بها [24]. ويكون متماثل وغير متماثل والانسيابي.

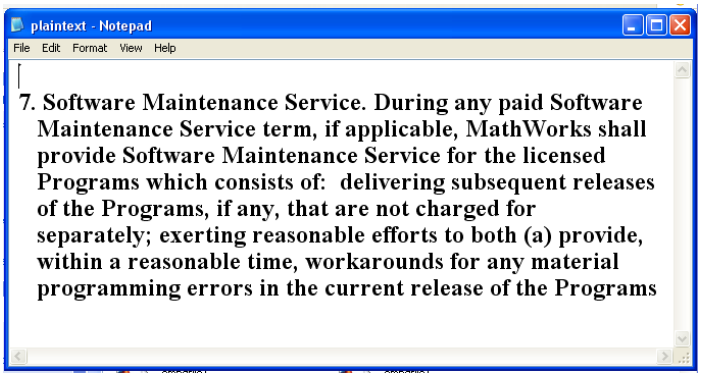
5 - الجانب العملي

5-1 التضمين في الملفات الصورية:

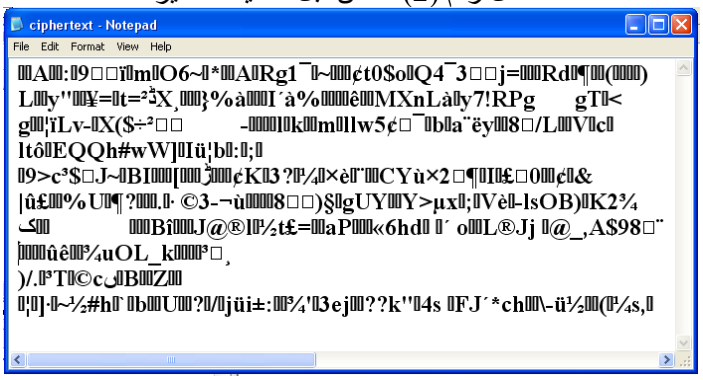
إن عملية الإخفاء تبدأ بإدخال صورة الغطاء والرسالة السرية ومفتاحي التشفير والإخفاء تتلخص عملية الإخفاء أولاً بتشفير الرسالة السرية باستخدام التشفير الانسيابي الخطي وأخيراً تضمين الرسالة السرية المشفرة في صورة. وتتناول الفقرات التالية شرح مراحل عملية الإخفاء بالتفصيل.

5-1-1 تشفير الرسالة السرية :

تم استخدام التشفير الانسيابي الخطي لتشفير الرسالة السرية . يتم أولاً إدخال المفتاح السري الذي يمثل مراحل LFSR)) والروابط فيما بينها , ثم إدخال بيانات النص الصريح (بعد تحويلها إلى سلسلة ثنائية) كما في الشكل (2) بعد ذلك سوف يتم عمل تزحيف للمراحل (Stages) باتجاه اليسار وبقيمة واحدة , ثم يتم تمرير القيمة اليسرى التي تم تزحيفها خلال دالة التغذية الخلفية ويتم جعل قيمة المسجل الأيمن مساوية لناتج دالة التغذية الخلفية. تستمر عملية ألتزحيف هذه إلى أن تكون السلسة الناتجة مساوية لطول سلسلة النص الصريح , بعد ذلك يتم عمل (XOR) بين سلسلة النص الصريح والسلسلة المولدة , فيكون الناتج سلسلة النص المشفر التي سيتم إخفائها داخل الصورة وكما في الشكل رقم (3).



الشكل رقم (2) النص قبل عملية التشفير



الشكل رقم (3) النص بعد عملية التشفير

2-1-5 عملية تضمين الرسالة المشفرة في الصورة

تم استخدام الصور الملونة او الرمادية(BMP,JPEG,TIF,PNG) كغطاء لخزن البيانات السرية المراد إخفاؤها فإذا كانت الصورة ملونة فيتم تحويل الصورة إلى صيغة YCbCr (هذه الصيغة ستحول الصور الملونة إلى ثلاث طبقات هي Y وهي تمثل شدة إضاءة الصورة , Cb التي تمثل التلوينة الزرقاء و Cr التي تمثل التلوينة الحمراء) ثم تغيير نقاط الصورة في طبقة Y عن طريق استخدام الخلية الثنائية الأقل أهمية (Least Significant Bits) من كل خلية ثمانية (Byte) .إما إذا كانت الصورة غير ملونة فتبقى كما هي بدون تحويل ويتم التضمين فيها مباشرة.

ولزيادة السرية فان عملية اختيار مواقع التضمين تمت بصورة عشوائية وليس تسلسلية باستخدام مواقع عشوائية يتم توليدها من دالة الأرقام العشوائية.ويتم استخدام مفتاح سري (Key) الذي يمثل البذرة (Seed) لدالة توليد الأرقام العشوائية.

يتم حساب طول السلسلة المراد تضمينها ثم يتم تحويل هذا الطول إلى النظام الثنائي ممثل بستة عشر خلية ثنائية (bit16) ثم يتم إبدال هذه القيم بقيم البت الثاني لأول(16byte) من صورة الغطاء (وذلك تجنباً للبت الاول والذي من المحتمل ان تختاره الدالة العشوائية عندما تتعرض لتلك ال 16 بايتات الاولى من الملف الغطاء) تعتبر هذه الخطوة ضرورية في عملية الاسترجاع. بعد الانتهاء من عملية التضمين يتم إرجاع الصورة إلى أصلها إذا كانت ملونة ثم خزنها وألا يتم خزنها مباشرة.

1-2-1-5 خطوات خوارزمية التضمين:

1- إدخال الصورة الغطاء (cover image)
2- إدخال الرسالة السرية المشفرة
3- إدخال مفتاح التضمين (seed)
4- تحويل الصورة من نظام RGB إلى نظام YCbCr إذا كانت الصورة ملونة واستخدام المصفوفة Y لغرض التضمين
5- تحويل الرسالة السرية إلى صيغة binary
6- خزن طول الرسالة ابتداءا من البت الثاني لأول (16 byte) من ملف الغطاء
7- توليد مصفوفة المواقع العشوائية R عدد عناصرها يساوي عدد عناصر المصفوفة Y لغرض نشر بتات الرسالة بصورة عشوائية على الصورة
8- لكل بت I من بتات الرسالة المشفرة استبدل قيمة ذالك البت بقيمة البت الأقل أهمية (LSB) لقيمة الموقع R(I) من مصفوفة الصورة (Yفي الصورة الملونة) حيث ان R هي مصفوفة المواقع العشوائية.

9- تحويل الصورة من نظام YCbCr إلى نظام RGB إذا كانت ملونة إما إذا كانت غير ملونة فتبقى كما هي ان ناتج هذه الخطوة هو الملف النهائي المضمن للمعلومات (Stego image)
10- خزن الملف المضمن للمعلومات (Stego image)
11- النهاية

2-5 عملية الاسترجاع من الملفات الصورية:

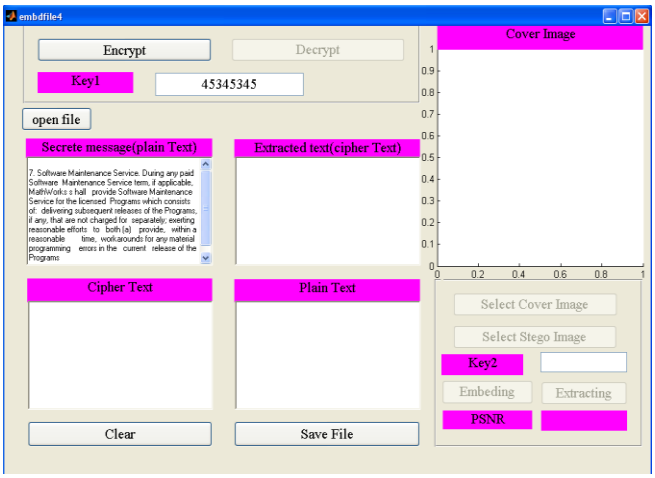
تتلخص العملية أولاً باسترجاع طول الرسالة , ثم استرجاع البيانات المشفرة من الصورة المضمنة , وأخيرا القيام بعملية فك الشفرة للبيانات باستخدام التشفير الانسيابي الخطي. في البداية يتم تحويل الصورة إذا كانت ملونة إلى صيغة YCbCr وألا تبقى كما هي أول خطوة في عملية الاسترجاع هو استرجاع طول البيانات المخفية من البت الثاني لأول (byte-16) من الصورة المضمنة ثم يتم الاعتماد على هذا الطول في استرجاع البيانات المخفية من باقي نقاط الصورة.بعدها يتم توليد المواقع العشوائية لمعرفة تسلسل المواقع التي تم إخفاء البيانات فيها إثناء عملية التضمين ويتم أيضا استخدام مفتاح سري (Key) الذي يمثل البذرة (Seed) لدالة توليد الأرقام العشوائية لتوليد نفس المواقع المستخدمة في عملية التضمين.

بعدها يتم استرجاع البيانات المخفية عن طريق عن طريق استخلاص البت الأول من قيم المواقع العشوائية في الصورة بعد استرجاع البيانات المشفرة يتم القيام بعملية فك الشفرة وذلك باستخدام نفس الخطوات التي تمت في عملية التشفير للحصول على النص الصريح.

1-2-5 خطوات خوارزمية الاسترجاع:

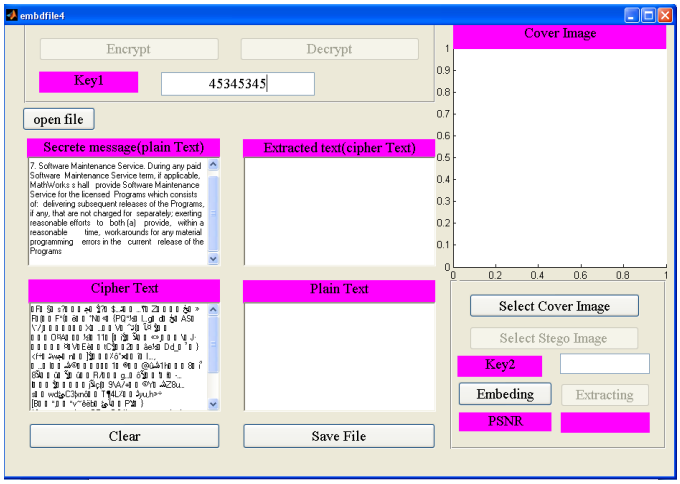
1- إدخال الصورة المضمنة (Stego image)
2- إدخال مفتاح التضمين (seed)
3- إدخال مفتاح التشفير
4- تحويل الصورة من نظام RGB إلى نظام YCbCr إذا كانت الصورة ملونة واستخدام المصفوفة Y لغرض استخلاص الرسالة
5- استخلاص طول الرسالة من البت الثاني لأول (byte-16) من الصورة
6- توليد مصفوفة المواقع العشوائية R عدد عناصرها يساوي عدد عناصر المصفوفة Y لغرض مواقع البيانات المخفية في الصورة
7- إلى ان يتم الوصول إلى طول الرسالة المشفرة استخلص قيمة البت I من الرسالة المشفرة من قيمة البت الأقل أهمية (LSB) لقيمة الموقع R(I) من مصفوفة الصورة (Yفي الصورة الملونة) حيث ان R هي مصفوفة المواقع العشوائية
8- فك تشفير البيانات الثنائية
9- عرض النص الصريح
10- النهاية

استخدام واجهة المستخدم الصورية GUI المدعومة من قبل بيئة MATLAB لتنفيذ خوارزميات الإخفاء المقترحة, لمناقشة النتائج يتم البدء أولا بإدخال والنص الرسالة السرية ويتم إدخالها إما بصورة مباشرة من لوحة المفاتيح او من ملف نصي موجود في الكومبيوتر عن طريق الضغط على زر Open file كما في الشكل رقم (4).

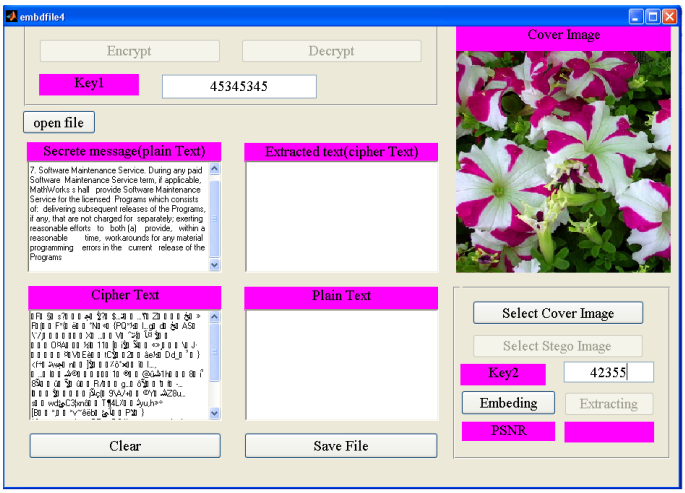


الشكل رقم (4) ادخال النص الصريح

الخطوة التالية هي الضغط على زر Encrypt ليتم تشفير الرسالة وعرض النص المشفر في مربع النص الثاني وعند الضغط على هذا الزر يتم تفعيل زر اختيار ملف الغطاء (cover image) select وزر التضمين (Embedding) وإيقاف تفعيل زر (Encrypt) كما في الشكل (5). الخطوة التالية إدخال صورة الغطاء عن طريق الضغط على زر(select cover image) وادخال مفتاح التضمين كما في الشكل (6).

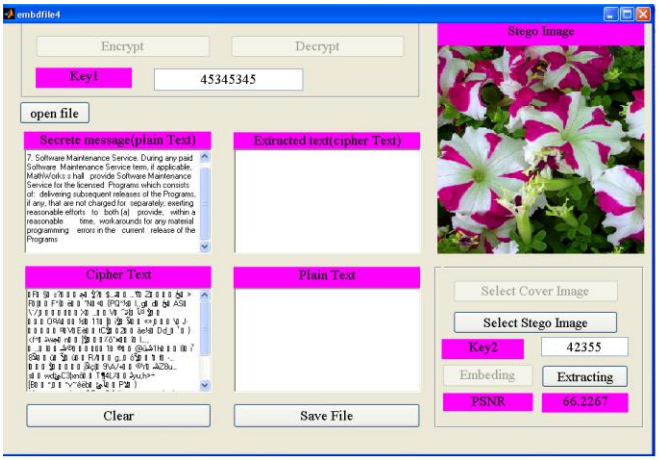


الشكل رقم (5):تشفير النص الصريح

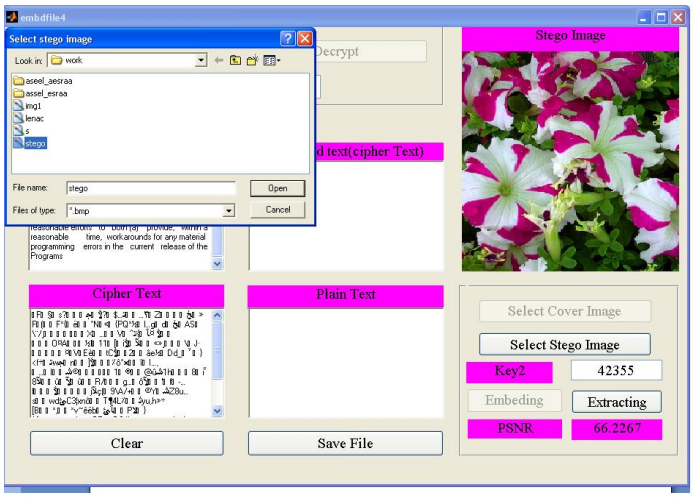


الشكل رقم (6) ادخال صورة الغطاء

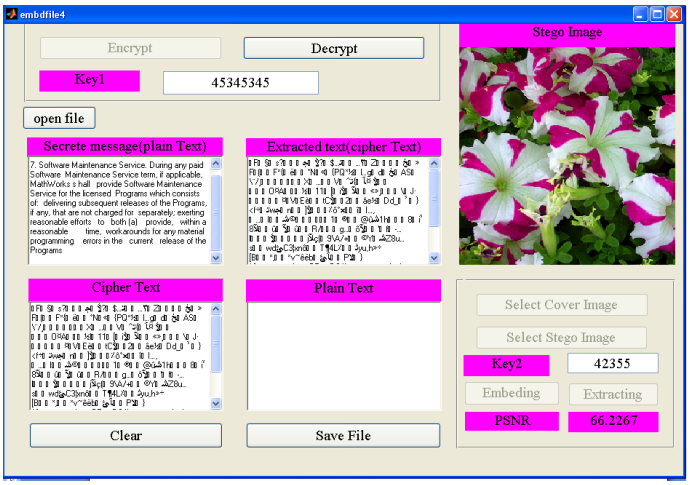
الخطوة الرابعة الضغط على زر (Embedding) ليتم تضمين النص المشفر عند اكتمال عملية التضمين يتم فتح نافذة لحفظ الملف المضمن و حساب قيمة PSNR وعرضها وبعدها يتم تفعيل زري اختيار الملف المضمن (select Stego image) وزر الاستخلاص (Extracting) وعرض الملف المضمن كما في الشكل (7). الخطوة الخامسة الضغط على زر (select Stego image) لاختيار ملف الغطاء ثم عرضه كما الشكل (8), الخطوة السادسة الضغط على زر Extracting لاسترجاع البيانات المشفرة وعرضها في مربع النص الثالث وتفعل زر Decrypt وإلغاء تفعيل زرselect Stego image وزر Extracting كما في الشكل (9).



الشكل رقم (7) تضمين النص

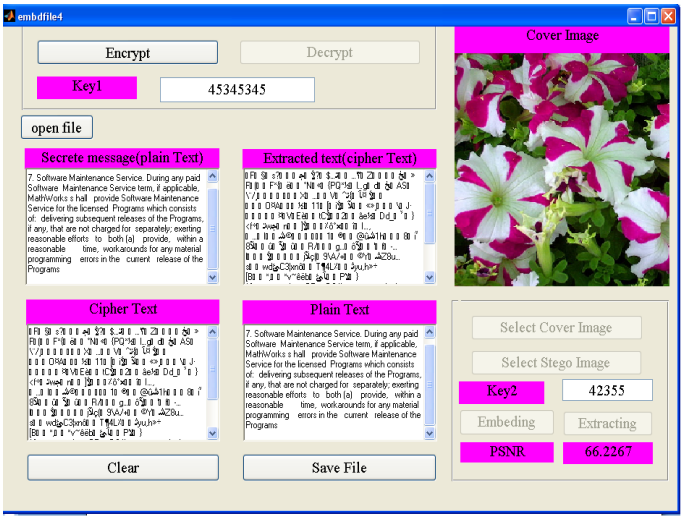


الشكل رقم (8) اختيار الملف الغطاء



الشكل رقم (9) استخلاص النص المشفر من صورة الغطاء

وأخيرا الضغط على زر Decrypt لفك تشفير الرسالة المشفرة وعرض النص الصريح في مربع النص الرابع وإلغاء تفعيل زر Decrypt كما في الشكل (10). ان وظيفة الزر Clear الموجود في أسفل الواجهة هو عمل Restart للبرنامج حيث يتم تصفير جميع البيانات المخزونة في البرنامج والبدء من جديد.



الشكل رقم (10) فك التشفير للنص وعرض النص الصريح

5- 3 حساب مقاييس جودة الطريقة:

ان تقييم الاداء لطريقة معينة بالاعتماد على رؤية الانسان يكون غامضاً وغير دقيق لانه يعتمد على خبرة الشخص ونظام الرؤية لديه،ولكن ممكن الاعتماد عليه لاثبات نجاح او فشل الطريقة،لذا يتم اعتماد طرق تقييم موضوعية لقياد جودة الطريقة المستخدمة ومن الطرق مقياس Root Mean Squar (RMSe) و(Peak Signal to Noise Ratio (PSNR

وقد تم تطبيق مقياس RMSe وحسب المعادلة التالية:

$$\mathbf{RMSe}=\sqrt{1/N^2\sum_{r=0}^{n-1}\sum_{c=0}^{n-1}[I_{new}(r,c)-I_{old}(r,c)]^2}$$

اذا ان:

N^2: تمثل حجم المصفوفة الكلي اذا كانت الصورة مربعة , وفي حالة كون الصورة غير مربعة تستبدل ب (N*M), حيث إنN تمثل البعد الأول و M تمثل البعد الثاني .

I_{new} : تمثل الصورة الجديدة.

I_{old}: تمثل الصورة القديمة

وقد تم اخذ 5 صور مختلفة الحجم وتطبيق الطريقة وكانت نتائج مقياس RMSe كما هو موضح بالجدول(1) بعد الحصول على هذه النتائج يتم مقرنتها مع الصفر فكلما كانت النتيجة اقرب الى الصفر كلما زادت جودة الطريقة, وكما تم تطبيق مقياس PSNR(Peak Signal to Noise Ratio) وكانت النتائج كما هو موضح في الجدول (1).

اسم الصورة	RMS	PSNR
Image1.Jpeg	0.053	66.2267
Image2.Jpeg	0.053	72.6501
Image3.Jpeg	0.027	72.7353
Image4.jpeg	0.071	84.9923

72.4395	0.028	Image5.jpeg
72.5225	0.028	Image6.jpeg
72.6501	0.055	Image7.jpeg
66.7532	0.034	Image8.jpeg
69.3899	0.012	Image9.jpeg
67.896	0.049	Image10.jpeg

جدول (1) يمثل نتائج مقياس (RMSe) و(PSNR) لأربع صور مختلفة

6-1 الاستنتاجات:

1- ان النص الذي تم استخلاصه من عملية الاسترجاع يشابه تماما النص الذي تم تضمينه في الصورة ومن الممكن حفظ البيانات المسترجعة في فايل نصي مستقل عن طريق الضغط على زر Save file في البرنامج حيث يتم فتح نافذة حفظ الملف تطلب من المستخدم إدخال اسم الملف النصي وبذلك يتم حفظ محتويات مربع النص الرابع الذي يحتوي على النص بعد عملية الاسترجاع في الفايل النصي الذي تم اختياره.
2- أثبتت النتائج العملية كفاءة الخوارزميات من ناحية ان المعلومات المخفية لم تحدث أي تغيير او تشوه على ملفات الغطاء المستخدمة.
3- تتميز خوارزميات الإخفاء المستخدمة بالقوة Robustness حيث انه من الصعب جدا الاستدلال على وجود أي معلومات مخفية وكشفها.
4- يتميز نظام الإخفاء المستخدم بالمرونة العالية وسهولة الاستخدام .

6-2 التوصيات:

- تطوير عملية إخفاء البيانات النصية وان يتم تطرق إلى طرق أخرى غير الطريقة المتبعة في هذا المشروع
- تطبيق خوارزمية الإخفاء على الملفات الصوتية او ألفيديوية.
- استخدام طرق تشفير أكثر تعقيدا لتشفير النص وتضمينه داخل الصورة.
- استخدام صوره من نوع PNG وGIF وذلك لانتشار هذه الأنواع من الصور نظرا لصغر حجمها وجودتها.

المصادر

[1] عبد المجيد،انسام، طريقة جديدة للكتابة المغطاة في الصور المكبوسة بالتكميم الاتجاهي،رسالة ماجستير،كلية علوم الحاسوب والرياضيات،جامعة الموصل 2011.

[2] بيبو, اميرة سلو,"تقنيات إخفاء المعلومات بإستخدام الشبكات العصبية وبروتوكولات الشبكة", بحث ماجستير ،كلية علوم الحاسوب والرياضيات،جامعة الموصل،العراق2009.

[3] Katzenbeisser, Stephan and Petitolas, Fabien (2000), "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Inc, London.

[4] Chandramouli R and Memon N,“Analysis of LSB based image steganography techniques”,Proceedings 2001 International Conference on Image,Vol. 3, pp.1019-1022.

[5] الصميدعي ، عامر تحسين سهيل، 2002،" تطبيق نظام التغطية "،بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[6] Xiangyang Luo, Fenlin Liu,” A LSB STEGANOGRAPHY APPROACH AGAINST PIXELS SAMPLE PAIRS STEGANALYSIS” International Journal of

Innovative Computing, Information and Control Vol 3, No. 3, June 2007 ISSN 1349-4198.

[7] Morkel.T, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference , Sandton, South Africa, (2005).

[8] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp. 1062-1078, July (1999).

[9] Weiqi Luo, , Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions Forensics and Security, Vol 5 ,No. 2, June 2010.

[10] Du W. C. and Hsu W. J., (2003), *"Adaptive Data Hiding Based on VQ Compressed Images"*, IEE Proc.-Vis. Image Signal Process., Vol. 150, No. 4, pp. 233-238.

[11] أحمد سامي نوري أحمد/ كلية علوم الحاسبات و الرياضيات /جامعة الموصل/اطروحة دكتوراه.

[12] Md. Khairullah " A Novel Text Steganography System in Cricket Match Scorecard", International Journal of Computer Applications (0975 – 8887) Volume 21– No.9, May 2011 43 Assistant Professor, Department of Computer Science and Engineering.

[13] الصميدعي،عامر تحسين سهيل،"تطبيق نظام التغطية"،بحث ماجستير،كلية علوم الحاسوب والرياضيات،جامعة الموصل، العراق،2002

[14] Al-Husainy M. A. F., (2009), "*Image Steganography by Mapping Pixels to Letters"*, J. Computer Sci.,Vol. 5, No. 1, pp. 33-38.

[15] Wang H. and Wang S., (2004), *"Cyber Warfare: Steganography vs. Steganalysis*", Communications of The ACM, Vol. 47,No. 10, pp.76-82.

[16] Rocha A., and Goldenstein S., "*Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?"*, RITA,Vol. 15, No. 1, pp.83-110. (2008).

[17] الحمامي،علاء حسين والحمامي، محمد علاء(2008)،"اخفاء المعلومات:الكتابة المخفية والعلامة المائية"،اثراء للنشر والتوزيع، الشارقة.

[18] Ali, Dujan Basheer Taha, (2004), "Digital Image Watermarking Techniques for Copyright Protection", Unpublished D. Ph. Thesis, University of Mosul, Iraq.

[19] Whitiak, Deborah A. ,2003, "The Art of steganography" (v1.4b).
http:\\www.giac.org/practical/GSEC/Deborah-Whitiak GEEC.pdf

[20] يحيى شيماء شكيب محمد ، الإخفاء في ملف صوت مكبوس، بحث ماجستير،2002 ،كلية علوم الحاسبات والرياضيات،جامعة الموصل،العراق.

[21] Jonathan Watkins ,"Steganography – Hidden In Bits", University of Southampton, SO17 1BJ, UK,15th December 2001.

[22] Saha.,Salah J. " image compression from DCT to wavelete Reio ahaimg coding.htm, http://www.acm.org/crossronds/xrds6-3/ , 2001.

[23] صالح، إبراهيم أحمد ,(2002)، " كبس الصور باستخدام تحويلات الموجة والمكمم الاتجاهي"، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، الموصل، العراق.

[24] الغريري،شهد عبدالرحمن حسو،2003،"تطبيق نظام حماية هجين وتطبيقه على النصوص"، بحث ماجستير،كلية علوم الحاسوب والرياضيات،جامعة الموصل، العراق.

[25] برزنجي، فوزي، "فن الاختزال " ،جامعة السليمانية www.boosla.com

Appendix

Image1.Jpeg:

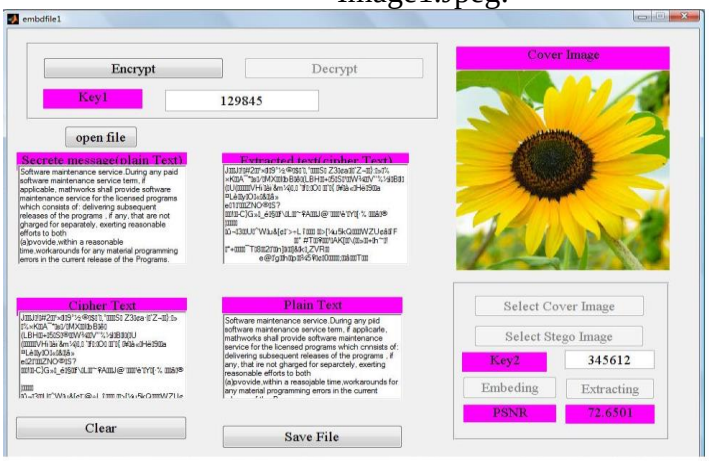


Image2.Jpeg:

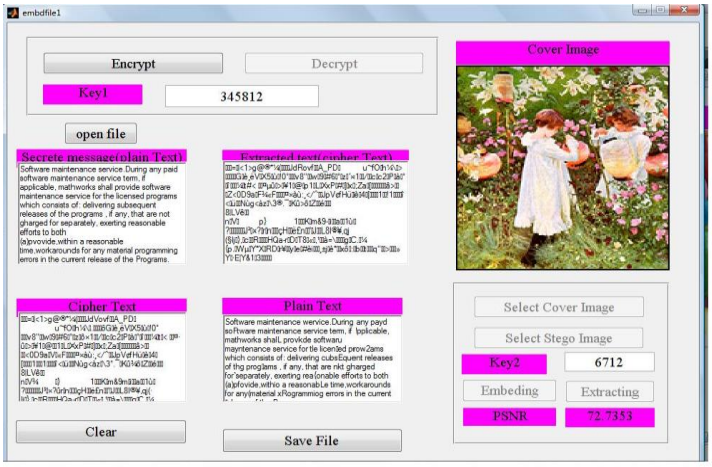


Image3.Jpeg

Image4.Jpeg

Image5.Jpeg

Image6. Jpeg

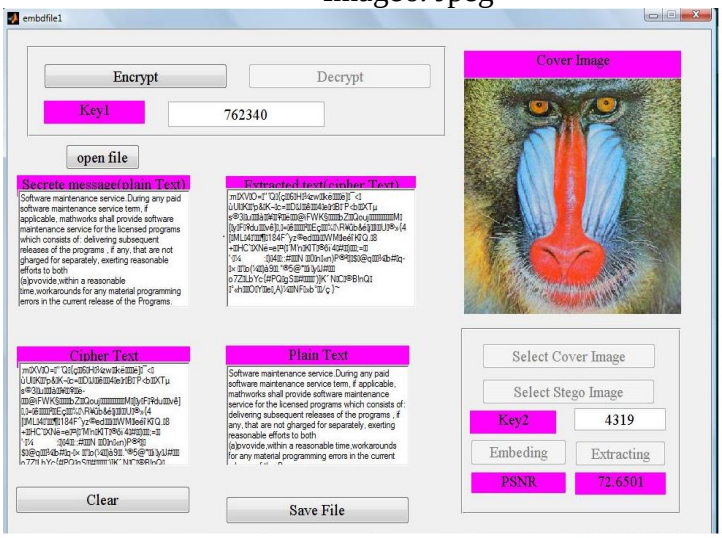


Image7.Jpeg

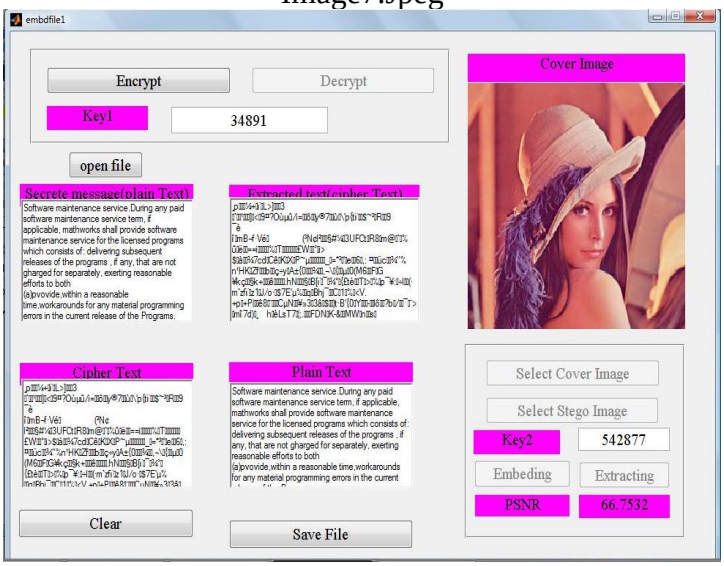


Image8.Jpeg

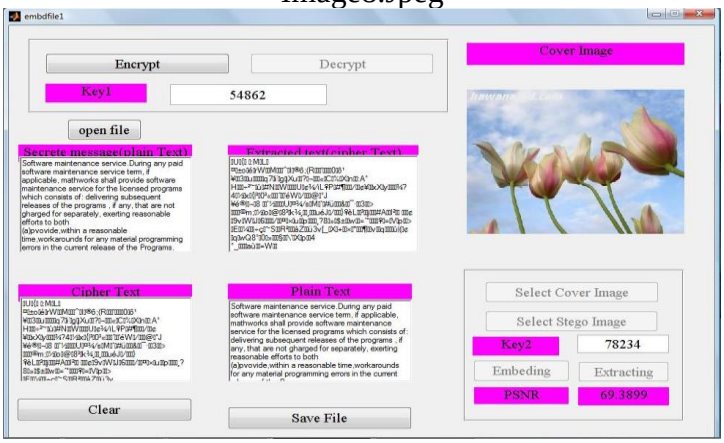


Image9.Jpeg