Use the Genetic Algorithm to Encode and Hide Gray Image Data

Raya Jassim Essa **Reham Jassim Essa** **Inam Muhammad Sulaiman**

College of Computer Science and Mathematics
University of Mosul, Mosul, Iraq

College of Education
University of Mosul, Mosul, Iraq

Received on: 09/10/2012 **Accepted on: 30/01/2013**

ABSTRACT

With the development of means of communication, computer science and information exchange via electronic information networks an urgent need emerged to find ways to save exchanged information. Encryption had a prominent role in this area. However, with the development of intrusion hackers become able to access to information and change it. This showed the need to adopt more sophisticated technology and more confidentiality in order to preserve the information. So, it become famous to use the system of coverage in which the sent the information being invisible to anyone, through hiding it inside the sent media, such as audio, image, text, and video.

This paper aims to apply the idea to hide image message, using the least significant bit algorithm inside an image and encrypt it in a new way for encryption using a genetic algorithm. For the purpose of increasing security of the access of the letter it is being encrypted to hide the message before using the genetic algorithm to generate random numbers employed in the process of concealment, for the highest extent of randomness. This in turn increases the strength of encryption and concealment. The study has been able to achieve this by adopting the recommended approach in such cases

Keywords: Encryption, genetic algorithm, security.

استخدام الخوارزمية الجينية في تشفير بيانات صورية رمادية وإخفاءها في صورة

ريا جاسم عيسى **رهام جاسم عيسى** **إنعام محمد سليمان**

كلية علوم الحاسوب والرياضيات
جامعة الموصل

كلية التربية
جامعة الموصل

تاريخ استلام البحث: 2012/10/09 **تاريخ قبول البحث: 2013/01/30**

الملخص

مع تطور وسائل الاتصال وعلم الحاسوب وتبادل المعلومات عبر شبكات المعلومات الإلكترونية برزت الحاجة الملحة لإيجاد وسائل لحفظ المعلومات المتبادلة. فكان للتشفير دور بارز في هذا المجال. على أية حال، 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 التغطية الذي تكون فيه المعلومات المرسلة غير مرئية لأي شخص وذلك عن طريق إخفائها داخل الوسائط المرسلة، مثل الصوت، الصورة، النص، والفيديو.

يهدف البحث إلى تطبيق فكرة إخفاء الرسالة الصورية باستخدام خوارزمية البت الأقل أهمية (LSB) داخل صورة وتشفيرها بطريقة جديدة للتشفير باستخدام الخوارزمية الجينية. ولغرض زيادة أمنية وصول هذه الرسالة يجري تشفير الرسالة قبل إخفائها باستخدام الخوارزمية الجينية لتوليد الأرقام العشوائية الموظفة في عملية الإخفاء، لتحقيق أعلى مدى من العشوائية. وهذا بدوره يزيد من قوة التشفير والإخفاء. وقد تمكنت الدراسة من تحقيق ذلك وأوصت باعتمادها أسلوبا في مثل هذه الحالات.

الكلمات المفتاحية: التشفير، الخوارزمية الجينية، امنية.

1- المقدمة

بات علم أمن المعلومات محل اهتمام كبير من قبل الباحثين والمهتمين والذين يحاولون الحصول على حلول وتقنيات جديدة ومحدثة لضمان حماية المعلومات التي ترسل وتستقبل عبر الشبكة العالمية للمعلومات (الانترنيت) دون حدوث أي اختراق أو كشف من قبل المتدخلين.لذلك كان لابد من مواكبة تطوير أمنية المعلومات وإنشاء تقنيات ووسائل متطورة ومن هنا ظهر علم إخفاء المعلومات (Information Hiding) وتطور باعتماد تقنية الإخفاء Steganography.

تعد تقنية الإخفاء من طرائق الحماية التي تجعل البيانات المرسلة والمستقبلة غير مرئية،وذلك بإخفاء رسائل معينة داخل غطاء معين. والهدف المتحقق بعملية الإخفاء هو عدم إثارة أي نقطة للشك بوجود بيانات مخفية، في حين أن هدف محلل الإخفاء هو الشك في كل الرسائل المُرسلة، وفحصها للتأكد من وجود بيانات مخفية فيها. تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية أو قراءتها أو تغييرها أو حذفها بعملية فك الإخفاء Steganalysis.

لذا ظهرت الحاجة إلى إيجاد وسائل متعددة، لغرض إيصال المعلومات والبيانات بصورة صحيحة ومحمية من اطلاع الجهات غير المخولة بالاطلاع على هذه المعلومات [6][5] فظهر علم التشفير (Cryptography) فهو العلم الذي يعنى بالطرائق التي تجهز المعنيين بحماية خزن المعلومات ونقلها في مجال واسع، وهذه الطرائق تعتمد على مفتاح سري يستخدم لتشفير البيانات.

وعلى الرغم من كون التشفير طريقة جيدة لحماية المعلومات إلا انه سهل الاكتشاف ويمكن لأي متطفل التلاعب بها، فكانت الحاجة إلى تقنية أكثر تطورا وأكثر سرية وحفاظا على المعلومات وخصوصا مع ظهور وتطور الشبكة العالمية للمعلومات(الانترنت) فتم اللجوء إلى نظام التغطية**[2]**، لان رؤية البيانات بصيغتها المشفرة تكفي لدفع المتطفل أو المهاجم إلى الاعتقاد بوجود بيانات مهمة أو حساسة تكمن في العشوائية أو في النص المشفر، فيبدأ باستخدام التقنيات المضادة للتشفير لمحاولة الحصول على محتواها، وحتى لو عجز عن تحقيق ذلك فانه قد يعبث بها أو يحرفها أو يستخدم بعض الوسائل المتاحة لمنع وصولها إلى هدفها [4].

إنّ التحدي الكبير والرئيسي الذي واجهه حقل أمنية المعلومات هو ظهور الشبكات الحاسوبية ووسائل الاتصال لكي يتم خزن المعلومات وإدخالها وتزويدها داخلياً ضمن المنظمات وخارجياً من الأجهزة المضيفة البعيدة وإليها. لذا تم إضافة تعبير جديد إلى مسرد أمنية المعلومات وهو أمنية الشبكات، والذي يعرف بأنه الحِماية الصحيحة لكلِّ المكونات المرتبطة بالشبكة الحاسوبية، بضمنها البيانات وأدوات الاتصال والبنية التحتية **[11]**

الدراسات السابقة:

هنالك دراسات عديدة سابقة في علم الإخفاء فقد قامت الباحثة شيماء شكيب محمد في سنة 2004 في البحث بموضوع الإخفاء في ملف صوت مكبوس ، والباحثة أميرة بيبو سلو في سنة 2009 في البحث بموضوع تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة، والباحثات نادية معن محمد وهمسة معن محمد وشيماء شكيب محمد في سنة 2011 في البحث بوضع طريقة خوارزمية جينية مثلى للإخفاء في جامعة الموصل.

اتجه الباحثون إلى استخدام المفاهيم الذكائية لحل مشكلات أمنية الشبكات. تم بتقنية كشف إساءة الاستخدام اختيار الخوارزمية الجينية بسبب خصائصها الجيدة، مثل الممانعة ضد التشويش Robust to (Noise)، والمرونة، وعدم الحاجة لمعلومات مرتبة لإيجاد حل امثل أو شبه امثل، وقابلية التعلم الذاتي، والأمثلية مع متغيرات مستمرة أو متقطعة، والتعامل مع عدد كبير من المتغيرات، وملاءمة للحواسيب المتوازية، والعمل مع مجموعة حلول لا حل منفرد، وتشفير المتغيرات، لذا تتم الأمثلية بمتغيرات مشفرة، والعمل مع بيانات مولدة عددياً، وبيانات تجريبية، أو دوال تحليلية [14]

وتعد الخوارزميات الجينية (Genetic Algorithms) والتي ابتكرها العالم (هولا ند) واحدة من خوارزميات البحث العامة المعتمدة على آلية الانتقاء الطبيعي ونظام الجينات الطبيعية، وفكرة العمل هنا تعتمد بشكل دقيق على أفكار الهندسة الوراثية والتي تتميز بالإنتاج المقصود لأفراد جديدة تمتلك صفات مرغوبة (جيدة) وذلك من خلال التبديل والتعديل المقصود للمجموعات الموروثة (إضافة مواد وراثية معينة أو استبدالها) بهدف تكوين أفراد ذات صفات جيدة، وعلى هذا الأساس تقوم الخوارزمية الجينية (Genetic Algorithms) بانتخاب الحلول المفضلة من عدد كبير من الحلول وإجراء بعض التداخلات والتبديلات بين هذه الحلول بهدف تكوين حلول أفضل [7].

2- أنواع الصور:

تقسم الصور الرقمية إلى الأنواع التالية:

1- الصور الثنائية: هي ابسط أنواع الصور تتمثل باللونين الأبيض والأسود أو يرمز له بالصفر أو الواحد فالصورة الثنائية يمكن أن يشار إليها بالمعنى (1 bit per pixel) [9].

2- الصور رمادية التدرج: هي النوع الثاني من الصور الرقمية تحوي معلومات إضاءة فقط لا توجد معلومات لون [3]، يشار إلى الصور ذات التدرج الرمادي بالمصطلح (Monochrome) أو بالصور ذات اللون الواحد (One Color Image)، وهي تحتوي معلومات الإضاءة (Brightness) فقط، تحتوي كل صورة على (8 Bit/Pixel) أي (1Byte) لتمثيل كل عنصر فيها، أي إنها تسمح لـ 256 مستوى من مستويات الإضاءة من 0 (أسود) إلى 255 (أبيض)[5] .

3- الصور الملونة: هناك مجموعة من الألوان تدركها العين البشرية والتي تنتج ببساطة بإضافة نسب من الألوان الأساسية (الأحمر والأخضر والأزرق) هذه الألوان تعرف بالألوان الأساسية ومن الممكن تكوين كل الألوان المرئية بتجميع الألوان الثلاثة. هذه الألوان الثلاثة شكلت الأساس لفضاء الألوان (RGB). وتتكون من ثلاثة أحزمة (3 Bands) كل حزمة تمثل بـ (Byte) واحداً لذا يمكن القول إن كل عنصر في الصورة الملونة يتم تمثيله بـ (3Byte) وهذا يوضح سبب كبر حجم الصور الملونة بالمقارنة مع سابقاتها [3].

3- الخوارزمية الجينية

تعد الخوارزمية الجينية Genetic Algorithms أحد أساليب الذكاء الاصطناعي وهي من الأساليب الحديثة، إذ برزت أهمية استخدام هذا الأسلوب في حل مسائل معقدة (كبيرة الحجم تمتلك كما هائلا من الحلول البديلة) خلال زمن مناسب. والحل الناتج من تطبيق الخوارزمية الجينية يكون في أغلب الأحيان حلا قريبا إلى المثالي (near optimal solution)، ويوفر هذا الأسلوب عند تطبيقه بحثا ذكيا بين عدد هائل من الخطط البديلة [7].

وقد استخدمت الخوارزمية الجينية بصورة واسعة في مجالات عديدة منها: معالجة الصور (Image Processing) وتمييز الأنماط (Pattern Recognition) وغيرها وقد لاقت نجاحاً كبيراً وعناية واسعة [13].

يعتمد أسلوب الخوارزمية الجينية في حل المسائل المختلفة على أفكار مستنبطة من علم الوراثة، والتي تهتم بشكل عام بكيفية إنتاج أفراد جديدة تمتلك صفات معينة (مرغوبة أو غير مرغوبة) وذلك من خلال التعديل أو التداخل أو التبديل الذي يحصل على المجموعات الموروثة بهدف تكوين أفراد جديدة [7]. تُعد الخوارزميات الجينية تقنيات أمثلية (Optimization) تستخدم عملية تطورية. وحل المشكلة يتمثل بوصفها هيكل بيانات يعرف بالكروموسومات. ويتم تقييم جودة الحل بدالة تسمى دالة التقييم (Fitness Function)، وتتولد سلسلة من الحلول الأولية (مجتمع عشوائي) من خلال مزيج من العمليات المشابهة لعملية تطورية، وتتجه العملية نحو تطوير حلول تمتلك جودة أفضل عند حساب دالة التقييم [10]، وتستمر عملية توليد الأجيال حسب قيمة معينة يتم اختيارها للتوقف [16].

والخوارزميات الجينية هي طرائق للبحث، والأمثلية وتعليم الماكنة المتوخاة بالمبادئ الطبيعية والحياتية. والخصائص الرئيسية التي تميز الخوارزميات الجينية من تقنيات الأمثلية الأخرى هي [10].

1. الخوارزمية الجينية تستعمل دالة التقييم مباشرة ولا تتوسع في معلومات إضافية.
2. الخوارزمية الجينية تبحث في المجتمع وهو عبارة عن مجموعة حلول وليس حلاً واحداً.
3. الخوارزمية الجينية تُرمِز كافة الحلول الكامنة للمسألة بدلاً من ضبط متغيرات القرار للمسألة مباشرة.
4. الخوارزمية الجينية تستخدم بعض قوانين الاحتمالية ولا تستخدم القوانين التقليدية.

وقد تم استخدام الشروط المعتمدة لاختبار العشوائية [8] وكما يأتي:

خوارزمية (1)

1- البداية
2- F=0
3- إذا كانت المراتب الثنائية المساوية لـ 1=المراتب الثنائية المساوية لـ0 فان F1=1 وإلا فان F1=0
4- إذا كان هناك كتلة من المراتب الثنائية بقياس n لا يوجد فجوة من المراتب الثنائية بقياس n فان F2=1 وإلا F2=0
5- إذا كان هناك فجوة من المراتب الثنائية بقياس n-1 وليست هنالك كتلة من المراتب الثنائية بقياس n-1 فان F3=1 وإلا F3=0
6- حساب دالة F=F1+F2+F3
7- إذا كان F=3 فان الفرد عشوائي وبخلافه فان الفرد غير عشوائي وسوف يتم اختيار الخوارزمية الجينية
8- النهاية

الخوارزمية الجينية

1- البداية
2- توليد جيل جديد عشوائي يسمى الجيل الابتدائي
3- حساب دالة F=Fitness وترتيبها
4- إيجاد الاحتمالية بقسمة قيمة (مجموع Fitness/Fitnesses)
5- إجراء عملية Seledtion باستخدام عجلة روليت وذلك بتوليد أفراد جدد عشوائيا أيضا.
6- إجراء عملية Crossover بين الجيل الجديد والقديم
7- إجراء الطفرة Mutation عشوائيا على الجيل الجديد
8- يتم اختبار نسبة من الجيل الجديد والجيل القديم
9- إعادة عملية اختبار العشوائية مرة أخرى على الجيل الجديد حسب الخوارزمية (1) لاختبار العشوائية
10- النهاية

4- التشفير والإخفاء

علم التشفير: يعود تاريخ التشفير إلى 4000 سنة حيث كان الإنسان يفضل أن يخفي كتابته. أن خوارزمية التشفير هي عبارة عن دالة رياضية تستخدم في عملية التشفير وفتح الشفرة، تستخدم اغلب خوارزميات التشفير مفتاح (K)، في بعض الأحيان تكون مفاتيح التشفير وفتح الشفرة هي نفسها ويسمى هذا النوع من التشفير بالمتناظر(symmetric). وفي أحيان أخرى تكون مفاتيح التشفير وفتح الشفرة على شكل أزواج تسمى خوارزميات التشفير من هذا النوع باللامتناظر (Asymmetric) [2].

إخفاء المعلومات: وهي طريقة لإخفاء البيانات بواسطة تغطيتها بوسائط معينة كملفات النصوص والصور والملفات الصوتية والفيديوية.[16] 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 [12].

إخفاء البيانات داخل الصورة

هناك نوعان من الصور ذات التمثيل الثماني:

- 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.

- الصور ذات التدرجات الرمادية

تم تجاوز مشكلة عدد المداخل اللونية وبقيت الحاجة إلى 256 لوناً فقط والتي تمثل التدرجات الرمادية.[1]
هناك عدة عوامل يجب أن تؤخذ بنظر الاعتبار عند اختيار نوع الصورة المراد استخدامها كحاملة للبيانات:

1. عند استخدام الصور الممثلة ببايت واحد لكل نقطة ذات التدرجات الرمادية تكون مناسبة للإخفاء، لان التغيير في القيم يكون اقل وضوحا واقل تمييزا من قبل العين البشرية، أما عند استخدام الصور الملونة ذات التمثيل الثماني فيفضل استخدام الصورة التي لا تحوي على مساحات لونية مستوية بنسبة كبيرة.
2. استخدام الصور الملونة الممثلة بثلاثة بايتات لكل نقطة توفر مرونة كبيرة عند استخدامها في الإخفاء، لان العدد الكبير من الألوان (أكثر 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 [15]

التقنيات المستخدمة لإخفاء البيانات داخل الصور:

1- الإخفاء في الخلية الثنائية الأقل أهمية

تعد تقنية الإخفاء في الخلية الثنائية الأقل أهمية Least Signifite Bit Insertion من أكثر التقنيات المعروفة وتمتاز بسهولة التنفيذ لكنها أكثر عرضة للهجوم، من الملاحظ في هذه الطريقة:

- إذا تم تغيير أول خلية ثنائية من كتلة الصورة الملونة الممثلة بـ 3 byte فان كل نقطة يتم فيها تغيير 3 bit، لان كل نقطة ممثلة بـ 3 byte وهذا التغيير لن يكون ملاحظاً للعين البشرية.
- عند استخدام الصورة الممثلة بـ 8 bit فيفضل استخدام الصور الرمادية، لان التغيير سيكون غير ملحوظ بينما تغيير أول بت من الصور الملونة لهذا النوع من التمثيل يؤدي إلى تغيير قيمة اللون من لون إلى أخر قد يكون مختلفاً عنه والذي يكون ملحوظاً.

2- الترشيح والحجب

تتم عملية الإخفاء بواسطة الترشيح والحجب Masking and Filtering بوضع علامة للصورة بشكل مشابه للعلامة المائية، تقنياً العلامة المائية لا تعد إخفاء، إذ أن الإخفاء هو إخفاء البيانات داخل الصورة أما العلامة المائية فهي امتداد لمعلومات الصورة وتعد ضمن صفات ملف الغطاء وتستخدم لضمان حقوق الملكية، هذه الطريقة أكثر ملاءمة للاستخدام مع الصور نوع JPEG بدلا من الطريقة السابقة بسبب الحصانة النسبية ضد الكبس [4].

5- الجانب العملي:

تم في هذا البحث إخفاء صور بامتدادات مختلفة (BMP, JPEG, TIF)، وصور ملونة أو غير ملونة، داخل صورة من نوع (BMP) ملونة أو غير ملونة، وقبل إخفاء الصورة يتم تشفير بياناتها باستخدام دالة Exclusive Or (XOR) مع أرقام عشوائية تم توليدها باستخدام الخوارزمية الجينية، وفيما يلي الخطوات الخاصة بالجانب التجريبي Empirical work. تقسم مراحل العمل إلى ثلاث مراحل:

المرحلة الأولى: يتم في هذه المرحلة توليد سلسلة من الأرقام العشوائية الثنائية باستخدام الخوارزمية الجينية وحسب الخطوات التالية:

1. يتم إنشاء الجيل الأول عشوائيا واستخدام طريقة الانتقاء الثنائي لعملية الانتقاء وطريقة التداخل وحيد النقطة لعملية التداخل وطريقة عكس إل bit لعملية الطفرة واستخدام الاختبار الإحصائي التطابق الذاتي Auto

Correlation Test لاختبار مدى لياقة أو جودة الكروموسوم. وتم تكوين ملف من BINARY.dat لخزن القيم المتولدة.

2. إدخال طول القيم العشوائية وعدد الأجيال المراد توليدها بالـ bytes عن طريق لوحة المفاتيح.
3. الانتقاء الذاتي يتم بإدخال حجم المجتمع وطول الكروموسوم بالبايت (LENC) وهيكل البيانات (كروموسومات وقيم دالة الهدف المحصورة بين (LENC)*8-1 فلو كان طول الـLENC يساوي 2 bytes فان قيمة دالة الهدف محصورة بين 1-16.
4. يتم إدخال حجم المجتمع وهيكل البيانات الخاص بالكروموسومات والحصول على كروموسوم واحد يمثل أباً واحداً ولهذا يجب استدعاءها مرتين لاختيار أبوين.
5. حساب الطفرة الوراثية باستخدام الجيل الأول والجيل الثاني وطول الكروموسوم.
6. خزن الأرقام العشوائية الناتجة في ملف Binary.dat.

وقد تم بناء دالتين لاختبار عشوائية المفتاح حيث تقوم الدالة الأولى بحساب عدد الواحدات والأصفار في المفتاح وترجع قيمة

المرحلة الثانية :

يتم في هذه المرحلة:

1- قراء ة الصورة المراد تشفيرها. كما في الشكل (1)
2- تحويل الصورة Gray Level إذا كانت الصورة ملونة. وستظهر الصورة كما في الشكل (2).
3- تشفير بيانات الصورة بتطبيق دالة XOR، (بين بيانات الصورة والأرقام العشوائية الناتجة من الخوارزمية الجينية والمخزونة في الملف Binary.dat) سيكون ناتج التشفير كما في الشكل (3).
4- إدخال صورة الغطاء إذ تم استخدام الصور من نوع (BMP) كغطاء لخزن الصورة المراد إخفاؤها باستخدام خوارزمية البت الأقل أهمية (LSB) لتغطية الصورة المشفرة كما في الشكل (4).
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.
5- إخفاء بيانات الصورة المشفرة في صورة من نوع BMP باستخدام خوارزمية البت الأقل أهمية.وتكون النتيجة كما في الشكل (5).

المرحلة الثالثة:

الاسترجاع من الملفات الصورية:

1- إدخال الصورة المضمنة
2- إدخال مفتاح التضمين (seed).
3- يتم استرجاع بيانات الصورة المشفرة من الصورة المضمنة، سيتم الحصول على صورة معتمة. كما في الشكل (6)
4- القيام بعملية فك الشفرة لبيانات الصورة المشفرة عن طريق إجراء عملية XOR مع الأرقام العشوائية المتولدة من الخوارزمية الجينية.سيتم الحصول على الصورة الأصلية المراد إخفاءها، كما في الشكل (7).

حساب مقاييس جودة الطريقة:

إن تقييم الأداء لطريقة معينة بالاعتماد على رؤية الإنسان يكون غامضاً وغير دقيق لأنه يعتمد على خبرة الشخص ونظام الرؤية لديه، ولكن يمكن الاعتماد عليه لإثبات نجاح أو فشل الطريقة، لذا يتم اعتماد طرائق تقييم موضوعية لقياد جودة الطريقة المستخدمة ومن الطرائق مقياس Root Mean Squar (RMSe) و Normalization Correlation Coefficint (NCC) و v

وقد تم تطبيق مقياس RMSe وحسب المعادلة التالية:

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

إذا أن:

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

I_{new}: تمثل الصورة الجديدة. I_{old}: تمثل الصورة القديمة.

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

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

اسم الصورة	ERMS	PSNR
Image1.bmp	**0.043**	**53.841**
Image2.bmp	**0.025**	**64.135**
Image3.jpg	**0.071**	**43.051**
Image4.jpg	**0.027**	**52.587**

نتائج التجريب

1- بعد تنفيذ العمل أثبتت النتائج إمكانية إخفاء صورة بأي امتداد كان في صورة من نوع BMP.

2- إن تشفير بيانات الصورة قبل إخفائها أعطى سرية اكبر إذ انه إذا تمكن الشخص غير المخول من إزالة الغطاء فانه سيجد صورة سوداء (معتمة) ولن يتوقع وجود صورة أخرى.

3- إن استخدام الخوارزمية الجينية في توليد الأرقام العشوائية أكفأ من استخدام الطرائق التقليدية لتوليد الأرقام.

4- بعد إزالة الغطاء وفك الشفرة فان الصورة الناتجة ستكون مطابقة تماما للصورة الأصلية ولكن بهيئة Gray Level.

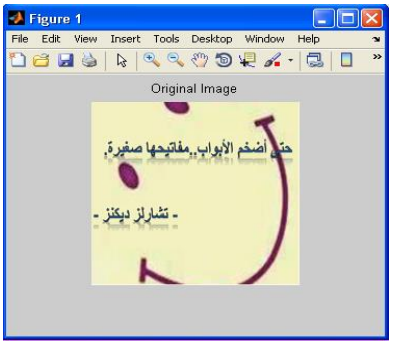
5- يتم في البداية توليد مجتمع ابتدائي من الأفراد، إذ أن إنشاء الجيل الابتدائي يعد نقطة الانطلاق لأي مسالة، وقد تم بناء الجيل الابتدائي بصورة عشوائية عن طريق استخدام الدالة (rand) الموجودة الماتلاب التي تعطي قيماً عشوائية تتراوح بين الصفر والواحد. وان عدد الأفراد يختلف من مسألة إلى أخرى.

التوصيات:

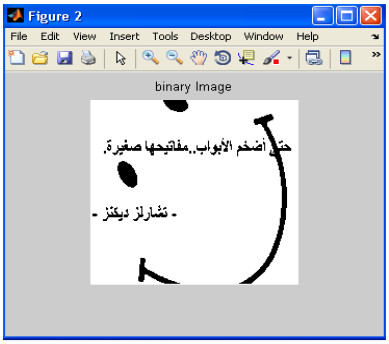
1- إرجاع الصورة المستخلصة بعد إزالة الغطاء وإزالة التشفير إلى الصورة الملونة.

2- تضمين الصور المشفرة في ملفات الوسائط المتعددة مثل الملفات الصوتية (MP3).

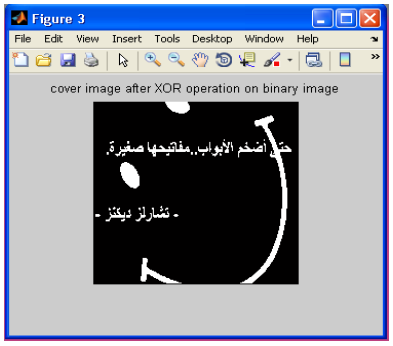
أشكال مراحل عملية إخفاء صورة مشفرة تحت صورة مرئية أخرى واسترجاعها



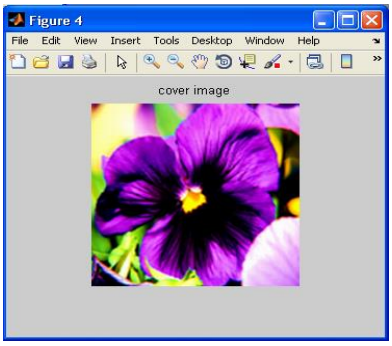
الشكل (1). الصورة المراد تشفيرها



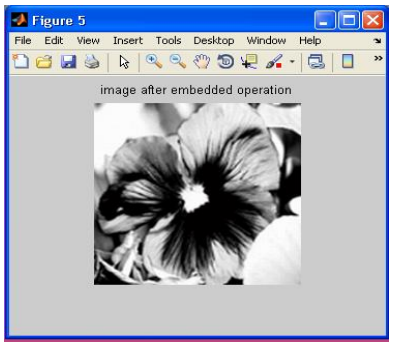
الشكل (2). الصورة المراد تشفيرها بعد تحويلها إلى Gray Level



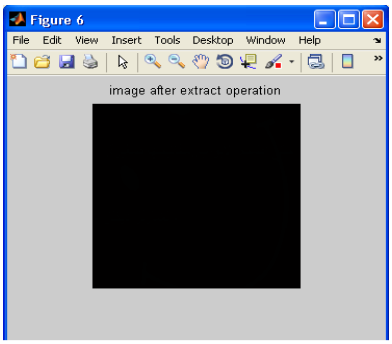
الشكل (3). الصورة المشفرة



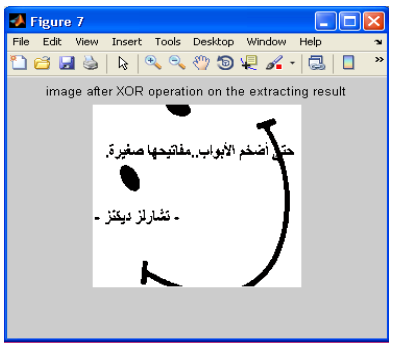
الشكل (4). صورة الغطاء المراد طمر الصورة المشفرة فيها



الشكل (5). الصورة الناتجة بعد طمر الصورة المشفرة



الشكل (6). الصورة الناتجة بعد رفع صورة الغطاء



الشكل (7). الصورة الناتجة بعد فك التشفير

المصادر

[1] الجوهرجي، شيماء شكيب، (2004)، "الإخفاء في ملف صوت مكبوس"، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[2] الحمامي، علاء حسين العاني، سعد عبد العزيز، (2007)، "تكنولوجيا أمنية المعلومات وأنظمة الحماية"، الطبعة الأولى، دار وائل للنشر.

[3] الصفار، لمى أكرم عبد الله (2001)، "تمييز اللهب في الصور الرقمية "، بحث ماجستير، كلية علوم الحاسوب والرياضيات، قسم علوم الحاسوب، جامعة الموصل، العراق.

[4] الصميدعي، عامر تحسين سهيل، (2002)، " تطبيق نظام التغطية"، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[5] النعيمي، سماح فخري، (2011)، "تحليل الإخفاء بالاعتماد على تقنيتي آلة المتجه الداعم ومميز فيشر الخطي في الصور الملونة"، رسالة ماجستير، كلية علوم الحاسوب والرياضيات، قسم علوم الحاسوب، جامعة الموصل، العراق.

[6] برزنجي، فوزي، (2008)، "اخفاء البيانات داخل الصورة"، جامعة السليمانية، العراق:
http://www.boosla.com/

[7] بشير، غصون سالم، (2003)، "استخدام الخوارزمية الجينية في مطابقة الصور"، رسالة ماجستير، جامعة الموصل، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[8] سعيد، ميلاد جادر، (2009)، "التشفير الانسيابي باستخدام الخوارزمية الجينية"، بحث منشور،مجلة الرافدين لعلوم الحاسبات والرياضيات، المجلد (6)، العدد (3).

[9] شعبان، هند رستم، (2008)، "أساسيات معالجة الصور الرقمية"، على موقع Kutub برقم 2866.

[10] محمد، هناء محمد عصمان، (2012)، "تحقيق وتطبيق نظام كشف وتصنيف التطفل المعتمد على الخوارزمية الجينية على بيانات NSL-KDD"، رسالة ماجستير، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[11] Al Shilany, Ismail Ali (2010), "Design and Implementation of Artificial Immune System for Detecting SYN-Flood Attack", MSc Thesis, Computer Science College, University of Mosul, Iraq.

[12] 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.

[13] Horn, J., Nafpliotis, N., (2001),"A Genetic Algorithms Search and Optimization Technique", on:
www.cs.unr.edu/~sushil/papers/conference/newpapers/2001/physics/atomicProcesses/poster.pdf

[14] Randy L. Haupt and Sue Ellen Haupt (2004), "Practical Genetic Algorithms", Second Edition, A John Willey & Enetic Sons, Inc., New York.

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

[16] MD. Khairullah (2011), "A Novel Text Steganography System in Cricket", International Journal of Computer Applications (0975–8887), Vol. 21, No.9, on:
www.nd.com/products/genetic/termination.htm

ملحق

Image 2


Figure 1
File Edit View Insert Tools Desktop Window Help
Original Image

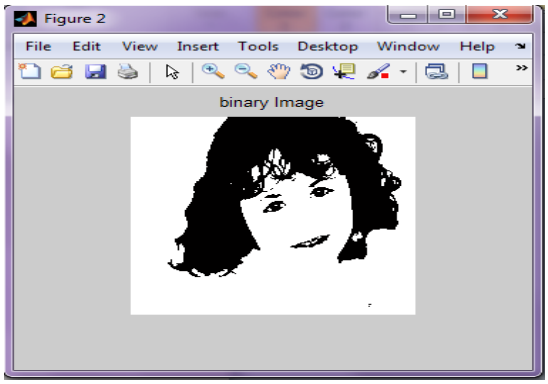


Figure 2
File Edit View Insert Tools Desktop Window Help
binary Image

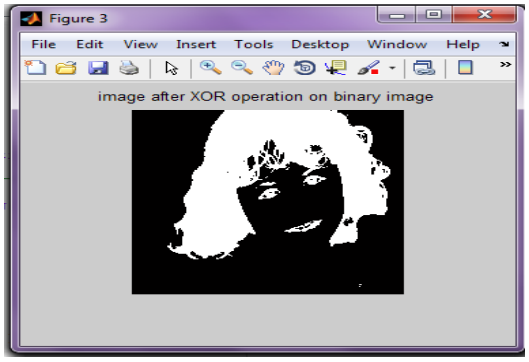


Figure 3
File Edit View Insert Tools Desktop Window Help
image after XOR operation on binary image

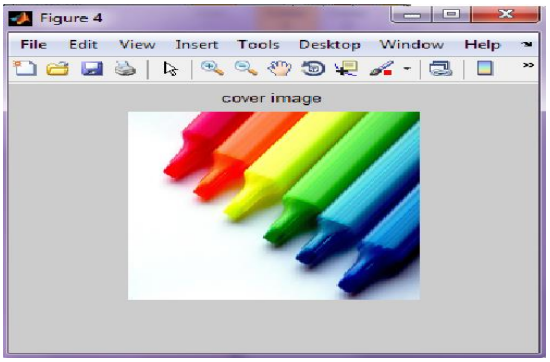


Figure 4
File Edit View Insert Tools Desktop Window Help
cover image

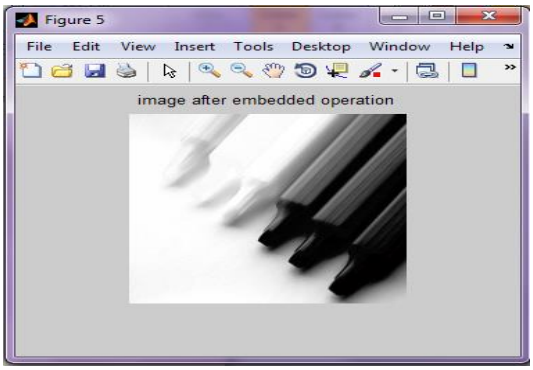


Figure 5
File Edit View Insert Tools Desktop Window Help
image after embedded operation

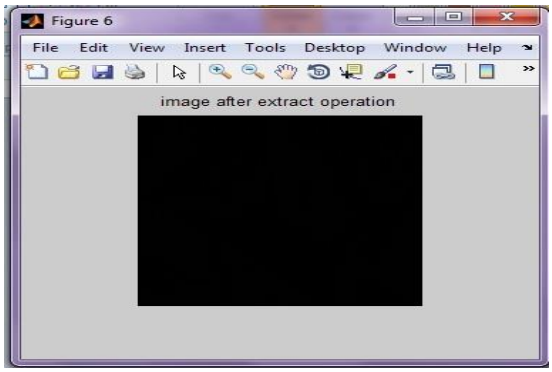


Figure 6
File Edit View Insert Tools Desktop Window Help
image after extract operation

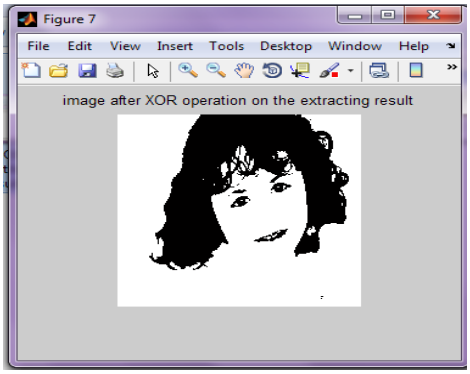


Figure 7
File Edit View Insert Tools Desktop Window Help
image after XOR operation on the extracting result

Image3

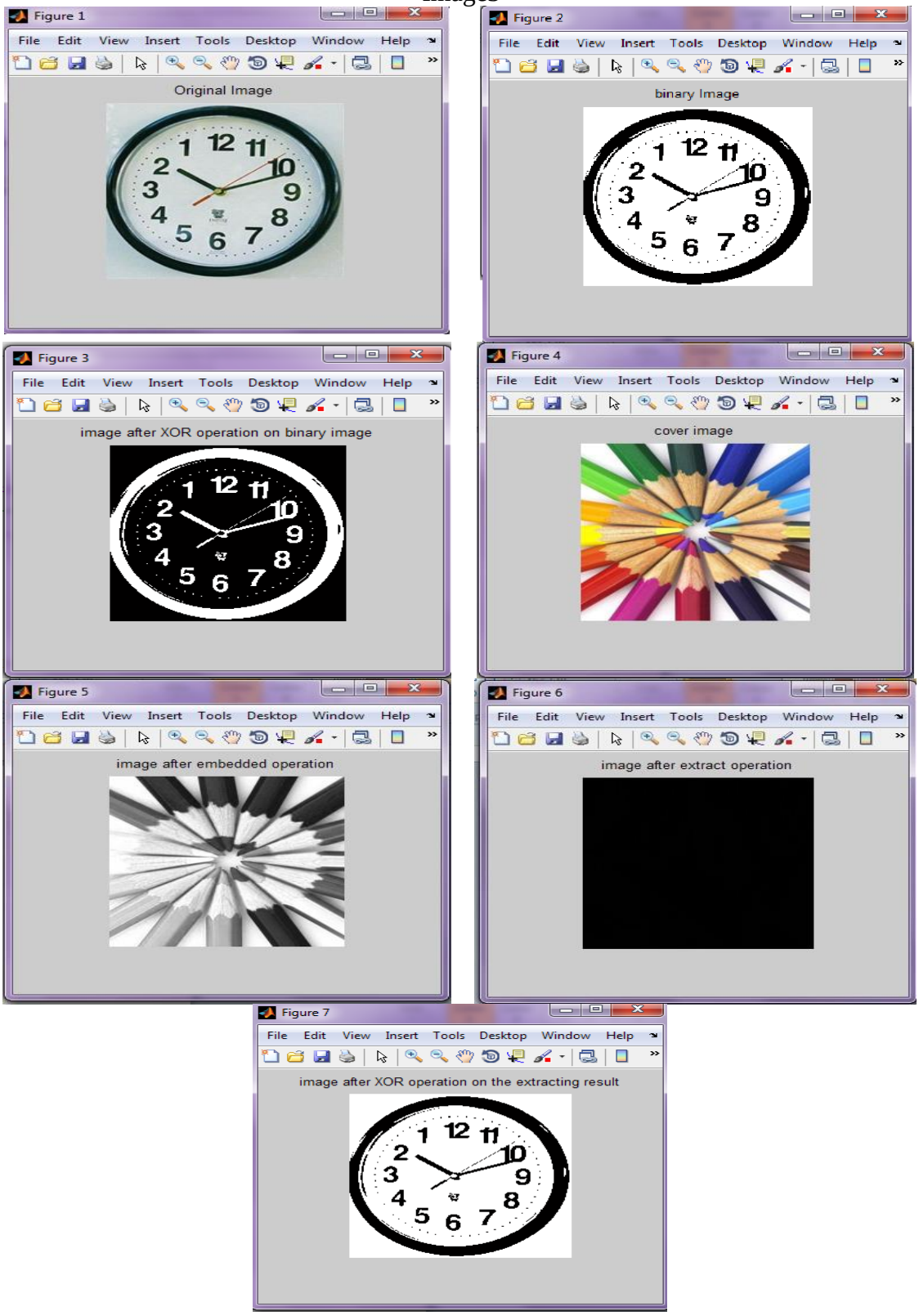


Figure 1
Original Image
Figure 2
binary Image
Figure 3
image after XOR operation on binary image
Figure 4
cover image
Figure 5
image after embedded operation
Figure 6
image after extract operation
Figure 7
image after XOR operation on the extracting result

Image4

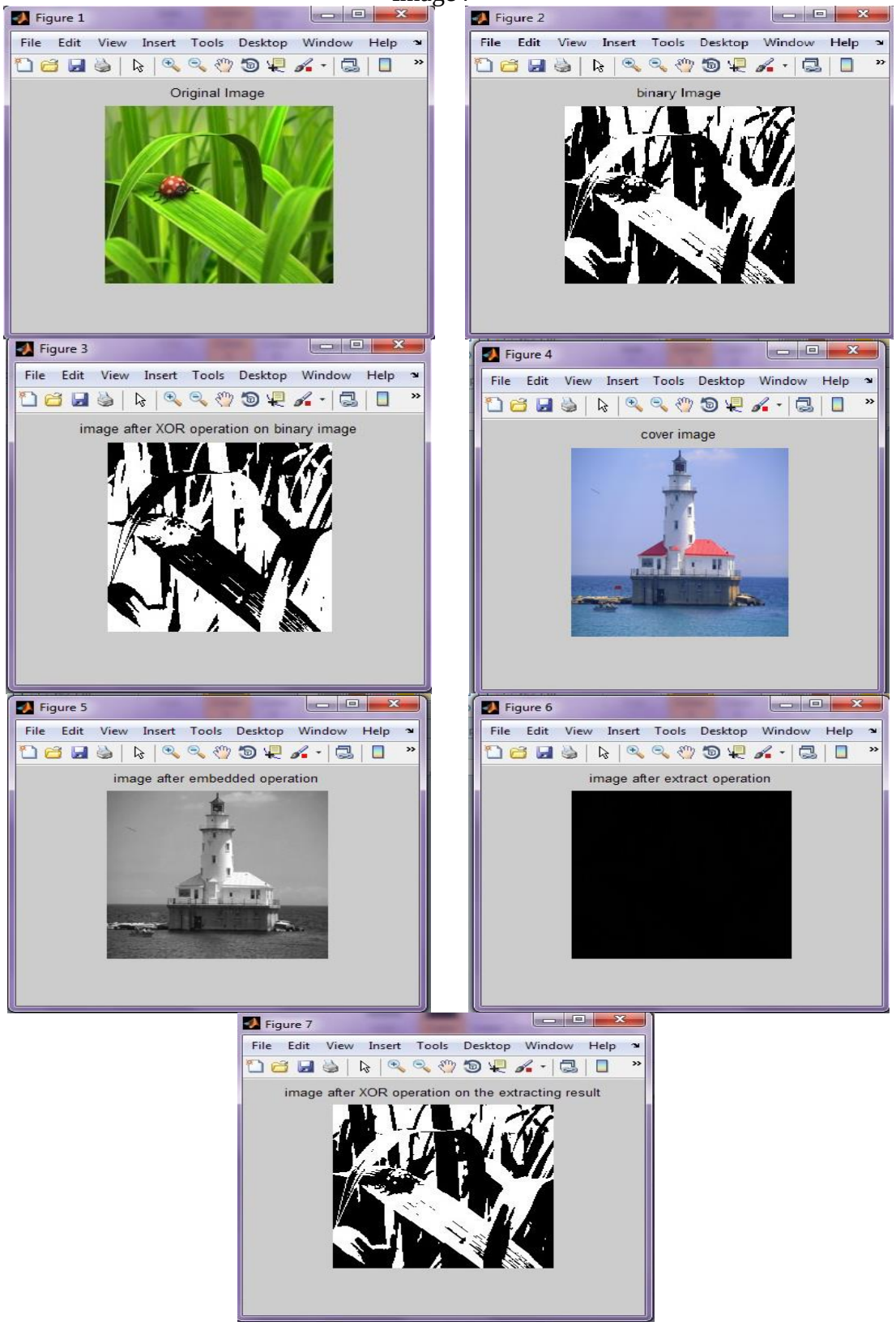


Figure 1
Original Image
Figure 2
binary Image
Figure 3
image after XOR operation on binary image
Figure 4
cover image
Figure 5
image after embedded operation
Figure 6
image after extract operation
Figure 7
image after XOR operation on the extracting result